AN TOÀN

Trong bối cảnh chuyển đổi số đang diễn ra nhanh chóng và sâu rộng, sinh viên – những công dân số tương lai – cần được trang bị đầy đủ kiến thức và kỹ năng để chủ động thích ứng, sử dụng công nghệ một cách hiệu quả và an toàn.

Chương trình đào tạo năng lực số cho sinh viên - miền năng lực An toàn được xây dựng đặc biệt nhằm hỗ trợ sinh viên phát triển khả năng nhận diện và ứng phó với các rủi ro trong môi trường số, dựa trên nhu cầu cá nhân và cộng đồng. Đây là nền tảng giúp các bạn không chỉ làm chủ công nghệ, mà còn đảm bảo sự an toàn thông tin và phát triển bền vững trong thế giới số ngày càng phức tạp và nhiều thách thức.

Khóa học này được thiết kế với mục tiêu toàn diện, tập trung vào ba khía cạnh chính:

Về kiến thức: Sinh viên sẽ được trang bị khả năng nhận diện và hiểu rõ các mối đe dọa từ tấn công mạng, mã độc, phần mềm gián điệp. Các bạn cũng sẽ nắm vững nguyên tắc bảo mật như tầm quan trọng của mật khẩu mạnh, xác thực đa yếu tố, và cập nhật phần mềm. Khóa học còn giúp các bạn hiểu về quyền riêng tư dữ liệu, cách phân biệt thông tin nhạy cảm và các quy định pháp lý liên quan. Đặc biệt, chúng ta sẽ cùng nhau nhận thức về tác động của công nghệ đối với sức khỏe, từ mỏi mắt, tư thế sai đến căng thẳng kỹ thuật số và nghiện internet. Cuối cùng, sinh viên sẽ nắm bắt tác động môi trường của công nghệ, hiểu về rác thải điện tử và khí thải số, từ đó có định hướng sử dụng công nghệ xanh.

Về kỹ năng: Khóa học sẽ giúp sinh viên bảo vệ thiết bị hiệu quả bằng cách thực hành cài đặt mật khẩu mạnh, thiết lập xác thực đa yếu tố, và sử dụng phần mềm bảo mật. Các bạn sẽ thành thạo kiểm soát dữ liệu và quyền riêng tư trên mạng xã hội và ứng dụng, cùng với kỹ năng bảo mật tài khoản trực tuyến cho email và ngân hàng. Để đảm bảo an sinh cá nhân, sinh viên sẽ học cách quản lý sức khỏe số, thiết lập thời gian sử dụng thiết bị hợp lý và nghỉ ngơi khoa học. Cuối cùng, các bạn sẽ thực hành tiêu dùng công nghệ bền vững, biết cách tiết kiệm năng lượng và tham gia tái sử dụng/tái chế linh kiện điện tử.

Về thái độ: Khóa học hướng tới việc hình thành ở sinh viên thái độ chủ động phòng ngừa các rủi ro mạng, không chủ quan trước những mối đe dọa. Các bạn sẽ phát triển sự tôn trọng quyền riêng tư của bản thân và người khác. Nâng cao trách nhiệm

với sức khỏe khi tương tác với công nghệ. Đặc biệt là ý thức môi trường, sử dụng công nghệ một cách bền vững và "xanh". Và luôn sẵn sàng cập nhật và học hỏi liên tục những kiến thức, kỹ năng an toàn số mới nhất.

Khóa học này tập trung vào bốn trụ cột chính để trang bị cho sinh viên một cách toàn diện:

1. Bảo vệ thiết bị: Các bạn sẽ được hướng dẫn cách bảo vệ điện thoại, máy tính, máy tính bảng khỏi tấn công mạng, mã độc và các mối đe dọa khác. Chúng ta sẽ cùng thực hành các biện pháp như cập nhật phần mềm, sử dụng mật khẩu mạnh, và thiết lập xác thực đa yếu tố để giữ an toàn cho công cụ học tập và làm việc của mình.

2. Bảo vệ dữ liệu cá nhân và quyền riêng tư: Trong thời đại dữ liệu, việc bảo vệ thông tin cá nhân là tối quan trọng. Khóa học giúp sinh viên hiểu tầm quan trọng của dữ liệu nhạy cảm, nắm bắt quy định pháp lý về quyền riêng tư, và học cách kiểm soát dữ liệu của bản thân trên các nền tảng số. Các bạn sẽ thực hành bảo mật tài khoản và cài đặt quyền riêng tư trên mạng xã hội một cách linh hoạt.

3. Bảo vệ sức khỏe và an sinh số: Sự gắn bó lâu dài với công nghệ có thể ảnh hưởng đến sức khỏe thể chất và tinh thần. Khóa học đặc biệt nhấn mạnh khía cạnh này, trang bị kiến thức về mỏi mắt, tư thế sai, rối loạn giấc ngủ, căng thẳng kỹ thuật số và nghiện internet. Đồng thời, các kỹ năng thiết lập thời gian sử dụng hợp lý, nghỉ ngơi khoa học sẽ được giới thiệu nhằm tăng cường an sinh cá nhân.

4. Bảo vệ môi trường: Phát triển công nghệ không thể tách rời trách nhiệm bảo vệ môi trường. Khóa học sẽ giáo dục sinh viên về tác động của rác thải điện tử, tiêu thụ năng lượng và khí thải số. Từ đó, các bạn sẽ hình thành ý thức sử dụng công nghệ theo hướng xanh và bền vững, thông qua việc tiết kiệm năng lượng, tái sử dụng/tái chế linh kiện điện tử và tham gia các sáng kiến công nghệ thân thiện môi trường.

Thông qua khóa học này, sinh viên không chỉ nâng cao năng lực sử dụng công nghệ an toàn mà còn phát triển tư duy phản biện, tinh thần trách nhiệm xã hội và ý thức công dân số. Đây là bước đệm quan trọng để các bạn hòa nhập hiệu quả, tự tin và bền vững trong kỷ nguyên số toàn cầu. Hãy cùng bắt đầu hành trình này!

BÀI 1: BẢO VỆ THIẾT BỊ

Chủ đề "Bảo vệ thiết bị" giúp người học nhận diện và áp dụng các biện pháp an toàn trong môi trường số một cách hiệu quả. Nội dung học tập tập trung vào việc phân biệt rõ ràng giữa các rủi ro và mối đe dọa có thể ảnh hưởng đến thiết bị và dữ liệu cá nhân. Qua đó, học viên sẽ biết cách lựa chọn các phương pháp bảo vệ phù hợp nhất, từ việc sử dụng phần mềm diệt virus, tường lửa, đến quản lý quyền truy cập và mã hóa thông tin. Ngoài ra, nội dung cũng đề cập đến khả năng đánh giá mức độ tin cậy và quyền riêng tư của các công cụ và dịch vụ số, từ đó giúp người học xây dựng thói quen sử dụng công nghệ một cách an toàn và có trách nhiệm. Đây là kiến thức nền tảng quan trọng để thích nghi và phát triển trong thế giới số hiện đại.

PHẦN I: THỰC TRẠNG TẤN CÔNG MẠNG NGÀY NAY

1. Thực trạng tấn công mạng trong quá khứ và hiện tại

"Tại sao chúng ta không thể ngăn chặn tất cả các cuộc tấn công này?" là một câu hỏi thường được nghe thấy. Mặc dù có vẻ như nên có một giải pháp đơn giản và dễ dàng để ngăn chặn các cuộc tấn công và bảo mật máy tính của chúng ta, nhưng trong thực tế không có một giải pháp đơn giản duy nhất nào. Điều này có thể được thấy qua các loại tấn công khác nhau mà người dùng máy tính phải đối mặt ngày nay cũng như những khó khăn trong việc phòng thủ chống lại các cuộc tấn công này.

Các cuộc tấn công ngày nay

Mặc dù an ninh thông tin tiếp tục được xếp vào nhóm mối quan tâm hàng đầu và hàng chục tỷ đô la được chi hàng năm cho an ninh máy tính, số lượng các cuộc tấn công thành công vẫn tiếp tục gia tăng. Thông tin về các cuộc tấn công gần đây bao gồm những điều sau đây:

- Các cuộc tấn công nhắm vào hệ thống điểm bán hàng (Point-of-Sale - PoS) tại các cửa hàng bán lẻ đã dẫn đến việc hơn 1,02 tỷ hồ sơ thông tin thẻ thanh toán của người tiêu dùng bị đánh cắp trong một năm. Con số này trung bình là 2,8 triệu hồ sơ bị đánh cắp mỗi ngày hoặc 32 hồ sơ mỗi giây.[1] Những phần trình độc hại này, được gọi là "memory-scrapers," đánh cắp số thẻ thanh toán của người dùng ngay khi thẻ được quẹt tại PoS. Vì các thiết bị đầu cuối PoS ngày nay là các máy tính để bàn hoặc máy tính bảng chuyên dụng, những kẻ tấn công đang lây nhiễm các thiết bị này bằng cách gửi email đến các nhà bán lẻ giả vờ là người tìm việc, với dòng tiêu đề là "Any Jobs?" (Có việc gì không?) hoặc "My Resume" (Sơ yếu lý lịch của tôi). Đính kèm email là một tệp Microsoft Word giả vờ là một sơ yếu lý lịch và thậm chí còn ghi "Protected Document: This file is protected by Microsoft Office" (Tài liệu được bảo vệ: Tệp này được bảo vệ bởi Microsoft Office). Tuy nhiên, tệp này chứa một phần trình độc hại mà khi mở ra sẽ lây nhiễm vào hệ thống PoS.
- Một trong những mục tiêu chính của những kẻ tấn công ngày nay là ngành công nghiệp chăm sóc sức khỏe. Đó là vì hồ sơ sức khỏe chứa nhiều thông tin hơn là chỉ số thẻ thanh toán của bệnh nhân. Những hồ sơ này chứa thông tin y tế và thông tin tài chính về bệnh nhân và gia đình, sau đó có thể được sử dụng để đánh cắp danh tính của họ. Ngoài ra, hồ sơ y tế bị đánh cắp có thể được sử dụng cho gian lận thanh toán

(tính phí các phương pháp điều trị y tế cho nạn nhân), cho trộm cắp danh tính y tế (giả vờ là nạn nhân để nhận chăm sóc y tế), và thậm chí để mua thuốc bán lại. Và vì luật pháp liên bang cấm các phần trình bảo hiểm sức khỏe có giới hạn đô la hàng năm hoặc trọn đời đối với hầu hết các phúc lợi y tế, những kẻ tấn công có thể sử dụng thông tin chăm sóc sức khỏe bị đánh cắp để thực hiện các hành vi gian lận dẫn đến số tiền khổng lồ. Một báo cáo ngành công nghiệp tiết lộ rằng trong một năm, các nhà cung cấp dịch vụ chăm sóc sức khỏe và các bên thanh toán đã báo cáo sự gia tăng 60% các cuộc tấn công được phát hiện, với tổn thất tài chính từ những cuộc tấn công này tăng 282% so với năm trước.[2] Một báo cáo khác chỉ ra rằng trong khoảng thời gian 24 tháng, 91% các tổ chức chăm sóc sức khỏe đã báo cáo ít nhất một vụ vi phạm, 39% báo cáo từ hai đến năm vụ vi phạm dữ liệu, và 40% có hơn năm vụ vi phạm dữ liệu. Tổng chi phí cho các vụ vi phạm dữ liệu chăm sóc sức khỏe là khoảng 6 tỷ đô la mỗi năm, với mức tổn thất trung bình cho mỗi tổ chức là 2.134.800 đô la.[3]

- Lỗ hổng trong thiết bị mạng không dây gia đình đã được tìm thấy trong 90 sản phẩm từ 25 nhà sản xuất lớn, có thể cho phép kẻ tấn công khởi chạy phần mềm độc hại của chúng chống lại bất kỳ thiết bị nào được kết nối với mạng gia đình. Dịch vụ dễ bị tổn thương chạy trên thiết bị không thể bị vô hiệu hóa và các cuộc tấn công từ Internet cũng không thể bị chặn. Trong khi một số nhà sản xuất đã ban hành các bản sửa lỗi ngay lập tức cho thiết bị của họ, các nhà sản xuất khác cho biết việc tạo và phân phối các bản sửa lỗi sẽ mất vài tháng. Và một số nhà sản xuất cho biết sản phẩm của họ đã đến giai đoạn "kết thúc vòng đời" ("end-of-life") và sẽ không được vá lỗi.[4]
- Một phóng viên tạp chí đã đồng ý để hai nhà nghiên cứu bảo mật trình diễn việc một chiếc xe có thể dễ dàng bị điều khiển từ xa như thế nào. Từ một địa điểm cách xa mười dặm, các nhà nghiên cứu đã thao túng hệ thống điều hòa không khí, radio và cần gạt nước kính chắn gió của chiếc xe, mà người lái xe không thể thay đổi. Khi người lái xe nhấn ga để nhập vào một đường cao tốc đông đúc, chiếc xe bắt đầu giảm tốc độ với một chiếc xe tải 18 bánh đang lao tới phía sau anh ta khi các nhà nghiên cứu tiếp tục thao túng chiếc xe. Các nhà nghiên cứu thậm chí còn vô hiệu hóa phanh khiến chiếc xe lao xuống một con mương.[5] Vụ việc này đã thúc đẩy Cơ quan Quản lý An toàn Giao thông Đường bộ Quốc gia (NHTSA) đã phải thu hồi 1,4 triệu xe để vá lỗ hổng này, đánh dấu lần đầu tiên xe ô tô bị thu hồi do một lỗ hổng bảo mật.[6]

- Đã có nhiều đồn đoán trong vài năm rằng ai đó có thể điều khiển máy bay trong khi bay vì các hệ thống kiểm soát máy bay không được bảo vệ đúng cách. Theo FBI, một nhà nghiên cứu bảo mật có thể đã thực sự làm điều đó. Trên một chuyến bay giữa Chicago và Syracuse, một nhà nghiên cứu đã tweet rằng anh ta đang thăm dò hệ thống máy bay của chuyến bay. Bộ phận Tình báo An ninh Mạng của hãng hàng không, chuyên theo dõi mạng xã hội, đã thấy dòng tweet và báo cho FBI. Theo FBI, một đặc vụ sau đó đã kiểm tra ghế hạng nhất nơi nhà nghiên cứu ngồi và phát hiện ra rằng anh ta đã can thiệp vào Hộp Điện tử Ghế (Seat Electronic Box - SEB), được đặt dưới một số ghế hành khách. Điều này cho phép anh ta kết nối máy tính xách tay của mình với hệ thống giải trí trên chuyến bay (in-flight entertainment - IFE) thông qua SEB. Một khi nhà nghiên cứu truy cập vào IFE, anh ta có thể truy cập các hệ thống khác trên máy bay. Nhà nghiên cứu tuyên bố rằng anh ta đã có thể khiến máy bay tăng độ cao sau khi điều khiển phần mềm của nó. Hãng hàng không hiện đã cấm anh ta trên tất cả các chuyến bay của mình.[7]

- Nhiều xe ô tô ngày nay cung cấp hệ thống Mở khóa và Khởi động không cần chìa khóa thụ động (Passive Keyless Entry and Start - PKES), cho phép người lái xe mở khóa cửa và khởi động xe mà không cần phải lấy chìa khóa ra khỏi túi hoặc ví. Tất cả những gì người lái xe cần làm là đến đủ gần xe để tín hiệu không dây từ chìa khóa của họ được xe phát hiện, và một khi được phát hiện, cửa sẽ tự động mở khóa và động cơ có thể được khởi động bằng cách nhấn một nút trên bảng điều khiển. Gần đây, một khu phố ở Los Angeles đã trải qua một loạt các vụ đột nhập bí ẩn vào những chiếc xe có hệ thống PKES. Một người, tình cờ là một phóng viên báo chí, đã bị đột nhập vào xe ba lần nhưng không có bằng chứng về việc bị cạy phá. Một ngày nọ, khi người phóng viên quan sát chiếc xe của mình từ bên trong nhà, anh ta thấy một cô gái trẻ đi xe đạp đến và sau đó lấy ra một thiết bị nhỏ màu đen từ ba lô của cô. Sau đó, cô đi đến, mở khóa xe và trèo vào trong. Người chủ nhà chạy ra ngoài và cô gái nhanh chóng rời đi. Rõ ràng cô gái đã sử dụng một bộ khuếch đại công suất rẻ tiền: khi cô bật bộ khuếch đại, nó đã tăng khoảng cách mà chiếc xe có thể tìm kiếm chìa khóa lên hơn 50 feet (15 mét). Mặc dù chìa khóa đang nằm trên quầy bếp bên trong nhà của người phóng viên, chiếc xe vẫn có thể phát hiện ra nó và bị lừa nghĩ rằng người lái xe đang đến gần.[8] Chi phí của bộ khuếch đại chỉ là 17 đô la. Các chủ xe muốn tự bảo vệ mình

khỏi cuộc tấn công này đang được khuyên nên đặt chìa khóa của họ vào tủ đông, điều này sẽ ngăn tín hiệu được khuếch đại tiếp cận chìa khóa.

- Một bộ mẫu gồm hàng chục ngàn tệp độc hại đã được quét bởi bốn sản phẩm chống virus được triển khai phổ biến nhất. Trong vòng một giờ đầu tiên, các sản phẩm chống virus chỉ xác định được 30% phần mềm độc hại. Phải mất 24 giờ trước khi các sản phẩm này xác định chính xác 66% các tệp bị nhiễm là độc hại, và sau bảy ngày tổng số tích lũy là 72%. Tuy nhiên, phải mất hơn sáu tháng để bốn sản phẩm chống virus xác định và bảo vệ chính xác tất cả các tệp độc hại. Dựa trên số lượng lây nhiễm trung bình được kẻ tấn công phân phối, điều này có nghĩa là các sản phẩm chống virus này sẽ bỏ lỡ 796 tệp độc hại mỗi ngày.[9]

- Nữ nghệ sĩ giải trí biểu tượng Madonna đã buộc phải nhanh chóng đẩy nhanh việc phát hành sáu bài hát từ một trong những album sắp tới của mình để mua ngay lập tức, mặc dù album này chưa được lên kế hoạch xuất hiện trong ba tháng nữa. Việc phát hành khẩn cấp này là do 13 bản ghi âm trước khi phát hành, có lẽ là toàn bộ album, đã bị đánh cắp và rò rỉ trên Internet. Ngoài ra, những bức ảnh chưa được công bố trước đây cũng đã bị lấy và đăng tải mà không có sự cho phép. Madonna tuyên bố rằng để chống lại các vụ rò rỉ trong tương lai, nội dung của cô sẽ không còn được đặt trên bất kỳ thiết bị nào kết nối với một mạng hoặc Internet. Thay vào đó, các ổ cứng chứa nhạc sẽ được chuyển tay đến người nhận. Madonna tiếp tục nói rằng tại bất kỳ buổi chụp ảnh hoặc quay video nào trong tương lai, mọi người liên quan sẽ phải để điện thoại di động của họ ở cửa.[10]

- Trong một cuộc khảo sát gần đây, 69% người Mỹ báo cáo rằng họ thường xuyên hoặc thỉnh thoảng lo lắng về việc thông tin thẻ thanh toán của họ bị kẻ tấn công mạng đánh cắp. Con số này so với 45% người lo lắng về việc nhà của họ bị trộm và 7% lo ngại về việc bị một đồng nghiệp hành hung. Người Mỹ trong độ tuổi từ 30 đến 64 lo lắng về điều này nhiều hơn so với những người Mỹ trẻ hơn và lớn tuổi hơn. Và gần một phần ba cho biết họ hoặc một thành viên khác trong gia đình đã bị kẻ tấn công máy tính đánh cắp thông tin từ một thẻ thanh toán được sử dụng tại một cửa hàng trong năm qua, khiến đây trở thành tội phạm được trải nghiệm thường xuyên nhất trong danh sách chín loại tội phạm.[11]

- Mặc dù thực tế là một số người dùng máy tính Apple có thể cảm thấy thiết bị của họ an toàn hơn so với các nhà sản xuất khác, các lỗ hổng trong thiết bị Apple vẫn tiếp tục bị phơi bày và lợi dụng bởi những kẻ tấn công. Gần đây, một lỗ hổng nghiêm trọng trên máy tính Apple đã được tìm thấy dựa trên một lỗi triển khai tính năng tiết kiệm năng lượng, khiến các biện pháp bảo vệ bị mở khóa trên các máy Mac bị ảnh hưởng sau khi chúng khởi động từ chế độ ngủ. Lỗ hổng này được đánh giá là nghiêm trọng vì nó có thể cung cấp cho kẻ tấn công quyền truy cập liên tục vào máy tính ngay cả khi người dùng đã xóa sạch ổ cứng và cài đặt lại hệ điều hành. Tất cả các mẫu máy tính Mac của Apple, trừ những mẫu mới nhất, đều bị ảnh hưởng bởi lỗ hổng này.[12]
- Số vụ vi phạm an ninh làm lộ dữ liệu số của người dùng cho kẻ tấn công vẫn tiếp tục gia tăng. Từ tháng 1 năm 2005 đến tháng 7 năm 2015, hơn 853 triệu hồ sơ dữ liệu điện tử tại Hoa Kỳ đã bị vi phạm, làm lộ ra cho kẻ tấn công một loạt dữ liệu điện tử cá nhân, như địa chỉ, số An sinh Xã hội, hồ sơ sức khỏe và số thẻ tín dụng.[13] Bảng 1-1 liệt kê một số vụ vi phạm an ninh xảy ra chỉ trong vòng một tháng, theo Privacy Rights Clearinghouse.[14]

Bảng 1-1 Các vụ vi phạm an ninh được chọn liên quan đến thông tin cá nhân trong một tháng

Tổ chức	Mô tả về vụ vi phạm an ninh	Số lượng danh tính bị lộ
Văn phòng Quản lý Nhân sự (Office of Personnel Management)	Các nhân viên liên bang hiện tại và trước đây bị lộ thông tin về phân công công việc, hiệu suất và đào tạo, và có thể đã bị lộ thông tin An sinh Xã hội và/hoặc thông tin tài chính.	4,000,000
CareFirst BlueCross BlueShield	Vụ vi phạm một cơ sở dữ liệu duy nhất đã làm lộ tên, ngày sinh, địa chỉ email và số nhận dạng bảo hiểm.	1,100,000
Trường Kỹ thuật của Đại học Penn State	Trong hai cuộc xâm nhập khác nhau, những kẻ tấn công đã truy cập "dữ liệu nhạy cảm" của tất cả sinh viên, giảng viên và nhân viên của Trường Kỹ thuật.	18,000

Salley Beauty	"Hoạt động bất thường của thẻ thanh toán tại một số cửa hàng" theo sau một cuộc tấn công tương tự 60 ngày trước đó, trong đó thông tin trên hơn 25.000 thẻ thanh toán của khách hàng đã bị đánh cắp.	Không rõ
AT&T	Trong ba sự cố riêng biệt, các nhân viên đã truy cập tên và số An sinh Xã hội của khách hàng, sau đó bán chúng cho những người bên ngoài, những người đã sử dụng thông tin đó để mở khóa các điện thoại di động bị đánh cắp.	280,000
Anthem BlueCross BlueShield	Tên, ngày sinh, ID y tế, số An sinh Xã hội, địa chỉ đường phố, địa chỉ email, thông tin việc làm và thu nhập đã bị đánh cắp trong một cuộc tấn công có thể đã không bị phát hiện trong mười tháng.	80,000,000

2. Các loại đối tượng tấn công mạng

Trước đây, thuật ngữ *hacker* dùng để chỉ một người sử dụng các kỹ năng máy tính tiên tiến để tấn công máy tính. Tuy nhiên, thuật ngữ đó không phản ánh chính xác các động cơ và mục tiêu khác nhau của những kẻ tấn công. Thay vào đó, ngày nay các loại kẻ tấn công được mô tả chi tiết hơn, bao gồm: tội phạm mạng (cybercriminals), script kiddies, nhà môi giới (brokers), người nội bộ (insiders), khủng bố mạng (cyberterrorists), nhà hoạt động tin tặc (hactivists), và kẻ tấn công được nhà nước bảo trợ (state-sponsored attackers).

Tội phạm mạng (Cybercriminals)

Thuật ngữ chung *tội phạm mạng* (cybercriminals) thường được dùng để mô tả những cá nhân phát động các cuộc tấn công chống lại những người dùng khác và máy tính của họ (một từ chung khác đơn giản là *kẻ tấn công* - attackers). Tuy nhiên, nói một cách chính xác, tội phạm mạng là một mạng lưới lỏng lẻo của những kẻ tấn công, những kẻ trộm danh tính, và những kẻ lừa đảo tài chính, những người có động cơ cao,

ít ngại rủi ro, được tài trợ tốt và ngoan cường. Một số chuyên gia bảo mật tin rằng nhiều tội phạm mạng thuộc về các băng nhóm tội phạm có tổ chức của những kẻ tấn công trẻ tuổi, thường tập trung ở các khu vực Đông Âu, Châu Á và Thế giới thứ ba. Tội phạm mạng thường gặp nhau trong các diễn đàn "ngầm" trực tuyến ẩn để trao đổi thông tin, mua bán dữ liệu bị đánh cắp và các công cụ tấn công, và thậm chí phối hợp các cuộc tấn công. Bảng 1-2 mô tả sự khác biệt giữa các diễn đàn này và các trang web thông thường.

Bảng 1-2 Các diễn đàn ngầm

Tên	Mô tả	Ví dụ
Surface web (Web bề mặt)	Bất cứ thứ gì có thể được tìm thấy và lập chỉ mục bởi một công cụ tìm kiếm	Trang web của nhà xuất bản sách giáo khoa
Deep web (Web chìm)	Nội dung không thể tìm thấy bởi một công cụ tìm kiếm mà chỉ có thể thông qua một hộp thoại tìm kiếm trên trang web đó	Cơ sở dữ liệu giấy phép y tế của tiểu bang
Dark web (Web tối)	Thông tin đã được cố tình che giấu và không thể truy cập thông qua một trình duyệt web tiêu chuẩn	Trang web chợ đen của kẻ tấn công

Thay vì tấn công một máy tính để khoe khoang kỹ năng công nghệ của mình (*fame* - danh tiếng), tội phạm mạng có một mục tiêu tập trung hơn là lợi ích tài chính (*fortune* - tài sản): tội phạm mạng khai thác các lỗ hổng để đánh cắp thông tin hoặc phát động các cuộc tấn công có thể tạo ra thu nhập. Sự khác biệt này làm cho những kẻ tấn công mới trở nên nguy hiểm hơn và các cuộc tấn công của chúng mang tính đe dọa hơn. Những cuộc tấn công nhắm mục tiêu vào các mạng tài chính và việc đánh cắp thông tin cá nhân đôi khi được gọi là *tội phạm mạng* (cybercrime).

Tội phạm mạng tài chính thường được chia thành hai loại. Loại đầu tiên tập trung vào các cá nhân và doanh nghiệp. Tội phạm mạng đánh cắp và sử dụng dữ liệu bị đánh cắp, số thẻ tín dụng, thông tin tài khoản tài chính trực tuyến, hoặc số An sinh Xã hội để trục lợi từ nạn nhân của họ hoặc gửi hàng triệu email spam để bán thuốc giả, phần mềm lậu, đồng hồ giả và nội dung khiêu dâm.

Loại thứ hai tập trung vào các doanh nghiệp và chính phủ. Tội phạm mạng cố gắng đánh cắp nghiên cứu về một sản phẩm mới từ một doanh nghiệp để họ có thể bán nó cho một nhà cung cấp nước ngoài vô đạo đức, người sau đó sẽ xây dựng một mô hình nhái của sản phẩm để bán trên toàn thế giới. Điều này tước đi lợi nhuận của doanh nghiệp hợp pháp sau khi đã đầu tư hàng trăm triệu đô la vào việc phát triển sản phẩm, và vì các nhà cung cấp nước ngoài này ở một quốc gia khác, họ nằm ngoài tầm với của các cơ quan thực thi pháp luật và tòa án trong nước. Chính phủ cũng là mục tiêu của tội phạm mạng: nếu thông tin mới nhất về một hệ thống phòng thủ tên lửa mới có thể bị đánh cắp, nó có thể được bán—với giá cao—cho kẻ thù của chính phủ đó.

LƯU Ý

Một số chuyên gia bảo mật cho rằng tội phạm mạng Đông Âu chủ yếu tập trung vào các hoạt động đánh cắp tiền từ cá nhân và doanh nghiệp, trong khi tội phạm mạng từ Đông Á quan tâm nhiều hơn đến việc đánh cắp dữ liệu từ chính phủ hoặc doanh nghiệp. Điều này dẫn đến các cách tiếp cận khác nhau trong các cuộc tấn công của họ. Tội phạm mạng Đông Âu có xu hướng sử dụng phần mềm độc hại (malware) được xây dựng tùy chỉnh, rất phức tạp trong khi những kẻ tấn công Đông Á sử dụng phần mềm độc hại có sẵn và các kỹ thuật đơn giản hơn. Ngoài ra, những kẻ tấn công Đông Âu làm việc trong các nhóm nhỏ, gắn kết chặt chẽ và trực tiếp hưởng lợi từ các cuộc tấn công của họ. Tội phạm mạng Đông Á thường là một phần của một nhóm lớn hơn của những kẻ tấn công làm việc theo chỉ đạo của các tổ chức lớn mà họ nhận được chỉ thị và hỗ trợ tài chính.

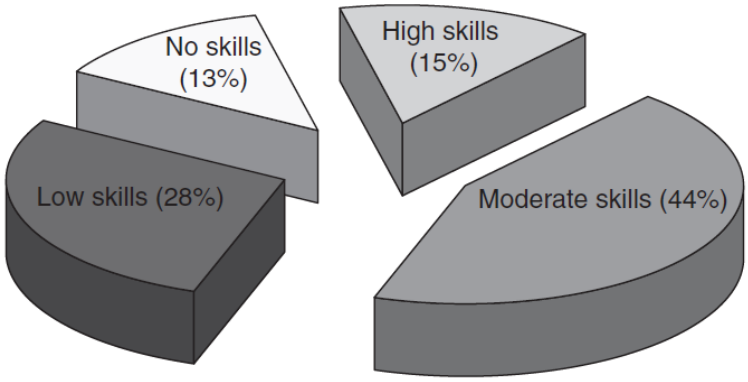
Script Kiddies

Script kiddies là những cá nhân trẻ tuổi muốn tấn công máy tính, nhưng lại thiếu kiến thức cần thiết về máy tính và mạng để làm điều đó. Thay vào đó, *script kiddies* thực hiện công việc của mình bằng cách tải xuống phần mềm tấn công tự động (scripts) từ các trang web và sử dụng nó để thực hiện các hành vi độc hại. Hình 1-1 minh họa các kỹ năng cần thiết để tạo ra các cuộc tấn công. Hơn 40% các cuộc tấn công đòi hỏi kỹ năng thấp hoặc không có kỹ năng và thường được thực hiện bởi *script kiddies*.

(Biểu đồ tròn thể hiện kỹ năng cần thiết để tạo ra các cuộc tấn công)

- Không có kỹ năng (13%)

- Kỹ năng thấp (28%)
- Kỹ năng trung bình (44%)
- Kỹ năng cao (15%)



Hình 1-1 Kỹ năng cần thiết để tạo ra các cuộc tấn công

Ngày nay, *script kiddies* có thể mua toàn bộ *exploit kits* (bộ công cụ khai thác) từ những kẻ tấn công khác để dễ dàng tạo ra một cuộc tấn công. *Script kiddies* có thể thuê hoặc mua bộ công cụ từ tác giả của nó và sau đó chỉ định các tùy chọn khác nhau để tùy chỉnh các cuộc tấn công của họ.

LƯU Ý

Ước tính có khoảng ba trong số bốn cuộc tấn công dựa trên Internet bắt nguồn từ các *exploit kits*.[20]

Nhà môi giới (Brokers)

Trong những năm gần đây, một số nhà cung cấp phần mềm đã bắt đầu thưởng tài chính cho những cá nhân phát hiện ra các lỗ hổng trong phần mềm của họ và sau đó báo cáo riêng cho các nhà cung cấp để các điểm yếu có thể được khắc phục. Một số nhà cung cấp thậm chí còn tài trợ các cuộc thi hàng năm gọi là "Bug Bounties" và trả hậu hĩnh cho những người có thể tấn công thành công phần mềm của họ để tiết lộ các lỗ hổng.

LƯU Ý

Google gần đây đã trả cho một nhà nghiên cứu bảo mật 150.000 đô la để phát hiện ra một lỗi duy nhất.[21] Trong một năm, Facebook đã trả cho 321 nhà nghiên cứu từ 65 quốc gia (Ấn Độ có nhiều đệ trình nhất với 196 trong khi Hoa Kỳ đứng thứ ba với 61) tổng cộng 1,3 triệu đô la để phát hiện ra các lỗi, điều này đã cho phép Facebook sửa chữa 61 lỗ hổng có mức độ nghiêm trọng cao, gấp đôi so với năm trước.[22]

Tuy nhiên, những cá nhân khác phát hiện ra các lỗ hổng không báo cáo cho nhà cung cấp phần mềm mà thay vào đó bán chúng cho người trả giá cao nhất. Được biết đến với tên gọi **brokers** (nhà môi giới), những kẻ tấn công này bán kiến thức của họ về một lỗ hổng cho những kẻ tấn công khác hoặc thậm chí cả các chính phủ. Những người mua này thường sẵn sàng trả giá cao vì lỗ hổng này chưa được nhà cung cấp phần mềm biết đến và do đó không có khả năng được "vá" cho đến khi các cuộc tấn công mới dựa trên nó đã lan rộng.

Người nội bộ (Insiders)

Một mối đe dọa nghiêm trọng khác đối với một tổ chức thực sự đến từ một nguồn không ngờ: nhân viên, nhà thầu và đối tác kinh doanh của chính tổ chức đó, thường được gọi là **insiders** (người nội bộ). Ví dụ, một nhân viên chăm sóc sức khỏe bất mãn về việc sắp bị chấm dứt hợp đồng có thể thu thập bất hợp pháp hồ sơ sức khỏe của những người nổi tiếng và bán chúng cho giới truyền thông, hoặc một nhà giao dịch chứng khoán thua lỗ hàng tỷ đô la trong các vụ cá cược cổ phiếu tồi tệ có thể sử dụng kiến thức của mình về hệ thống an ninh máy tính của ngân hàng để che giấu các khoản lỗ thông qua các giao dịch giả mạo. Trong một nghiên cứu về 900 trường hợp "rò rỉ dữ liệu" kinh doanh, hơn 48% các vụ vi phạm được cho là do những người nội bộ lạm dụng quyền truy cập thông tin của công ty.[23] Những cuộc tấn công này khó nhận biết hơn vì chúng đến từ bên trong tổ chức nhưng lại có thể gây tốn kém hơn so với các cuộc tấn công từ bên ngoài.

Hầu hết các cuộc tấn công độc hại từ người nội bộ bao gồm việc phá hoại hoặc trộm cắp tài sản trí tuệ. Một nghiên cứu cho thấy hầu hết các trường hợp phá hoại đến từ những nhân viên đã thông báo nghỉ việc hoặc đã bị khiển trách, giáng chức hoặc sa thải chính thức. Khi có hành vi trộm cắp, thủ phạm thường là nhân viên bán hàng, kỹ sư, lập trình viên máy tính hoặc nhà khoa học, những người thực sự tin rằng dữ liệu tích lũy là của họ chứ không phải của tổ chức (hầu hết các vụ trộm này xảy ra trong vòng 30 ngày sau khi nhân viên nghỉ việc). Trong một số trường hợp, nhân viên chuyển sang một công việc mới và muốn mang "công việc của họ" theo, trong khi ở các trường hợp khác, nhân viên đã bị mua chuộc hoặc bị áp lực để đánh cắp dữ liệu. Trong khoảng 8% các sự cố trộm cắp, nhân viên đã bị áp lực để đánh cắp từ chủ lao động của họ thông qua tống tiền hoặc đe dọa bạo lực.[24]

LƯU Ý

Trong những năm gần đây, những người nội bộ làm việc trực tiếp hoặc gián tiếp cho một chính phủ đã đánh cắp một lượng lớn thông tin nhạy cảm và sau đó công bố nó. Mục đích là để cảnh báo công dân về các hành động bí mật của chính phủ và gây áp lực để chính phủ thay đổi chính sách của mình.

Khủng bố mạng (Cyberterrorists)

Nhiều chuyên gia an ninh lo ngại rằng những kẻ khủng bố sẽ chuyển các cuộc tấn công của chúng sang mạng lưới và cơ sở hạ tầng máy tính của một quốc gia để gây ra sự gián đoạn và hoảng loạn trong dân chúng. Được biết đến với tên gọi **cyberterrorists** (khủng bố mạng), động cơ của chúng là ý thức hệ, tấn công vì nguyên tắc hoặc niềm tin của chúng. Khủng bố mạng có thể là những kẻ tấn công đáng sợ nhất, vì gần như không thể dự đoán được khi nào hoặc ở đâu một cuộc tấn công có thể xảy ra. Không giống như tội phạm mạng liên tục thăm dò hệ thống hoặc tạo ra các cuộc tấn công, khủng bố mạng có thể không hoạt động trong vài năm và sau đó đột ngột tấn công theo một cách mới. Mục tiêu của chúng có thể bao gồm một nhóm nhỏ các máy tính hoặc mạng có thể ảnh hưởng đến số lượng người dùng lớn nhất, chẳng hạn như các máy tính điều khiển lưới điện của một tiểu bang hoặc khu vực.

Hactivists

Một nhóm khác có động cơ ý thức hệ là **hactivists**. Không giống như những kẻ khủng bố mạng phát động các cuộc tấn công chống lại các quốc gia nước ngoài để gây hoảng loạn, *hactivists* (một sự kết hợp của các từ *hack* và *activism* - hoạt động) thường không được định nghĩa rõ ràng. Các cuộc tấn công của *hactivists* có thể liên quan đến việc đột nhập vào một trang web và thay đổi nội dung trên trang đó như một phương tiện để đưa ra một tuyên bố chính trị chống lại những người phản đối niềm tin của họ. Ngoài các cuộc tấn công như một phương tiện để phản đối hoặc thúc đẩy một chương trình nghị sự chính trị, các cuộc tấn công khác có thể mang tính trả đũa. Ví dụ, các hactivist có thể vô hiệu hóa trang web của một ngân hàng vì ngân hàng đó đã ngừng chấp nhận các khoản thanh toán trực tuyến được gửi vào các tài khoản thuộc về các hactivist.

Kẻ tấn công được Nhà nước bảo trợ (State-Sponsored Attackers)

Thay vì sử dụng một đội quân để hành quân qua chiến trường để tấn công đối thủ, các chính phủ đang sử dụng **state-sponsored attackers** (kẻ tấn công được nhà nước bảo trợ) để phát động các cuộc tấn công máy tính chống lại kẻ thù của họ. Kẻ thù có thể là các chính phủ nước ngoài hoặc thậm chí là công dân của chính quốc gia đó mà chính phủ coi là thù địch hoặc đe dọa. Một số lượng ngày càng tăng các cuộc tấn công ngày nay từ các kẻ tấn công được nhà nước bảo trợ được hướng tới các doanh nghiệp ở các nước ngoài với mục tiêu gây tổn hại tài chính hoặc làm tổn hại đến danh tiếng của tổ chức.

LƯU Ý

Nhiều nhà nghiên cứu bảo mật tin rằng những kẻ tấn công được nhà nước bảo trợ có thể là những kẻ tấn công nguy hiểm nhất. Đó là bởi vì những kẻ tấn công được nhà nước bảo trợ có kỹ năng cao và có đủ nguồn lực của chính phủ để vượt qua hầu hết mọi biện pháp phòng thủ an ninh. Khi một kẻ tấn công có động cơ tài chính, như tội phạm mạng, thấy rằng hệ thống phòng thủ của mục tiêu quá mạnh, kẻ tấn công chỉ đơn giản chuyển sang một mục tiêu hứa hẹn khác với hệ thống phòng thủ kém hiệu quả hơn. Với những kẻ tấn công được nhà nước bảo trợ, mục tiêu rất cụ thể và những kẻ tấn công tiếp tục làm việc cho đến khi họ thành công, thể hiện cả nguồn lực sâu rộng và sự kiên trì.

Bảng 1-3 liệt kê một số đặc điểm của các loại kẻ tấn công khác nhau này.

Bảng 1-3 Đặc điểm của các kẻ tấn công

Loại kẻ tấn công	Mục tiêu	Mục tiêu điển hình	Cuộc tấn công mẫu
Cybercriminals (Tội phạm mạng)	Tài sản hơn danh tiếng	Người dùng, doanh nghiệp, chính phủ	Đánh cắp thông tin thẻ tín dụng
Script kiddies	Cảm giác mạnh, tai tiếng	Doanh nghiệp, người dùng	Xóa dữ liệu
Brokers (Nhà môi giới)	Bán lỗ hổng cho người trả giá cao nhất	Bất kỳ ai	Tìm lỗ hổng trong hệ điều hành
Insiders (Người nội	Trả thù chủ lao	Chính phủ, doanh	Đánh cắp tài liệu để

bộ)	động, làm xấu mặt chính phủ	nghiệp	công bố thông tin nhạy cảm
Cyberterrorists (Khủng bố mạng)	Gây gián đoạn và hoảng loạn	Doanh nghiệp	Vô hiệu hóa máy tính kiểm soát xử lý nước
Hactivists	Sửa chữa một sai lầm nhận thức chống lại họ	Chính phủ, doanh nghiệp	Phá hoại trang web tài chính

3. Khó khăn trong việc phòng thủ chống lại các cuộc tấn công

Thách thức trong việc giữ an toàn cho máy tính chưa bao giờ lớn hơn, không chỉ vì số lượng các cuộc tấn công mà còn vì những khó khăn gặp phải trong việc phòng thủ chống lại chúng. Những khó khăn này bao gồm:

- **Các thiết bị kết nối toàn cầu.** Ngày nay, không thể tưởng tượng được bất kỳ thiết bị công nghệ nào—máy tính để bàn, máy tính bảng, máy tính xách tay hoặc điện thoại thông minh—lại không được kết nối với Internet. Mặc dù điều này mang lại những lợi ích to lớn, nó cũng khiến cho một kẻ tấn công ở nửa vòng trái đất có thể âm thầm khởi động một cuộc tấn công chống lại một thiết bị được kết nối.
- **Tốc độ tấn công tăng lên.** Với công nghệ hiện đại, những kẻ tấn công có thể nhanh chóng quét hàng triệu thiết bị để tìm điểm yếu và khởi động các cuộc tấn công với tốc độ chưa từng thấy. Các công cụ tấn công ngày nay khởi tạo các cuộc tấn công mới mà không cần sự tham gia của con người, do đó làm tăng tốc độ tấn công các hệ thống.
- **Sự tinh vi ngày càng cao của các cuộc tấn công.** Các cuộc tấn công ngày càng trở nên phức tạp, khiến việc phát hiện và phòng thủ chống lại chúng trở nên khó khăn hơn. Những kẻ tấn công ngày nay sử dụng các giao thức và ứng dụng Internet phổ biến để thực hiện các cuộc tấn công, gây khó khăn cho việc phân biệt một cuộc tấn công với lưu lượng mạng hợp pháp. Các công cụ tấn công khác thay đổi hành vi của chúng để cùng một cuộc tấn công xuất hiện khác nhau mỗi lần, làm phức tạp thêm việc phát hiện.

- **Sự sẵn có và đơn giản của các công cụ tấn công.** Trong khi trước đây một kẻ tấn công cần có kiến thức kỹ thuật sâu rộng về mạng và máy tính cũng như khả năng viết một phần trình để tạo ra cuộc tấn công, thì ngày nay điều đó không còn đúng nữa. Các công cụ tấn công phần mềm ngày nay không đòi hỏi bất kỳ kiến thức phức tạp nào từ phía kẻ tấn công. Thực tế, nhiều công cụ, như giao diện Kali Linux được hiển thị trong Hình 1-1, có giao diện người dùng đồ họa (GUI) cho phép người dùng dễ dàng chọn các tùy chọn từ một menu. Những công cụ này có sẵn miễn phí hoặc có thể được mua từ những kẻ tấn công khác với chi phí thấp đến đáng ngạc nhiên.
- **Phát hiện lỗ hổng nhanh hơn.** Điểm yếu trong phần cứng và phần mềm có thể được phát hiện và khai thác nhanh hơn với các công cụ và kỹ thuật phần mềm mới.
- **Chậm trễ trong việc cập nhật bảo mật.** Các nhà cung cấp phần cứng và phần mềm đang quá tải khi cố gắng theo kịp việc cập nhật sản phẩm của họ để chống lại các cuộc tấn công. Một viện bảo mật phần mềm diệt virus nhận được hơn 390.000 đệ trình về phần mềm độc hại tiềm năng mỗi ngày.[15] Với tốc độ này, các nhà cung cấp phần mềm diệt virus sẽ phải tạo và phân phối các bản cập nhật mỗi vài giây để giữ cho người dùng được bảo vệ hoàn toàn. Sự chậm trễ này trong việc phân phối các bản cập nhật bảo mật làm tăng thêm khó khăn trong việc phòng thủ chống lại các cuộc tấn công.
- **Phân phối cập nhật bảo mật yếu kém.** Trong khi các nhà cung cấp sản phẩm chính thống, như Microsoft, Apple và Adobe, có một hệ thống để thông báo cho người dùng về các bản cập nhật bảo mật cho nhiều sản phẩm của họ và phân phối chúng một cách thường xuyên, thì rất ít nhà cung cấp phần mềm khác đã đầu tư vào các hệ thống phân phối tốn kém này. Người dùng thường không biết rằng có một bản cập nhật bảo mật tồn tại cho một sản phẩm vì không có phương tiện đáng tin cậy nào để nhà cung cấp cảnh báo người dùng. Ngoài ra, những nhà cung cấp này thường không tạo ra các bản cập nhật bảo mật nhỏ để "vá" phần mềm hiện có, mà thay vào đó họ sửa lỗi trong một phiên bản hoàn toàn mới của phần mềm—và sau đó yêu cầu người dùng trả tiền cho phiên bản cập nhật có chứa bản vá.

Hình 1-2 Menu của các công cụ tấn công *(Nguồn: Kali Linux)*

LƯU Ý

Các nhà cung cấp hệ điều hành điện thoại thông minh đặc biệt nổi tiếng vì không cung cấp các bản cập nhật bảo mật một cách kịp thời, nếu có. Hầu hết các nhà cung cấp và nhà mạng không dây không cố gắng cung cấp cho người dùng các bản cập nhật quan trọng (chẳng hạn như từ phiên bản 5.6 lên 5.7), thay vào đó hy vọng rằng người dùng sẽ mua một chiếc điện thoại thông minh hoàn toàn mới—và hợp đồng dịch vụ—để có thiết bị mới nhất và an toàn nhất.

- **Các cuộc tấn công phân tán.** Những kẻ tấn công có thể sử dụng hàng trăm ngàn máy tính dưới sự kiểm soát của chúng trong một cuộc tấn công chống lại một máy chủ hoặc mạng duy nhất. Cách tiếp cận "nhiều đánh một" này làm cho việc ngăn chặn một cuộc tấn công bằng cách xác định và chặn một nguồn duy nhất trở nên gần như không thể.

- **Sự bối rối của người dùng.** Người dùng ngày càng được yêu cầu đưa ra các quyết định bảo mật khó khăn liên quan đến hệ thống máy tính của họ, đôi khi với rất ít hoặc không có thông tin để hướng dẫn họ. Không có gì lạ khi một người dùng được hỏi các câu hỏi bảo mật như *Bạn có muốn chỉ xem nội dung được gửi một cách an toàn không?* hoặc *Có an toàn để cách ly tệp đính kèm này không?* hoặc *Bạn có muốn cài đặt tiện ích mở rộng này không?* Với ít hoặc không có sự hướng dẫn, người

dùng có xu hướng cung cấp câu trả lời cho các câu hỏi mà không hiểu rõ các rủi ro bảo mật. Ngoài ra, thông tin phổ biến được lưu hành về bảo mật thông qua các hãng tin tiêu dùng hoặc các trang web thường không chính xác hoặc gây hiểu lầm, dẫn đến sự bối rối của người dùng càng nhiều hơn.

Bảng 1-4 tóm tắt các lý do tại sao khó có thể phòng thủ trước các cuộc tấn công ngày nay.

Bảng 1-4 Những khó khăn trong việc phòng thủ chống lại các cuộc tấn công

Lý do	Mô tả
Thiết bị kết nối toàn cầu	Kẻ tấn công từ bất kỳ đâu trên thế giới đều có thể tấn công.
Tốc độ tấn công gia tăng	Kẻ tấn công có thể khởi động các cuộc tấn công chống lại hàng triệu máy tính trong vòng vài phút.
Sự tinh vi ngày càng cao của các cuộc tấn công	Các công cụ tấn công thay đổi hành vi của chúng để cùng một cuộc tấn công xuất hiện khác nhau mỗi lần.
Sự sẵn có và đơn giản của các công cụ tấn công	Các cuộc tấn công không còn bị giới hạn ở những kẻ tấn công có kỹ năng cao.
Phát hiện lỗ hổng nhanh hơn	Kẻ tấn công có thể phát hiện các lỗ hổng bảo mật trong phần cứng hoặc phần mềm nhanh hơn.
Chậm trễ trong việc cập nhật bảo mật	Các nhà cung cấp đang quá tải khi cố gắng theo kịp việc cập nhật sản phẩm của họ để chống lại các cuộc tấn công mới nhất.
Phân phối cập nhật bảo mật yếu	Nhiều sản phẩm phần mềm thiếu phương tiện để phân phối các bản cập nhật bảo mật một cách kịp thời.
Tấn công phân tán	Kẻ tấn công sử dụng hàng ngàn máy tính trong một cuộc tấn công chống lại một máy tính hoặc mạng duy nhất.
Sự bối rối của người dùng	Người dùng được yêu cầu đưa ra các quyết định bảo mật khó khăn với ít hoặc không có sự hướng dẫn.

PHẦN II: AN NINH MẠNG VÀ TẦM QUAN TRỌNG CỦA AN NINH MẠNG

1. Khái niệm về an ninh mạng.

Định nghĩa An ninh Thông tin

Thuật ngữ *an ninh thông tin* thường được sử dụng để mô tả các nhiệm vụ bảo mật thông tin ở định dạng kỹ thuật số. Thông tin kỹ thuật số này được xử lý bởi một bộ vi xử lý (chẳng hạn như trên một máy tính cá nhân), được lưu trữ trên một thiết bị lưu trữ (như ổ cứng hoặc ổ flash USB), và được truyền qua một mạng (chẳng hạn như mạng cục bộ hoặc Internet).

Cũng giống như an ninh có thể được xem như cả một mục tiêu và một quá trình, điều tương tự cũng đúng với an ninh thông tin. An ninh thông tin có thể được hiểu rõ nhất bằng cách xem xét các mục tiêu của nó và quá trình thực hiện nó. Cùng với nhau, những điều này có thể giúp tạo ra một định nghĩa vững chắc về an ninh thông tin.

An ninh thông tin không thể ngăn chặn hoàn toàn các cuộc tấn công thành công hoặc đảm bảo rằng một hệ thống hoàn toàn an toàn, cũng như các biện pháp an ninh được thực hiện cho một ngôi nhà không bao giờ có thể đảm bảo an toàn tuyệt đối khỏi một tên trộm hoặc một cơn bão. Mục đích của an ninh thông tin là để đảm bảo rằng các biện pháp bảo vệ được triển khai đúng cách để chống lại các cuộc tấn công và cung cấp sự bảo vệ ở mức độ cao nhất có thể. Nó cũng nên ngăn chặn sự sụp đổ hoàn toàn của hệ thống khi một cuộc tấn công thành công xảy ra. Do đó, an ninh thông tin trước hết là *sự bảo vệ*.

LƯU Ý

An ninh thông tin không nên được xem như một cuộc chiến thắng hay bại. Cũng như tội phạm như trộm cắp không bao giờ có thể bị loại bỏ hoàn toàn, các cuộc tấn công vào các thiết bị công nghệ cũng vậy. Mục tiêu không phải là một chiến thắng hoàn toàn mà là duy trì sự cân bằng: khi những kẻ tấn công lợi dụng một điểm yếu trong hàng phòng thủ, những người phòng thủ phải đáp lại bằng một hàng phòng thủ được cải tiến. An ninh thông tin là một chu kỳ vô tận giữa kẻ tấn công và người phòng thủ.

Thứ hai, an ninh thông tin nhằm *bảo vệ thông tin mang lại giá trị* cho con người và các tổ chức. Có ba sự bảo vệ phải được mở rộng trên thông tin: tính bí mật, tính toàn vẹn và tính sẵn sàng, đôi khi được gọi là bộ ba CIA:

1. **Tính bí mật (Confidentiality).** Điều quan trọng là chỉ những cá nhân được chấp thuận mới có thể truy cập thông tin quan trọng. Ví dụ, số thẻ tín dụng được sử dụng để mua hàng trực tuyến phải được giữ an toàn và không được cung cấp cho các bên khác. Tính bí mật đảm bảo rằng chỉ những bên được ủy quyền mới có thể xem thông tin. Việc cung cấp tính bí mật có thể liên quan đến một số công cụ bảo mật khác nhau, từ phần mềm để "xáo trộn" số thẻ tín dụng được lưu trữ trên máy chủ web đến khóa cửa để ngăn chặn truy cập vào các máy chủ đó.

2. **Tính toàn vẹn (Integrity).** Tính toàn vẹn đảm bảo rằng thông tin là chính xác và không có người không được ủy quyền hoặc phần mềm độc hại nào đã thay đổi dữ liệu. Trong ví dụ về việc mua hàng trực tuyến, một kẻ tấn công có thể thay đổi số tiền của một giao dịch mua từ $10.000,00 xuống còn $1,00 sẽ vi phạm tính toàn vẹn của thông tin.

3. **Tính sẵn sàng (Availability).** Thông tin có giá trị nếu các bên được ủy quyền, những người được đảm bảo về tính toàn vẹn của nó, có thể truy cập thông tin. Tính sẵn sàng đảm bảo rằng dữ liệu có thể truy cập được bởi người dùng được ủy quyền (và thông tin không bị "khóa chặt" đến mức họ không thể truy cập được). Điều đó cũng có nghĩa là những kẻ tấn công đã không thực hiện một cuộc tấn công để dữ liệu không thể truy cập được. Trong ví dụ này, tổng số các mặt hàng được đặt hàng do một giao dịch mua trực tuyến phải được cung cấp cho một nhân viên trong kho để các mặt hàng chính xác có thể được vận chuyển cho khách hàng.

Ngoài bộ ba CIA, một bộ bảo vệ khác phải được triển khai để bảo mật thông tin. Đó là xác thực, ủy quyền và ghi nhận—hay AAA:

1. **Xác thực (Authentication).** Xác thực đảm bảo rằng cá nhân đó chính là người mà cô ấy tự nhận (người thật hoặc chính danh) và không phải là kẻ mạo danh. Một người truy cập máy chủ web chứa số thẻ tín dụng của người dùng phải chứng minh rằng cô ấy thực sự là người mà cô ấy tự nhận và không phải là một kẻ tấn công gian lận. Một cách để thực hiện xác thực là người đó cung cấp một mật khẩu mà chỉ cô ấy biết.

2. **Ủy quyền (Authorization).** Ủy quyền là việc cấp phép hoặc chấp thuận cho các tài nguyên công nghệ cụ thể. Sau khi một người đã cung cấp xác thực, cô ấy có thể có quyền truy cập số thẻ tín dụng hoặc vào một phòng chứa máy chủ web, miễn là cô ấy đã được cấp phép trước đó.

3. **Ghi nhận (Accounting).** Ghi nhận cung cấp việc theo dõi ("dấu vết kiểm toán") các sự kiện. Điều này có thể bao gồm một bản ghi về người đã truy cập máy chủ web, từ vị trí nào và vào thời điểm cụ thể nào.

Vậy thông tin được bảo vệ như thế nào? Bởi vì thông tin này được lưu trữ trên phần cứng máy tính, được xử lý bởi phần mềm và được truyền qua các phương tiện truyền thông, mỗi lĩnh vực này phải được che chở. Mục tiêu thứ ba của an ninh thông tin là *bảo vệ tính toàn vẹn*, tính bí mật và tính sẵn sàng của thông tin trên các thiết bị lưu trữ, xử lý và truyền tải thông tin.

An ninh thông tin được thực hiện thông qua một quy trình là sự kết hợp của ba thực thể. Như được thể hiện trong Hình 1-1 và Bảng 1-1, thông tin và phần cứng, phần mềm, và truyền thông được bảo vệ trong ba lớp: sản phẩm, con người, và chính sách và quy trình. Ba lớp này tương tác với nhau: quy trình cho phép con người hiểu cách sử dụng sản phẩm để bảo vệ thông tin.

Hình 1-1 Các lớp an ninh thông tin

(Sơ đồ các vòng tròn đồng tâm. Lõi trong cùng là "Thông tin" với các thuộc tính "Bí mật", "Toàn vẹn", "Sẵn sàng". Thông tin này được "Xử lý", "Lưu trữ" và "Truyền đi". Các lớp bảo vệ bên ngoài lần lượt là "Sản phẩm", "Con người", và "Chính sách và quy trình".)

Bảng 1-1 Các lớp an ninh thông tin

Lớp	Mô tả
Sản phẩm	Hình thành lớp an ninh xung quanh dữ liệu. Có thể đơn giản như khóa cửa hoặc phức tạp như thiết bị an ninh mạng.
Con người	Những người triển khai và sử dụng đúng các sản phẩm bảo mật để bảo vệ dữ liệu.
Chính sách và quy trình	Các kế hoạch và chính sách được một tổ chức thiết lập để đảm bảo mọi người sử dụng đúng các sản phẩm.

Một định nghĩa toàn diện về an ninh thông tin bao gồm cả mục tiêu và quy trình. An ninh thông tin có thể được định nghĩa là *thứ bảo vệ tính toàn vẹn, tính bí mật*

và tính sẵn sàng của thông tin trên các thiết bị lưu trữ, xử lý và truyền tải thông tin thông qua các sản phẩm, con người và quy trình.

Thuật ngữ An ninh Thông tin

Cũng như nhiều môn học nâng cao khác, an ninh thông tin có bộ thuật ngữ riêng. Kịch bản sau đây giúp minh họa các thuật ngữ an ninh thông tin và cách chúng được sử dụng.

Giả sử Ellie muốn mua một chiếc xe tay ga Ý mới để đi từ căn hộ của mình đến trường và nơi làm việc. Tuy nhiên, vì một số chiếc xe tay ga đã bị đánh cắp gần căn hộ của cô, cô lo lắng về việc bảo vệ nó. Mặc dù cô đỗ xe tay ga trong bãi đậu xe có cổng ở phía trước căn hộ của mình, nhưng một lỗ hổng trên hàng rào xung quanh khu chung cư khiến người khác có thể vào bãi đậu xe mà không bị hạn chế. Chiếc xe tay ga của Ellie và mối đe dọa đối với nó được minh họa trong Hình 1-2.

Hình 1-2 Phép loại suy về các thành phần an ninh thông tin

(Hình ảnh mô tả: Một chiếc xe tay ga (tài sản - asset). Một tên trộm (tác nhân đe dọa - threat agent) đang đi qua một lỗ hổng trên hàng rào (lỗ hổng - vulnerability). Hành động đi qua lỗ hổng là "khai thác" (exploit). Mối đe dọa (threat) là "mất xe tay ga". Rủi ro (risk) là "xe tay ga bị đánh cắp".)

Chiếc xe tay ga mới của Ellie là một **tài sản (asset)**, được định nghĩa là một vật có giá trị. Điều mà Ellie đang cố gắng bảo vệ chiếc xe tay ga của mình khỏi là một **mối đe dọa (threat)**, là một loại hành động có khả năng gây hại. Các mối đe dọa an ninh thông tin là các sự kiện hoặc hành động đại diện cho một mối nguy hiểm đối với tài sản thông tin. Một mối đe dọa tự nó không có nghĩa là an ninh đã bị xâm phạm; đúng hơn, nó chỉ đơn giản có nghĩa là tiềm năng gây ra tổn thất là có thật.

Một **tác nhân đe dọa (threat agent)** là một người hoặc yếu tố có sức mạnh để thực hiện một mối đe dọa. Đối với Ellie, tác nhân đe dọa là một tên trộm. Trong an ninh thông tin, một tác nhân đe dọa có thể là một người cố gắng đột nhập vào một mạng máy tính an toàn. Nó cũng có thể là một thế lực tự nhiên như một cơn bão có thể

phá hủy thiết bị máy tính và do đó phá hủy thông tin, hoặc nó có thể là phần mềm độc hại tấn công mạng máy tính.

Ellie muốn bảo vệ chiếc xe tay ga của mình và lo lắng về một lỗ hổng trên hàng rào quanh căn hộ của cô. Lỗ hổng trên hàng rào là một **vulnerability (lỗ hổng)**, tức là một sai sót hoặc điểm yếu cho phép một tác nhân đe dọa vượt qua hàng rào an ninh. Một ví dụ về lỗ hổng mà an ninh thông tin phải đối phó là một lỗi phần mềm trong hệ điều hành cho phép người dùng không được ủy quyền giành quyền kiểm soát một máy tính mà không có sự cho phép hay hiểu biết của người dùng.

Nếu một tên trộm có thể đến được chiếc xe tay ga của Ellie vì có lỗ hổng trên hàng rào, thì tên trộm đó đang lợi dụng lỗ hổng đó. Điều này được gọi là **exploiting the vulnerability (khai thác lỗ hổng)** thông qua một **threat vector (vector đe dọa)**, hay phương tiện mà một cuộc tấn công có thể xảy ra. Một kẻ tấn công, biết rằng một lỗi trong hệ điều hành của máy chủ web chưa được vá, có thể sử dụng một vector đe dọa (khai thác lỗ hổng) để đánh cắp mật khẩu người dùng.

Ellie phải đưa ra quyết định: xác suất (**threat likelihood - khả năng xảy ra mối đe dọa**) mà mối đe dọa sẽ thành hiện thực và chiếc xe tay ga của cô bị đánh cắp là bao nhiêu? Điều này có thể được hiểu theo thuật ngữ **risk (rủi ro)**. Rủi ro là một tình huống liên quan đến việc tiếp xúc với một số loại nguy hiểm. Có nhiều lựa chọn khác nhau mà Ellie có thể thực hiện liên quan đến rủi ro chiếc xe tay ga của mình bị đánh cắp. Ellie có thể quyết định dựa trên rủi ro bị đánh cắp xe mà cô sẽ không mua chiếc xe tay ga mới (**risk avoidance - tránh rủi ro**). Hoặc cô có thể chấp nhận rủi ro và mua chiếc xe tay ga mới, biết rằng có khả năng nó sẽ bị một tên trộm đi qua lỗ hổng trên hàng rào đánh cắp (**risk acceptance - chấp nhận rủi ro**). Cô có thể phàn nàn với người quản lý căn hộ về lỗ hổng trên hàng rào để nó được sửa chữa và làm cho rủi ro trở nên ít nghiêm trọng hơn (**risk mitigation - giảm thiểu rủi ro**) hoặc yêu cầu người quản lý treo biển báo có nội dung "Người xâm nhập sẽ bị trừng phạt theo quy định của pháp luật" (**risk deterrence - răn đe rủi ro**). Điều mà Ellie rất có thể sẽ làm là mua bảo hiểm để công ty bảo hiểm sẽ gánh chịu tổn thất và trả tiền cho cô nếu chiếc xe tay ga bị đánh cắp, về cơ bản là làm cho người khác chịu trách nhiệm (**risk transference - chuyển giao rủi ro**).

Bảng 1-2 tóm tắt các thuật ngữ an ninh thông tin này.

Bảng 1-2 Thuật ngữ an ninh thông tin

Thuật ngữ	Ví dụ trong kịch bản của Ellie	Ví dụ trong an ninh thông tin
Asset (Tài sản)	Xe tay ga	Cơ sở dữ liệu nhân viên
Threat (Mối đe dọa)	Đánh cắp xe tay ga	Đánh cắp dữ liệu
Threat agent (Tác nhân đe dọa)	Tên trộm	Kẻ tấn công, cơn bão
Vulnerability (Lỗ hổng)	Lỗ hổng trên hàng rào	Lỗi phần mềm
Threat vector (Vector đe dọa)	Trèo qua lỗ hổng trên hàng rào	Truy cập mật khẩu máy chủ web qua lỗi phần mềm
Threat likelihood (Khả năng xảy ra mối đe dọa)	Xác suất xe tay ga bị đánh cắp	Khả năng nhiễm virus
Risk (Rủi ro)	Không mua xe tay ga	Không cài đặt mạng không dây

2. Tầm quan trọng của An ninh mạng

An ninh thông tin quan trọng đối với cá nhân cũng như các tổ chức. Đó là bởi vì an ninh thông tin có thể hữu ích trong việc ngăn chặn hành vi trộm cắp dữ liệu, ngăn chặn hành vi trộm cắp danh tính, tránh các hậu quả pháp lý của việc không bảo mật thông tin, duy trì năng suất và chống lại khủng bố mạng.

Ngăn chặn trộm cắp dữ liệu An ninh thường gắn liền nhất với việc ngăn chặn trộm cắp: Ellie có thể đỗ chiếc xe tay ga của mình trong một gara có khóa để ngăn nó bị đánh cắp. Điều tương tự cũng đúng với an ninh thông tin: ngăn chặn việc dữ liệu bị đánh cắp thường được coi là mục tiêu chính của an ninh thông tin. Đối với một doanh nghiệp, việc bảo vệ chống lại trộm cắp dữ liệu là cần thiết. Những kẻ tấn công rất háo hức đánh cắp thông tin kinh doanh độc quyền, chẳng hạn như nghiên cứu cho một sản phẩm mới hoặc danh sách khách hàng.

Cá nhân cũng thường là mục tiêu của hành vi trộm cắp dữ liệu. Một loại dữ liệu cá nhân là mục tiêu hàng đầu của những kẻ tấn công là số thẻ thanh toán, chẳng hạn như thẻ ghi nợ, thẻ tín dụng và thẻ quà tặng. Những con số bị đánh cắp này có thể được bán trên thị trường chợ đen để mua hàng ngàn đô la hàng hóa trực tuyến—mà

không cần có thẻ thực tế—trước khi nạn nhân hoặc ngân hàng nhận ra rằng số thẻ đã bị đánh cắp. Một số kỹ thuật phổ biến được bọn trộm thẻ thanh toán sử dụng bao gồm:

- Bọn trộm xác định xem một số thẻ bị đánh cắp có còn hoạt động hay không bằng cách thực hiện một giao dịch mua nhỏ, điều này khó có thể gây sự chú ý của người dùng hoặc ngân hàng phát hành thẻ.
- Một số người bán trên thị trường chợ đen sẽ cung cấp bảo đảm rằng các số thẻ bị đánh cắp sẽ vẫn hoạt động trong một khoảng thời gian cụ thể hoặc cho việc mua một lượng hàng hóa tối thiểu trước khi số thẻ bị thu hồi.
- Những người bán hàng trên thị trường chợ đen thường sẽ giám sát cách khách hàng của họ sử dụng các thẻ bị đánh cắp để đảm bảo họ không gây quá nhiều sự chú ý và do đó có nguy cơ bị phát hiện, điều này sẽ ngăn cản các khách hàng khác đã mua các thẻ tương tự có thể thực hiện giao dịch mua.
- Các số thẻ bị đánh cắp mà cũng bao gồm thông tin cá nhân như ngày sinh và số An sinh Xã hội của chủ thẻ có giá trị hơn chỉ số thẻ. Đó là bởi vì bọn trộm có thể sử dụng thông tin này để khám phá các thông tin cá nhân khác về nạn nhân và do đó có vị thế tốt hơn để trả lời các câu hỏi thách thức bảo mật có thể được ngân hàng hỏi nếu một giao dịch mua lớn được thực hiện.

Ngăn chặn trộm cắp danh tính Trộm cắp danh tính liên quan đến việc đánh cắp thông tin cá nhân của người khác, chẳng hạn như số An sinh Xã hội, và sau đó sử dụng thông tin đó để mạo danh nạn nhân, thường là để trục lợi tài chính. Bọn trộm thường tạo ra các tài khoản ngân hàng hoặc thẻ tín dụng mới dưới tên của nạn nhân và sau đó các giao dịch mua lớn được tính vào các tài khoản này, khiến nạn nhân phải chịu trách nhiệm về các khoản nợ và làm hỏng xếp hạng tín dụng của họ.

LƯU Ý

Trong một số trường hợp, bọn trộm đã mua ô tô và thậm chí cả nhà cửa bằng cách vay tiền dưới tên của người khác.

Một lĩnh vực phát triển nhanh chóng của hành vi trộm cắp danh tính liên quan đến việc những kẻ trộm danh tính nộp các tờ khai thuế thu nhập giả mạo cho Sở Thuế vụ Hoa Kỳ (IRS) để nhận được tiền hoàn thuế của nạn nhân. Theo IRS, mỗi năm có hơn 6 tỷ đô la séc hoàn thuế được gửi đến những kẻ trộm danh tính đã nộp tờ khai thuế gian lận. Tuy nhiên, việc thực thi pháp luật vẫn còn là một vấn đề.[16]

Duy trì năng suất Việc dọn dẹp sau một cuộc tấn công làm lãng phí thời gian, tiền bạc và các nguồn lực khác khỏi các hoạt động bình thường. Những người dùng là nạn nhân của một cuộc tấn công thành công có thể phải mất nhiều ngày để khôi phục máy tính của họ về trạng thái trước khi bị tấn công, hoặc họ có thể phải trả tiền cho một chuyên gia công nghệ để hoàn thành công việc. Trong thời gian này, máy tính không khả dụng và năng suất cá nhân bị ảnh hưởng.

Nhân viên của một tổ chức cũng bị ảnh hưởng tương tự do một cuộc tấn công làm cho thiết bị của họ trở nên vô dụng. Những người lao động này không thể làm việc hiệu quả và hoàn thành các nhiệm vụ quan trọng trong hoặc sau một cuộc tấn công vì máy tính và mạng không thể hoạt động bình thường. Bảng 1-3 cung cấp một ước tính mẫu về tiền lương bị mất và năng suất bị mất trong một cuộc tấn công và việc dọn dẹp sau đó.

Bảng 1-3 Tổn thất do các cuộc tấn công

Số lượng nhân viên	Lương trung bình mỗi giờ	Số lượng nhân viên để chống lại cuộc tấn công	Số giờ cần thiết để ngăn chặn cuộc tấn công và dọn dẹp	Tổng lương bị mất	Tổng số giờ năng suất bị mất
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1,000	$30	10	96	$220,000	1293

Chống khủng bố mạng FBI định nghĩa khủng bố mạng là bất kỳ "cuộc tấn công có chủ ý, mang động cơ chính trị chống lại thông tin, hệ thống máy tính, chương trình máy tính và dữ liệu gây ra bạo lực chống lại các mục tiêu phi chiến đấu bởi các nhóm dưới quốc gia hoặc các tác nhân bí mật."[18] Không giống như một cuộc tấn công được thiết kế để đánh cắp thông tin hoặc xóa ổ cứng của người dùng, các cuộc tấn công khủng bố mạng nhằm mục đích gây hoảng loạn hoặc kích động bạo lực trong dân chúng. Các cuộc tấn công được nhắm vào các mục tiêu như ngành ngân hàng, các cơ sở quân sự, nhà máy điện, trung tâm kiểm soát không lưu và hệ thống cấp nước. Đây

là những mục tiêu đáng mong muốn vì chúng có thể làm gián đoạn đáng kể các hoạt động bình thường của một bộ phận dân cư lớn. Ví dụ,

việc vô hiệu hóa một nhà máy điện có thể làm tê liệt các doanh nghiệp, nhà cửa, dịch vụ vận tải và thông tin liên lạc trên một khu vực rộng lớn. Tuy nhiên, một trong những thách thức trong việc chống khủng bố mạng là nhiều mục tiêu chính không thuộc sở hữu và quản lý của chính phủ liên bang. Vì chúng không được kiểm soát tập trung, nên rất khó để phối hợp và duy trì an ninh.

LƯU Ý

Bộ An ninh Nội địa Mỹ đã xác định 7.200 hệ thống kiểm soát công nghiệp quan trọng là một phần của cơ sở hạ tầng trọng yếu và được kết nối trực tiếp với Internet, khiến chúng dễ bị tấn công khủng bố mạng. Trong một năm, số vụ tấn công đã tăng 52%, dẫn đến 198 cuộc tấn công trực tiếp vào các hệ thống này, gây ra một số vụ đột nhập thành công.[19]

3. Các biện pháp bảo vệ cần thiết

Mặc dù số lượng các cuộc tấn công nhằm vào an ninh cá nhân của người dùng ngày càng tăng, có những biện pháp phòng thủ có thể được sử dụng để chống lại các cuộc tấn công này. Các biện pháp phòng thủ này bao gồm việc sử dụng mật khẩu mạnh, nhận diện các cuộc tấn công lừa đảo, thực hiện các bước để tránh trộm cắp danh tính và bảo mật các trang mạng xã hội.

Các Biện Pháp Phòng Thủ Mật Khẩu

Cách tiếp cận tốt nhất để thiết lập bảo mật mạnh mẽ với mật khẩu là sử dụng công nghệ để quản lý mật khẩu. Nếu không sử dụng các công cụ này, thì các kỹ thuật để tạo và ghi nhớ mật khẩu mạnh phải được thực hiện.

Sử dụng Công Cụ Quản Lý Mật Khẩu

Ngoài các đặc điểm đã được liệt kê trước đó về mật khẩu yếu (chẳng hạn như sử dụng từ điển thông thường, tạo mật khẩu ngắn hoặc sử dụng thông tin cá nhân trong mật khẩu), còn có hai đặc điểm bổ sung của mật khẩu yếu:

- Bất kỳ mật khẩu nào có thể **ghi nhớ** được đều là mật khẩu yếu.
- Bất kỳ mật khẩu nào **được lặp lại** trên nhiều tài khoản đều là mật khẩu yếu.

Do những hạn chế của trí nhớ con người và tốc độ xử lý nhanh của máy tính ngày nay được kẻ tấn công sử dụng, người dùng bình thường không thể ghi nhớ nhiều

mật khẩu dài có thể chống lại các cuộc tấn công. Thay vì dựa vào trí nhớ con người cho mật khẩu, các chuyên gia bảo mật ngày nay khuyến nghị sử dụng công nghệ để lưu trữ và quản lý mật khẩu. Các công nghệ được sử dụng để bảo mật mật khẩu được gọi là **password managers** (trình quản lý mật khẩu). Có ba loại trình quản lý mật khẩu cơ bản:

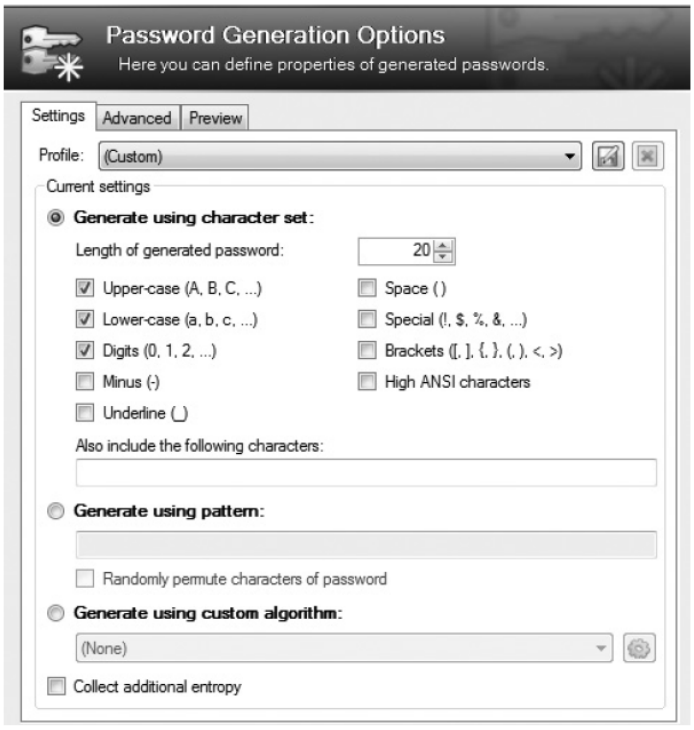
- **Password generators** (trình tạo mật khẩu). Đây là các tiện ích mở rộng của trình duyệt web tạo mật khẩu. Người dùng nhập một mật khẩu chính và trình tạo mật khẩu sẽ tạo ra một mật khẩu dựa trên mật khẩu chính và URL của trang web "tức thì." Nhược điểm của trình tạo mật khẩu là tiện ích mở rộng trình duyệt phải được cài đặt trên mỗi máy tính và trình duyệt web.
- **Online vaults** (hầm trực tuyến). Một hầm trực tuyến cũng sử dụng tiện ích mở rộng trình duyệt web nhưng thay vì tạo mật khẩu của người dùng mỗi lần, nó truy xuất mật khẩu từ một kho lưu trữ trung tâm trực tuyến. Nhược điểm là các trang web trực tuyến lưu trữ mật khẩu này dễ bị kẻ tấn công tấn công.
- **Password management applications** (ứng dụng quản lý mật khẩu). Một ứng dụng quản lý mật khẩu là một chương trình được cài đặt trên máy tính mà qua đó người dùng có thể tạo và lưu trữ nhiều mật khẩu mạnh trong một tệp "hầm" duy nhất được bảo vệ bởi một mật khẩu chính mạnh. Người dùng có thể truy xuất các mật khẩu riêng lẻ khi cần bằng cách mở tệp của người dùng, do đó giải phóng người dùng khỏi nhu cầu ghi nhớ nhiều mật khẩu. Nhược điểm là chương trình phải được mang theo người dùng hoặc cài đặt trên nhiều máy tính.

LƯU Ý

Hầu hết các trình duyệt web cho phép người dùng lưu mật khẩu đã nhập khi sử dụng trình duyệt. Tuy nhiên, tính năng này có một số nhược điểm. Người dùng chỉ có thể truy xuất mật khẩu trên máy tính nơi chúng được lưu trữ (trừ khi thông tin trình duyệt được đồng bộ hóa với các máy tính khác). Ngoài ra, mật khẩu có thể dễ bị tấn công nếu người dùng khác được phép truy cập vào máy tính của họ. Thêm vào đó, các ứng dụng có sẵn miễn phí cho phép hiển thị tất cả mật khẩu mà không cần nhập mật khẩu chính.

Hầu hết các chuyên gia bảo mật đều khuyến nghị sử dụng ứng dụng quản lý mật khẩu vì nó cung cấp mức độ bảo mật cao nhất. Các ứng dụng này cũng bao gồm các tính năng bổ sung sau:

- **Bảo vệ bộ nhớ trong (In-memory protection)**. Mật khẩu được "xáo trộn" khi ứng dụng đang chạy, để ngay cả khi hệ điều hành thực hiện các chức năng, nó sẽ không tiết lộ bất kỳ mật khẩu nào.
- **Tệp khóa (Key files)**. Một tệp khóa là một tệp riêng biệt, duy nhất có thể được mang trên USB flash drive hoặc thiết bị tương tự khác. Để mở cơ sở dữ liệu mật khẩu, không chỉ phải nhập mật khẩu, mà tệp khóa cũng phải có mặt. Điều này ngăn kẻ tấn công lấy được mật khẩu cơ sở dữ liệu sử dụng nó.
- **Khóa vào tài khoản người dùng (Lock to user account)**. Cơ sở dữ liệu có thể được khóa để nó chỉ có thể được mở bởi cùng một người đã tạo ra nó.
- **Nhập và xuất (Import and export)**. Danh sách mật khẩu có thể được xuất sang nhiều định dạng khác nhau và các mật khẩu mới có thể được nhập vào.
- **Trình tạo mật khẩu ngẫu nhiên (Random password generator)**. Một trình tạo mật khẩu ngẫu nhiên tích hợp có thể tạo mật khẩu mạnh dựa trên các cài đặt khác nhau như trình tạo KeePass được hiển thị trong Hình 1-3.



Hình 1-3 Trình tạo mật khẩu ngẫu nhiên KeePass

Nguồn: KeePass

Giá trị của việc sử dụng một ứng dụng quản lý mật khẩu là có thể dễ dàng tạo và sử dụng các mật khẩu mạnh, độc đáo như WUuAôxB$2aWøBnd&Tf7MfEtm cho tất cả các tài khoản.

LƯU Ý

Mặc dù giá trị của các trình quản lý mật khẩu, hầu hết người dùng không tận dụng chúng. Một nghiên cứu gần đây đã so sánh phản hồi của các chuyên gia bảo mật với những người không chuyên về những gì họ làm để giữ an toàn. Kết quả cho thấy số lượng chuyên gia sử dụng trình quản lý mật khẩu cho ít nhất một số tài khoản của họ gấp ba lần số người không chuyên (73% so với 24%), và số lượng chuyên gia nói rằng việc sử dụng trình quản lý mật khẩu là một trong những điều quan trọng nhất họ làm để giữ an toàn trực tuyến gấp bốn lần.[11]

Tạo Mật Khẩu Mạnh

Nếu không sử dụng ứng dụng quản lý mật khẩu, thì cần tạo mật khẩu mạnh cho từng tài khoản riêng biệt. Các quan sát chung sau đây liên quan đến việc tạo mật khẩu bao gồm:

- Không sử dụng mật khẩu bao gồm các từ điển hoặc từ phát âm.
- Không lặp lại ký tự (xxx) hoặc sử dụng các chuỗi (abc, 123, qwerty).
- Không sử dụng ngày sinh, tên thành viên gia đình, tên thú cưng, địa chỉ hoặc bất kỳ thông tin cá nhân nào.
- Không sử dụng mật khẩu ngắn. Một mật khẩu mạnh nên có độ dài tối thiểu là 18 ký tự.

Mật khẩu nên càng dài càng tốt. Điều này là vì mật khẩu càng dài thì càng an toàn hơn mật khẩu ngắn, bởi vì mật khẩu càng dài, kẻ tấn công càng phải thực hiện nhiều nỗ lực hơn để cố gắng xác định nó. Công thức để xác định số lượng mật khẩu có thể có được khi biết số lượng ký tự có thể được sử dụng trong mật khẩu và độ dài mật khẩu là:

Số_Phím_Bàn_Phím ^ Độ_Dài_Mật_Khẩu = Tổng_Số_Mật_Khẩu_Có_Thể_Có.

Bảng 1-4 minh họa số lượng mật khẩu có thể có cho các độ dài mật khẩu khác nhau bằng cách sử dụng bàn phím tiêu chuẩn 80 phím. Mật khẩu dài hơn buộc kẻ tấn công phải dành nhiều thời gian hơn để cố gắng phá vỡ chúng.

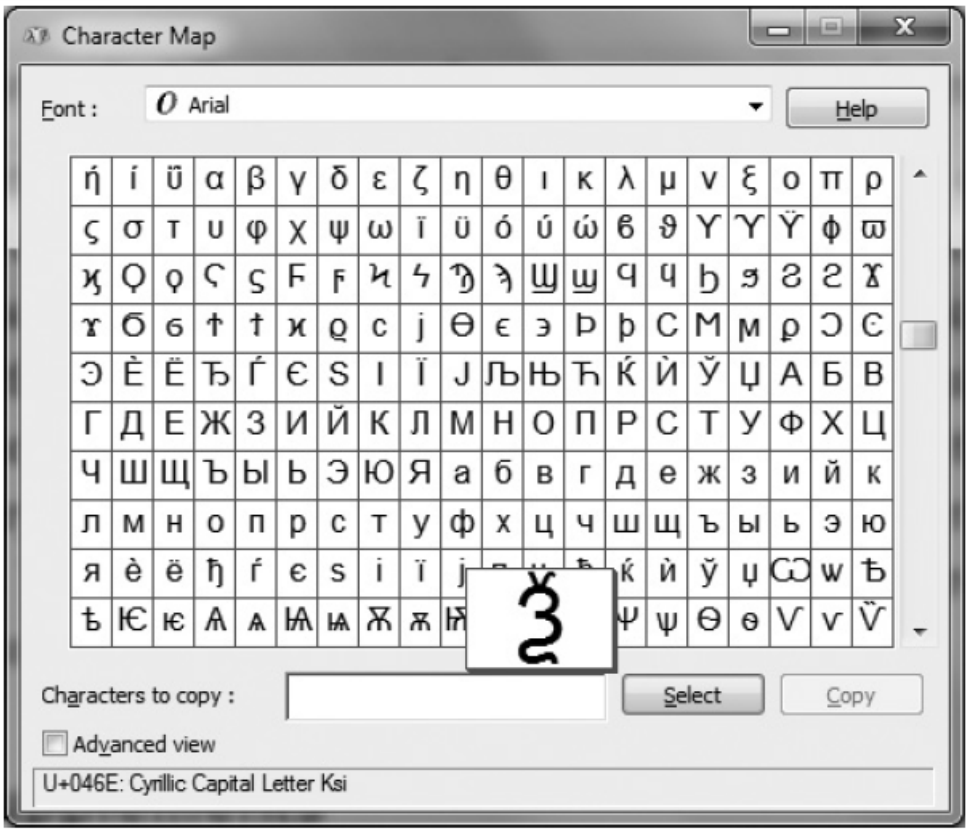
Bảng 1-4 Số lượng mật khẩu có thể có

Phím bàn phím	Độ dài mật khẩu	Số lượng mật khẩu có thể có
80	2	6.400
80	3	512.000
80	4	4.096.000
80	5	3.276.800.000
80	8	1.677.721.600.000.000

LƯU Ý

Về mặt kỹ thuật, việc tăng độ dài của mật khẩu sẽ làm tăng sức mạnh của nó theo cấp số nhân, trong khi việc tăng độ phức tạp chỉ tăng tuyến tính. Vì độ dài quan trọng hơn độ phức tạp, mật khẩu thisisalongerpassword được coi là mạnh hơn u$^#16.

Một cách để làm cho mật khẩu mạnh hơn là sử dụng các ký tự không có trên bàn phím, hoặc các ký tự đặc biệt không xuất hiện trên bàn phím. Đối với hệ điều hành Microsoft Windows, các ký tự này được tạo bằng cách giữ phím ALT đồng thời gõ một số trên bàn phím số (nhưng không phải các số ở hàng trên cùng của bàn phím). Ví dụ, ALT + 0163 tạo ra ký hiệu £. Một danh sách tất cả các ký tự không có trên bàn phím có sẵn có thể được xem bằng cách nhập charmap.exe tại màn hình Start, và sau đó nhấp vào một ký tự. Mã ALT + Oxxx sẽ xuất hiện ở góc dưới bên trái màn hình (nếu ký tự đó có thể được tái tạo trong Windows). Hình 1-4 hiển thị một bản đồ ký tự Windows.



Hình 1-4 Bản đồ ký tự Windows

Nguồn: Microsoft Windows

Nhận Diện Các Cuộc Tấn Công Lừa Đảo

Mặc dù các cuộc tấn công **phishing** (lừa đảo) khác nhau, chúng thường bắt đầu bằng việc nhận được một tin nhắn email tuyên bố đến từ một nguồn đáng tin cậy, chẳng hạn như một ngân hàng hoặc trang web mà người dùng có tài khoản. Tin nhắn email có thể chứa những điều sau:

- **Logo chính thức**. Những kẻ lừa đảo thường bao gồm logo của nhà cung cấp và cố gắng làm cho email trông giống như trang web của nhà cung cấp để thuyết phục người nhận rằng tin nhắn là thật. Tuy nhiên, sự hiện diện của logo không có nghĩa là email là hợp pháp.
- **Liên kết web**. Các email lừa đảo hầu như luôn chứa một liên kết mà người dùng được yêu cầu nhấp vào. Thông thường các địa chỉ này là những biến thể gần giống với địa chỉ hợp pháp, chẳng hạn như www.ebay_secure.com, www.e--bay.com, hoặc www.e-baynet.com.

- **Yêu cầu khẩn cấp**. Hầu hết các email lừa đảo khuyến khích người nhận hành động ngay lập tức nếu không tài khoản của họ sẽ bị vô hiệu hóa hoặc một hành động đe dọa tương tự sẽ xảy ra trong thời gian ngắn.

Ngay cả khi bạn kiểm tra cẩn thận các tin nhắn email của mình, vẫn có thể khó nhận ra các cuộc tấn công lừa đảo. Cách tiếp cận tốt nhất là coi bất kỳ email không mong đợi nào tuyên bố đến từ một nguồn đáng tin cậy là một tin nhắn lừa đảo.

CẢNH BÁO

Bạn không bao giờ nên nhấp vào một liên kết URL có trong tin nhắn email. Điều này là do liên kết được hiển thị (chẳng hạn như www.ebay.com) có thể che giấu liên kết thực sự ẩn trong tin nhắn (chẳng hạn như www.evil.com).

Tránh Trộm Cắp Danh Tính

Identity theft (Trộm cắp danh tính) xảy ra khi kẻ tấn công sử dụng thông tin cá nhân của người khác, chẳng hạn như số An sinh xã hội, số thẻ tín dụng hoặc các thông tin nhận dạng khác, để giả mạo cá nhân đó với mục đích thực hiện hành vi gian lận hoặc các tội phạm khác. Việc tránh trộm cắp danh tính bao gồm hai bước cơ bản. Bước đầu tiên là ngăn chặn kẻ trộm bằng cách bảo vệ thông tin. Điều này bao gồm:

- Xé nhỏ các tài liệu tài chính và giấy tờ chứa thông tin cá nhân trước khi vứt bỏ.
- Không mang theo số An sinh xã hội trong ví hoặc viết lên séc.
- Không cung cấp thông tin cá nhân qua điện thoại hoặc qua tin nhắn email.
- Giữ thông tin cá nhân ở nơi an toàn trong nhà hoặc căn hộ.

Bước thứ hai là theo dõi các báo cáo tài chính và tài khoản bằng cách thực hiện những điều sau:

- Cảnh giác với các dấu hiệu có thể cho thấy hoạt động bất thường trong tài khoản, chẳng hạn như một hóa đơn không đến đúng hạn hoặc số lượng lớn thẻ tín dụng hoặc sao kê tài khoản không được yêu cầu.
- Theo dõi các cuộc gọi liên quan đến các giao dịch mua hàng không được thực hiện.
- Xem xét cẩn thận các báo cáo tài chính và hóa đơn mỗi tháng ngay khi chúng đến.

Luật pháp đã được thông qua nhằm giúp người dùng Hoa Kỳ theo dõi thông tin tài chính của họ. Đạo luật Giao dịch Tín dụng Công bằng và Chính xác (Fair and Accurate Credit Transactions Act - FACTA) năm 2003 chứa các quy tắc liên quan đến quyền riêng tư của người tiêu dùng. FACTA cấp cho người tiêu dùng quyền yêu cầu một báo cáo tín dụng miễn phí từ mỗi trong ba công ty báo cáo tín dụng quốc gia mỗi 12 tháng. Nếu người tiêu dùng phát hiện ra vấn đề trên báo cáo tín dụng của mình, cô ấy phải gửi thư đến công ty báo cáo tín dụng trước. Theo luật liên bang, cơ quan này có 30 ngày để điều tra và phản hồi thông tin không chính xác được cho là và đưa ra một báo cáo đã sửa đổi. Nếu khiếu nại được chấp thuận, tất cả ba cơ quan báo cáo tín dụng phải được thông báo về các thông tin không chính xác, để họ có thể sửa đổi hồ sơ của mình. Nếu cuộc điều tra không giải quyết được vấn đề, một tuyên bố từ người tiêu dùng có thể được đưa vào hồ sơ và trong bất kỳ báo cáo tín dụng tương lai nào.

Thiết Lập Các Biện Pháp Phòng Thủ Mạng Xã Hội

Các trang mạng xã hội chứa một kho tàng thông tin cho kẻ tấn công, chẳng hạn như cung cấp thông tin cho kẻ trộm danh tính hoặc cung cấp cho kẻ tấn công cái nhìn sâu sắc về câu trả lời cho các câu hỏi bảo mật của người dùng được sử dụng để đặt lại mật khẩu (ví dụ: Tên thời con gái của mẹ bạn là gì?). Với tất cả thông tin có giá trị này, các trang mạng xã hội nên được đặt lên hàng đầu về bảo mật ngày nay; đáng buồn thay, đó không phải lúc nào cũng là trường hợp. Các trang mạng xã hội đã có lịch sử cung cấp bảo mật lỏng lẻo, không cung cấp cho người dùng sự hiểu biết rõ ràng về cách các tính năng bảo mật hoạt động, và thay đổi các tùy chọn bảo mật mà ít hoặc không có cảnh báo.

Có một số biện pháp phòng thủ chung có thể được sử dụng cho bất kỳ trang mạng xã hội nào. Trước hết và quan trọng nhất, người dùng nên cẩn trọng về những thông tin được đăng trên các trang mạng xã hội. Việc đăng Tôi sẽ đi Florida vào thứ Sáu trong hai tuần có thể cho thấy rằng nhà hoặc căn hộ sẽ trống trong thời gian đó, một lời mời hấp dẫn cho kẻ trộm. Thông tin khác được đăng có thể sau này gây ra sự xấu hổ. Việc đặt các câu hỏi như Sếp của tôi có chấp thuận không? Hoặc Mẹ tôi sẽ nghĩ gì về điều này? trước khi đăng có thể tạo động lực để suy nghĩ lại về tài liệu đó một lần nữa trước khi đăng.

Thứ hai, người dùng nên cẩn trọng về người có thể xem thông tin của họ. Một số loại thông tin có thể gây xấu hổ nếu được đọc bởi một số đối tượng nhất định, chẳng hạn như nhà tuyển dụng tiềm năng. Thông tin khác nên được giữ bí mật. Người dùng được khuyến khích xem xét cẩn thận ai được chấp nhận làm bạn bè trên mạng xã hội. Một khi một người đã được chấp nhận làm bạn bè, người đó sẽ có thể truy cập bất kỳ thông tin cá nhân hoặc hình ảnh nào. Thay vào đó, có thể nên hiển thị cho "bạn bè giới hạn" một phiên bản rút gọn của hồ sơ, chẳng hạn như những người quen hoặc đối tác kinh doanh thông thường.

Cuối cùng, vì các cài đặt bảo mật có sẵn trên các trang mạng xã hội thường xuyên được cập nhật bởi trang web mà không có cảnh báo, người dùng nên chú ý kỹ đến thông tin về các cài đặt bảo mật mới hoặc được cập nhật. Các cài đặt mới thường cung cấp mức độ bảo mật cao hơn nhiều bằng cách cho phép người dùng tinh chỉnh các tùy chọn hồ sơ tài khoản của họ.

Bảng 1-5 liệt kê một số khuyến nghị về quyền riêng tư và bảo mật cho trang mạng xã hội Facebook.

Bảng 1-5 Các khuyến nghị và giải thích về Facebook

Khuyến nghị	Giải thích
Xem xét cách bạn muốn sử dụng Facebook	Nếu bạn chỉ muốn giữ liên lạc với mọi người và có thể liên hệ với họ thì bạn nên hạn chế hơn về những gì bạn đăng và các chức năng của Facebook.
Xem lại Hướng dẫn Quyền riêng tư của Facebook	Dành thời gian đọc Hướng dẫn Quyền riêng tư của Facebook, chứa các chức năng và chính sách quyền riêng tư mới nhất.
Điều chỉnh cài đặt quyền riêng tư của Facebook để bảo vệ danh tính của bạn	Facebook cung cấp các tùy chọn bảo vệ mạnh mẽ nhưng chúng phải được người dùng cấu hình vì các tùy chọn mặc định thường rất dễ dãi.
Xem trang của bạn qua mắt người dùng khác	Nút Xem trước hồ sơ của tôi trên bất kỳ trang cài đặt quyền riêng tư nào cho phép người dùng kiểm tra cách thông tin của họ hiển thị cho người khác.
Cẩn thận suy nghĩ về người bạn cho phép trở thành bạn bè của	Một khi bạn đã chấp nhận ai đó làm bạn bè, họ sẽ có thể truy cập hầu như bất kỳ thông tin nào về bạn – bao gồm cả hình ảnh – mà bạn đã đánh dấu là có thể xem được.

mình	
Hiển thị cho người quen một phiên bản giới hạn hồ sơ của bạn	Đối với những người quen hoặc những người mà bạn không muốn chia sẻ tất cả thông tin của mình, hãy chọn họ làm người quen thay vì bạn bè.
Hạn chế Dòng thời gian và Thẻ	Xem xét việc chặn bạn bè thêm vào dòng thời gian của bạn. Xem lại ảnh người dùng khác cố gắng gắn thẻ bạn trong Dòng thời gian và Cài đặt Thẻ bằng cách bật tính năng cho phép bạn xem lại các thẻ mà mọi người thêm vào bài đăng của bạn trước khi chúng xuất hiện. Cũng quyết định xem đề xuất gắn thẻ có nên xuất hiện khi ảnh trông giống bạn được tải lên hay không.
Tắt các tùy chọn, sau đó mở từng tùy chọn một	Tắt một tùy chọn cho đến khi bạn quyết định rằng bạn muốn và cần nó, thay vì bắt đầu với tất cả mọi thứ đều có thể truy cập.

PHẦN III: CHIẾN LƯỢC BẢO MẬT

1. Ngăn chặn tấn công – Xây dựng hàng rào bảo mật vững chắc

Ngăn chặn tấn công là nền tảng của mọi chiến lược bảo mật. Nó tập trung vào việc chủ động xây dựng các rào cản, khiến kẻ tấn công khó có thể xâm nhập vào hệ thống. Giống như một pháo đài được xây dựng kiên cố, các biện pháp ngăn chặn nhằm mục đích phát hiện, làm chệch hướng và vô hiệu hóa các mối đe dọa trước khi chúng có thể gây hại. Để đạt được điều này, cần có sự kết hợp của nhiều công nghệ và quy trình.

Tường lửa (Firewall) và Hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS)

Tường lửa là tuyến phòng thủ đầu tiên, hoạt động như một bộ lọc kiểm soát lưu lượng truy cập mạng. Nó giám sát tất cả các gói dữ liệu ra vào, cho phép hoặc chặn chúng dựa trên các quy tắc bảo mật đã được định cấu hình. Một tường lửa mạnh mẽ giúp ngăn chặn truy cập trái phép từ bên ngoài và kiểm soát lưu lượng truy cập nội bộ, giảm thiểu nguy cơ lây lan của mã độc.

Bên cạnh tường lửa, **Hệ thống phát hiện xâm nhập (IDS)** và **Hệ thống ngăn chặn xâm nhập (IPS)** đóng vai trò bổ sung. IDS giám sát lưu lượng mạng để tìm kiếm các hoạt động đáng ngờ hoặc các mẫu tấn công đã biết, cảnh báo quản trị viên khi phát hiện mối đe dọa. IPS tiến thêm một bước bằng cách không chỉ phát hiện mà còn chủ động ngăn chặn các cuộc tấn công này, ví dụ như chặn địa chỉ IP nguồn gây ra hành vi độc hại. Việc triển khai kết hợp IDS/IPS giúp tăng cường khả năng phản ứng tự động và giảm thiểu thời gian phơi nhiễm trước các cuộc tấn công.

Quản lý danh tính và truy cập (IAM)

Quản lý danh tính và truy cập (IAM) là một trụ cột quan trọng trong việc ngăn chặn tấn công. IAM đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên phù hợp. Điều này bao gồm việc triển khai các chính sách mật khẩu mạnh, xác thực đa yếu tố (MFA), và kiểm soát truy cập dựa trên vai trò (RBAC).

- **Chính sách mật khẩu mạnh:** Yêu cầu người dùng tạo mật khẩu phức tạp, dài và thay đổi định kỳ.

- **Xác thực đa yếu tố (MFA):** Thêm một lớp bảo mật bằng cách yêu cầu người dùng cung cấp hai hoặc nhiều yếu tố xác minh để truy cập. Ví dụ: mật khẩu và mã OTP gửi qua điện thoại.
- **Kiểm soát truy cập dựa trên vai trò (RBAC):** Gán quyền truy cập dựa trên vai trò công việc của người dùng. Điều này đảm bảo rằng nhân viên chỉ có quyền truy cập vào những thông tin và hệ thống cần thiết cho công việc của họ, giảm thiểu rủi ro lạm dụng quyền truy cập.

Mã hóa dữ liệu

Mã hóa dữ liệu là một biện pháp bảo mật thiết yếu để bảo vệ thông tin cả khi truyền tải và khi lưu trữ. Khi dữ liệu được mã hóa, nó sẽ trở nên không thể đọc được đối với những người không có khóa giải mã.

- **Mã hóa khi truyền tải (Data in transit encryption):** Sử dụng các giao thức như SSL/TLS để bảo vệ dữ liệu khi nó di chuyển qua mạng, ngăn chặn việc chặn bắt và nghe trộm.
- **Mã hóa khi lưu trữ (Data at rest encryption):** Áp dụng mã hóa cho dữ liệu được lưu trữ trên ổ cứng, cơ sở dữ liệu, hoặc các thiết bị lưu trữ khác. Điều này đảm bảo rằng ngay cả khi kẻ tấn công có quyền truy cập vật lý vào thiết bị, dữ liệu vẫn được bảo vệ.

Đào tạo và nâng cao nhận thức người dùng

Con người thường là mắt xích yếu nhất trong chuỗi bảo mật. Kẻ tấn công thường nhắm vào yếu tố con người thông qua các kỹ thuật tấn công phi kỹ thuật (social engineering), phổ biến nhất là **tấn công lừa đảo (phishing)**. Do đó, việc **đào tạo và nâng cao nhận thức người dùng** là cực kỳ quan trọng để ngăn chặn tấn công.

- **Đào tạo định kỳ:** Tổ chức các buổi huấn luyện thường xuyên về các mối đe dọa an ninh mạng mới nhất, cách nhận biết các email lừa đảo, và các thực hành tốt nhất về bảo mật.
- **Kiểm tra giả lập:** Thực hiện các cuộc tấn công lừa đảo giả lập để kiểm tra khả năng nhận diện và phản ứng của nhân viên, từ đó đưa ra các phản hồi và cải thiện kịp thời.
- **Văn hóa bảo mật:** Xây dựng một văn hóa nơi mọi người coi trọng bảo mật và hiểu rằng họ đóng vai trò quan trọng trong việc bảo vệ thông tin.

2. Cập nhật phòng thủ – Thường xuyên cập nhật các biện pháp bảo mật

Thế giới an ninh mạng luôn thay đổi không ngừng. Các mối đe dọa mới xuất hiện hàng ngày, và các lỗ hổng bảo mật được phát hiện liên tục. Do đó, **cập nhật phòng thủ** không phải là một hoạt động một lần mà là một quá trình liên tục, đòi hỏi sự cảnh giác và hành động kịp thời. Việc duy trì các biện pháp bảo mật lỗi thời giống như việc cố gắng chống lại vũ khí hiện đại bằng khiên gỗ.

Quản lý lỗ hổng (Vulnerability Management) và vá lỗi (Patch Management)

Quản lý lỗ hổng là quá trình xác định, đánh giá và ưu tiên các lỗ hổng bảo mật trong hệ thống. Điều này bao gồm việc quét lỗ hổng định kỳ, phân tích kết quả và lên kế hoạch khắc phục.

Vá lỗi (Patch Management) là hành động cụ thể để khắc phục các lỗ hổng đã được xác định. Các nhà cung cấp phần mềm thường xuyên phát hành các bản vá (patches) để sửa lỗi và khắc phục các lỗ hổng bảo mật. Việc áp dụng các bản vá này một cách kịp thời là cực kỳ quan trọng.

- **Tự động hóa:** Tự động hóa quá trình quét lỗ hổng và áp dụng các bản vá khi có thể để đảm bảo tính nhất quán và hiệu quả.
- **Ưu tiên:** Ưu tiên vá các lỗ hổng nghiêm trọng và những lỗ hổng có khả năng bị khai thác cao nhất.
- **Kiểm thử:** Luôn kiểm thử các bản vá trong môi trường thử nghiệm trước khi triển khai trên môi trường sản phẩm để tránh gây ra các vấn đề không mong muốn.

Cập nhật phần mềm bảo mật

Các giải pháp bảo mật như phần mềm diệt virus, hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS), và tường lửa cần được **cập nhật thường xuyên** với các định nghĩa virus mới nhất và các quy tắc phát hiện tấn công mới nhất. Các nhà cung cấp liên tục nghiên cứu và phát triển để đối phó với các mối đe dọa mới, và việc không cập nhật sẽ khiến hệ thống trở nên dễ bị tổn thương.

- **Phần mềm diệt virus:** Đảm bảo rằng cơ sở dữ liệu virus được cập nhật hàng ngày để nhận diện và loại bỏ các loại mã độc mới nhất.
- **IDS/IPS:** Cập nhật các quy tắc (signatures) để nhận diện các mẫu tấn công mới và hành vi bất thường.

- **Hệ thống tường lửa:** Cập nhật các quy tắc và tính năng để đối phó với các phương thức tấn công mới.

Theo dõi và phân tích nhật ký (Log Monitoring and Analysis)

Việc **theo dõi và phân tích nhật ký hệ thống** là một phần không thể thiếu của quá trình cập nhật phòng thủ. Nhật ký (logs) ghi lại các sự kiện diễn ra trên hệ thống, từ các lần đăng nhập, truy cập tệp, đến các lỗi hệ thống. Phân tích nhật ký giúp phát hiện sớm các hoạt động đáng ngờ hoặc dấu hiệu của một cuộc tấn công.

- **Hệ thống quản lý thông tin và sự kiện bảo mật (SIEM):** Triển khai một hệ thống SIEM để thu thập, tương quan và phân tích nhật ký từ nhiều nguồn khác nhau. SIEM có thể tự động hóa việc phát hiện các mối đe dọa và cảnh báo quản trị viên.
- **Kiểm tra nhật ký định kỳ:** Dù có SIEM hay không, việc kiểm tra nhật ký định kỳ bởi các chuyên gia bảo mật vẫn rất quan trọng để phát hiện những điều bất thường mà hệ thống tự động có thể bỏ sót.

Tình báo mối đe dọa (Threat Intelligence)

Tình báo mối đe dọa cung cấp thông tin về các mối đe dọa hiện tại và tiềm ẩn, bao gồm các phương thức tấn công mới, các lỗ hổng chưa được vá, và các nhóm tội phạm mạng. Việc tích hợp tình báo mối đe dọa vào chiến lược bảo mật giúp tổ chức chủ động hơn trong việc dự đoán và đối phó với các cuộc tấn công.

- **Nguồn tin cậy:** Đăng ký các dịch vụ tình báo mối đe dọa từ các nhà cung cấp uy tín hoặc tham gia các diễn đàn chia sẻ thông tin về an ninh mạng.
- **Phân tích và hành động:** Sử dụng thông tin tình báo để điều chỉnh các chính sách bảo mật, cập nhật hệ thống phòng thủ, và đào tạo nhân viên.

3. Giảm thiểu thiệt hại – Sao lưu dữ liệu định kỳ để phòng trường hợp bị tấn công

Mặc dù đã áp dụng các biện pháp ngăn chặn và phòng thủ tốt nhất, không có hệ thống nào là hoàn toàn miễn nhiễm với các cuộc tấn công. Khi một cuộc tấn công xảy ra, mục tiêu chính là **giảm thiểu thiệt hại** ở mức thấp nhất. Trong đó, **sao lưu dữ liệu định kỳ** là biện pháp quan trọng nhất để đảm bảo khả năng phục hồi sau thảm họa.

Sao lưu dữ liệu thường xuyên

Việc **sao lưu dữ liệu thường xuyên** là xương sống của mọi kế hoạch phục hồi sau thảm họa. Dữ liệu là tài sản quý giá nhất của một tổ chức, và việc mất dữ liệu có thể dẫn đến những hậu quả nghiêm trọng.

- **Tần suất sao lưu:** Tần suất sao lưu cần được xác định dựa trên mức độ quan trọng của dữ liệu và tần suất thay đổi của nó. Đối với dữ liệu quan trọng và thay đổi liên tục, sao lưu có thể cần diễn ra hàng giờ hoặc hàng ngày. Dữ liệu ít thay đổi có thể sao lưu hàng tuần hoặc hàng tháng.
- **Loại sao lưu:**
  - **Sao lưu toàn bộ (Full Backup):** Sao chép tất cả dữ liệu.
  - **Sao lưu gia tăng (Incremental Backup):** Chỉ sao chép dữ liệu đã thay đổi kể từ lần sao lưu gần nhất (toàn bộ hoặc gia tăng).
  - **Sao lưu khác biệt (Differential Backup):** Chỉ sao chép dữ liệu đã thay đổi kể từ lần sao lưu toàn bộ gần nhất. Sự kết hợp các loại sao lưu này giúp tối ưu hóa thời gian và dung lượng lưu trữ.

Lưu trữ bản sao lưu an toàn

Việc sao lưu dữ liệu sẽ không có ý nghĩa nếu bản sao lưu cũng bị ảnh hưởng bởi cuộc tấn công. Do đó, **lưu trữ bản sao lưu an toàn** là cực kỳ quan trọng.

- **Quy tắc 3-2-1:** Đây là một quy tắc vàng trong sao lưu:
  - **3 bản sao:** Giữ ít nhất 3 bản sao dữ liệu của bạn.
  - **2 loại phương tiện khác nhau:** Lưu trữ các bản sao trên 2 loại phương tiện lưu trữ khác nhau (ví dụ: ổ đĩa cục bộ và đám mây, hoặc ổ đĩa cục bộ và băng từ).
  - **1 bản sao bên ngoài:** Giữ ít nhất 1 bản sao bên ngoài địa điểm vật lý của tổ chức (ví dụ: trung tâm dữ liệu từ xa, dịch vụ đám mây).
- **Bảo vệ bản sao lưu:** Các bản sao lưu cũng cần được bảo vệ khỏi truy cập trái phép bằng cách mã hóa và áp dụng các biện pháp kiểm soát truy cập nghiêm ngặt.
- **Kiểm tra tính toàn vẹn:** Định kỳ kiểm tra tính toàn vẹn của các bản sao lưu để đảm bảo rằng chúng có thể được phục hồi thành công khi cần thiết.

Kế hoạch phục hồi sau thảm họa (Disaster Recovery Plan - DRP)

Một **kế hoạch phục hồi sau thảm họa (DRP)** chi tiết là điều kiện tiên quyết để giảm thiểu thiệt hại. DRP phác thảo các bước cần thiết để khôi phục hoạt động kinh doanh sau một sự cố an ninh mạng hoặc thảm họa khác.

- **Xác định mục tiêu thời gian phục hồi (RTO) và mục tiêu điểm phục hồi (RPO):**
    - **RTO (Recovery Time Objective):** Thời gian tối đa mà hệ thống hoặc ứng dụng có thể ngừng hoạt động.
    - **RPO (Recovery Point Objective):** Lượng dữ liệu tối đa mà tổ chức có thể chấp nhận mất. Các mục tiêu này sẽ định hình chiến lược sao lưu và phục hồi.
- **Quy trình từng bước:** DRP cần mô tả chi tiết các bước cần thực hiện, bao gồm ai chịu trách nhiệm, công cụ nào được sử dụng và các quy trình liên lạc.
- **Kiểm tra và cập nhật định kỳ:** DRP cần được kiểm tra định kỳ thông qua các bài diễn tập và cập nhật để phản ánh những thay đổi trong hệ thống hoặc môi trường kinh doanh.

Kế hoạch ứng phó sự cố (Incident Response Plan - IRP)

Kế hoạch ứng phó sự cố (IRP) là một phần quan trọng khác để giảm thiểu thiệt hại. IRP là một bộ hướng dẫn chi tiết về cách phát hiện, phân tích, ngăn chặn và phục hồi sau một sự cố an ninh mạng.

- **Phát hiện:** Làm thế nào để phát hiện một cuộc tấn công?
- **Phân tích:** Làm thế nào để điều tra và hiểu phạm vi của sự cố?
- **Ngăn chặn:** Làm thế nào để cô lập và ngăn chặn cuộc tấn công lây lan?
- **Xóa bỏ:** Làm thế nào để loại bỏ mối đe dọa khỏi hệ thống?
- **Phục hồi:** Làm thế nào để khôi phục hệ thống và dữ liệu về trạng thái bình thường?
- **Bài học rút ra:** Đánh giá sự cố và cải thiện các biện pháp phòng thủ. Việc có một IRP được đào tạo và kiểm tra tốt giúp tổ chức phản ứng nhanh chóng và hiệu quả, giảm thiểu tác động của một cuộc tấn công.

4. Các lớp bảo vệ (Layer) – Sử dụng nhiều lớp bảo mật để tăng cường an toàn

Trong an ninh mạng, khái niệm **"bảo mật theo chiều sâu" (defense in depth)** hay **"bảo mật đa lớp"** là một nguyên tắc cốt lõi. Thay vì dựa vào một lớp phòng thủ duy nhất, chiến lược này khuyến khích việc triển khai nhiều lớp bảo mật khác nhau, chồng lên nhau. Ý tưởng là nếu một lớp phòng thủ bị vượt qua, vẫn còn các lớp khác để ngăn chặn kẻ tấn công tiến xa hơn. Điều này giống như việc xây dựng một lâu đài với nhiều bức tường, hào nước và cổng canh gác.

Bảo vệ biên (Perimeter Security)

Bảo vệ biên là lớp phòng thủ đầu tiên, tập trung vào việc bảo vệ ranh giới mạng của tổ chức khỏi các mối đe dọa bên ngoài.

- **Tường lửa và IPS/IDS:** Như đã đề cập, đây là những công cụ cơ bản để kiểm soát và giám sát lưu lượng ra vào mạng.
- **Cổng bảo mật web (Web Security Gateway):** Lọc các trang web độc hại và chặn truy cập vào các trang không an toàn.
- **Cổng bảo mật email (Email Security Gateway):** Chặn các email lừa đảo (phishing), mã độc và thư rác trước khi chúng đến hộp thư của người dùng.
- **Mạng riêng ảo (VPN):** Cung cấp kết nối an toàn cho người dùng từ xa, mã hóa dữ liệu khi truyền tải qua mạng công cộng.

Bảo vệ mạng nội bộ (Internal Network Security)

Ngay cả khi kẻ tấn công vượt qua được lớp bảo vệ biên, cần có các biện pháp để bảo vệ mạng nội bộ.

- **Phân đoạn mạng (Network Segmentation):** Chia mạng thành các phân đoạn nhỏ hơn (VLANs). Điều này giới hạn sự lây lan của một cuộc tấn công nếu một phân đoạn bị xâm nhập. Ví dụ, tách biệt mạng dành cho khách, mạng dành cho máy chủ và mạng dành cho người dùng cuối.
- **Kiểm soát truy cập mạng (Network Access Control - NAC):** Đảm bảo rằng chỉ các thiết bị tuân thủ chính sách bảo mật mới được phép kết nối vào mạng.
- **Hệ thống phát hiện/ngăn chặn xâm nhập nội bộ (Internal IDS/IPS):** Giám sát lưu lượng truy cập trong mạng nội bộ để phát hiện các hoạt động đáng ngờ, đặc biệt là các chuyển động ngang (lateral movement) của kẻ tấn công.

Bảo vệ điểm cuối (Endpoint Security)

Bảo vệ điểm cuối tập trung vào việc bảo vệ các thiết bị cuối cùng được sử dụng bởi người dùng, như máy tính để bàn, máy tính xách tay, điện thoại thông minh và máy chủ.

- **Phần mềm diệt virus/chống mã độc:** Các giải pháp bảo mật điểm cuối hiện đại không chỉ phát hiện virus mà còn chống lại mã độc tống tiền, trojan và các mối đe dọa tiên tiến khác.
- **Quản lý lỗ hổng và vá lỗi:** Đảm bảo rằng tất cả các điểm cuối đều được cập nhật các bản vá bảo mật mới nhất cho hệ điều hành và các ứng dụng.
- **Kiểm soát thiết bị ngoại vi:** Hạn chế hoặc kiểm soát việc sử dụng các thiết bị USB và các thiết bị lưu trữ khác để ngăn chặn lây nhiễm mã độc.
- **Mã hóa ổ đĩa:** Mã hóa toàn bộ ổ đĩa trên các thiết bị điểm cuối để bảo vệ dữ liệu trong trường hợp thiết bị bị mất hoặc bị đánh cắp.

Bảo vệ dữ liệu (Data Security)

Dữ liệu là tài sản quý giá nhất, vì vậy việc bảo vệ dữ liệu là một lớp bảo mật quan trọng.

- **Mã hóa dữ liệu:** Mã hóa dữ liệu cả khi truyền tải và khi lưu trữ.
- **Quản lý quyền truy cập dữ liệu:** Đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập và sửa đổi dữ liệu.
- **Phòng chống mất mát dữ liệu (Data Loss Prevention - DLP):** Các giải pháp DLP giúp ngăn chặn việc dữ liệu nhạy cảm rời khỏi mạng hoặc bị chia sẻ không đúng cách.

Bảo vệ ứng dụng (Application Security)

Các ứng dụng phần mềm thường là mục tiêu phổ biến của các cuộc tấn công.

- **Kiểm tra bảo mật ứng dụng:** Thường xuyên kiểm tra các ứng dụng để tìm lỗ hổng bảo mật, bao gồm kiểm thử bảo mật tĩnh (SAST) và động (DAST).
- **Tường lửa ứng dụng web (Web Application Firewall - WAF):** Bảo vệ các ứng dụng web khỏi các cuộc tấn công phổ biến như SQL Injection và Cross-Site Scripting (XSS).
- **Cập nhật ứng dụng:** Đảm bảo rằng tất cả các ứng dụng đều được cập nhật các bản vá bảo mật mới nhất từ nhà cung cấp.

5. Luôn trong tư thế phòng thủ – Không bao giờ chủ quan với các nguy cơ tấn công

Luôn trong tư thế phòng thủ là một triết lý an ninh mạng. Nó thừa nhận rằng các mối đe dọa luôn hiện hữu và không có giải pháp bảo mật nào là hoàn hảo. Thay vì coi bảo mật là một điểm đến, nó là một hành trình liên tục, đòi hỏi sự cảnh giác, thích ứng và chủ động. Việc chủ quan có thể dẫn đến những hậu quả nghiêm trọng, bởi vì kẻ tấn công chỉ cần một kẽ hở duy nhất để xâm nhập.

Giám sát liên tục và phản ứng chủ động

Một phần cốt lõi của việc luôn trong tư thế phòng thủ là **giám sát liên tục** hệ thống và mạng lưới. Điều này bao gồm:

- **Giám sát hoạt động mạng:** Sử dụng các công cụ như SIEM, NIDS (Network Intrusion Detection System) để theo dõi lưu lượng mạng, tìm kiếm các dấu hiệu bất thường hoặc các mẫu tấn công.
- **Giám sát hành vi người dùng (User Behavior Analytics - UBA):** Phân tích các hành vi của người dùng để phát hiện những sai lệch so với hành vi bình thường, có thể là dấu hiệu của tài khoản bị xâm nhập hoặc hoạt động nội bộ độc hại.
- **Giám sát nhật ký (Log Monitoring):** Đảm bảo rằng nhật ký từ tất cả các hệ thống và ứng dụng quan trọng được thu thập, lưu trữ và phân tích thường xuyên. **Phản ứng chủ động** liên quan đến việc không chỉ chờ đợi các mối đe dọa mà còn chủ động tìm kiếm và vô hiệu hóa chúng. Điều này bao gồm:
- **Săn lùng mối đe dọa (Threat Hunting):** Các chuyên gia bảo mật chủ động tìm kiếm các dấu hiệu của kẻ tấn công trong mạng, ngay cả khi không có cảnh báo rõ ràng từ hệ thống.
- **Kiểm tra thâm nhập (Penetration Testing):** Thuê các chuyên gia bên ngoài để mô phỏng các cuộc tấn công nhằm tìm kiếm các lỗ hổng mà kẻ tấn công có thể khai thác.
- **Diễn tập ứng phó sự cố:** Thường xuyên diễn tập các kịch bản tấn công để đảm bảo rằng đội ngũ ứng phó sự cố đã sẵn sàng và các kế hoạch là hiệu quả.

Đánh giá rủi ro định kỳ

Môi trường kinh doanh và công nghệ luôn thay đổi, kéo theo sự thay đổi về các mối đe dọa và lỗ hổng. Do đó, việc **đánh giá rủi ro định kỳ** là cần thiết để đảm bảo rằng chiến lược bảo mật vẫn phù hợp.

- **Xác định tài sản:** Liệt kê và phân loại tất cả các tài sản thông tin quan trọng.
- **Xác định mối đe dọa:** Phân tích các mối đe dọa tiềm ẩn đối với từng tài sản.
- **Xác định lỗ hổng:** Tìm kiếm các điểm yếu có thể bị khai thác.
- **Đánh giá rủi ro:** Ước tính khả năng xảy ra và tác động của từng rủi ro.
- **Đưa ra biện pháp giảm thiểu:** Đề xuất và triển khai các biện pháp để giảm thiểu rủi ro xuống mức chấp nhận được.

Đào tạo và nâng cao nhận thức liên tục

Như đã đề cập, yếu tố con người là một phần quan trọng của bảo mật. Việc **đào tạo và nâng cao nhận thức liên tục** là cần thiết để giữ cho tất cả nhân viên được cập nhật về các mối đe dọa mới nhất và các thực hành bảo mật tốt nhất.

- **Các buổi huấn luyện thường xuyên:** Không chỉ là một lần, mà là các buổi huấn luyện định kỳ, cập nhật nội dung để phù hợp với tình hình thực tế.
- **Thông báo và cảnh báo:** Chia sẻ thông tin về các cuộc tấn công lừa đảo mới, các lỗ hổng đã biết, và các lời khuyên bảo mật hữu ích.
- **Khuyến khích báo cáo:** Tạo một môi trường nơi nhân viên cảm thấy thoải mái khi báo cáo các hoạt động đáng ngờ hoặc các sự cố bảo mật mà không sợ bị đổ lỗi.

Văn hóa bảo mật

Cuối cùng, việc luôn trong tư thế phòng thủ đòi hỏi phải xây dựng một **văn hóa bảo mật mạnh mẽ** trong toàn tổ chức. Điều này có nghĩa là bảo mật không chỉ là trách nhiệm của đội ngũ IT hoặc an ninh mạng, mà là trách nhiệm của tất cả mọi người.

- **Sự cam kết của lãnh đạo:** Lãnh đạo cấp cao cần thể hiện sự cam kết mạnh mẽ đối với an ninh mạng, phân bổ đủ nguồn lực và làm gương trong việc tuân thủ các chính sách bảo mật.
- **Tích hợp vào quy trình làm việc:** Bảo mật cần được tích hợp vào mọi quy trình làm việc, từ phát triển phần mềm (Security by Design) đến quản lý dự án và hoạt động hàng ngày.

- **Khuyến khích trách nhiệm cá nhân:** Mỗi cá nhân cần hiểu vai trò của mình trong việc bảo vệ thông tin và tài sản của tổ chức.

BÀI 2: BẢO VỆ DỮ LIỆU CÁ NHÂN VÀ QUYỀN RIÊNG TƯ

Chủ đề "Bảo vệ dữ liệu cá nhân và quyền riêng tư" trang bị cho người học khả năng nhận diện và áp dụng các biện pháp phù hợp nhằm bảo vệ thông tin cá nhân trong môi trường số. Nội dung học tập giúp học viên hiểu rõ tầm quan trọng của việc kiểm soát thông tin định danh cá nhân, từ đó lựa chọn cách thức sử dụng và chia sẻ dữ liệu một cách an toàn và hợp lý. Ngoài ra, người học còn được hướng dẫn cách đánh giá các chính sách quyền riêng tư để xác định mức độ minh bạch và phù hợp trong việc thu thập, xử lý và sử dụng dữ liệu cá nhân bởi các tổ chức, dịch vụ số. Kiến thức này đóng vai trò thiết yếu trong việc xây dựng nhận thức về quyền riêng tư và góp phần hình thành thói quen sử dụng công nghệ có trách nhiệm và an toàn.

PHẦN I: DỮ LIỆU VÀ DỮ LIỆU CÁ NHÂN

1. Dữ liệu là gì?

Dữ liệu (Data) là nền tảng của mọi hoạt động trong môi trường số. Dữ liệu có thể được hiểu là các **thông tin hoặc giá trị** được **thu thập, lưu trữ, xử lý** nhằm mục đích phục vụ cho phân tích, truyền thông tin, ra quyết định hoặc vận hành hệ thống. Dữ liệu tồn tại ở nhiều dạng khác nhau, bao gồm:

- **Số học**: các con số định lượng như điểm số, số liệu thống kê, nhiệt độ, v.v.
- **Văn bản**: thông tin dạng chữ, ký hiệu, đoạn văn bản.
- **Hình ảnh**: các tệp tin ảnh tĩnh như JPG, PNG.
- **Âm thanh**: bản ghi âm, nhạc số.
- **Video**: tệp hình ảnh động có âm thanh như MP4, AVI.
- **Dữ liệu nhị phân**: dạng dữ liệu được máy tính sử dụng trực tiếp.

Trong môi trường mạng, dữ liệu có thể được tạo ra và lan truyền với tốc độ cực lớn. Từ một tìm kiếm Google, một lượt thích trên mạng xã hội, hay một giao dịch ngân hàng, tất cả đều tạo ra dữ liệu. Những dữ liệu này, khi được thu thập và phân tích, có thể mang lại giá trị to lớn về kinh tế, khoa học và quản trị.

2. Khái niệm dữ liệu cá nhân

2.1 Định nghĩa

Dữ liệu cá nhân (Personal Data) là một loại dữ liệu đặc biệt, có **liên quan trực tiếp hoặc gián tiếp đến một cá nhân đã được xác định hoặc có thể được xác định**. Việc xác định có thể thông qua một yếu tố (ví dụ: số căn cước công dân) hoặc nhiều yếu tố kết hợp (ví dụ: tên, địa chỉ và ngày sinh).

Các cơ quan quản lý như Liên minh châu Âu (EU) với GDPR định nghĩa dữ liệu cá nhân một cách nghiêm ngặt, nhằm bảo vệ quyền riêng tư của người dân trong thời đại kỹ thuật số.

2.2 Ví dụ về dữ liệu cá nhân

Dữ liệu cá nhân rất đa dạng và có thể bao gồm:

- **Thông tin định danh**: Họ tên, ngày sinh, số CMND/CCCD, ảnh chân dung
- **Dữ liệu liên lạc**: Số điện thoại, địa chỉ nhà, email
- **Dữ liệu sinh trắc học**: Vân tay, khuôn mặt, võng mạc

- **Thông tin định vị**: Vị trí GPS, địa chỉ IP
- **Dữ liệu tài chính**: Tài khoản ngân hàng, số thẻ tín dụng
- **Dữ liệu y tế**: Hồ sơ bệnh án, kết quả xét nghiệm
- **Dữ liệu hành vi**: Lịch sử tìm kiếm, thói quen tiêu dùng, mạng xã hội

3. Vì sao dữ liệu cá nhân lại quan trọng?

3.1 Là tài sản vô hình có giá trị

Dữ liệu cá nhân là nguồn nguyên liệu cho các hệ thống phân tích, dự đoán, tiếp thị và điều hành. Các công ty công nghệ lớn thường sử dụng dữ liệu người dùng để xây dựng hồ sơ hành vi, tối ưu quảng cáo và cá nhân hóa dịch vụ.

Một cá nhân không cung cấp bất kỳ thông tin nào cũng vẫn có thể bị "truy dấu" qua hành vi trực tuyến. Dữ liệu chính là "dấu vết số" mà mỗi người để lại khi sử dụng Internet.

3.2 Là mục tiêu chính của tội phạm mạng

Tội phạm mạng thường xuyên tấn công vào hệ thống lưu trữ dữ liệu cá nhân để:

- **Đánh cắp danh tính** (Identity Theft): Mạo danh người khác để vay tiền, mở tài khoản, hoặc thực hiện hành vi phạm pháp.
- **Lừa đảo tài chính**: Sử dụng thông tin ngân hàng, thẻ tín dụng để rút tiền hoặc chi tiêu trái phép.
- **Tống tiền, đe dọa**: Dựa vào các thông tin riêng tư để ép buộc nạn nhân phải trả tiền.
- **Theo dõi và kiểm soát cá nhân**: Dữ liệu về vị trí, mối quan hệ, cuộc gọi... có thể bị lợi dụng để giám sát.
- **Làm mất uy tín cá nhân hoặc tổ chức**: Khi dữ liệu cá nhân bị rò rỉ trên mạng, hậu quả về hình ảnh có thể nghiêm trọng.

3.3 Khó thay thế nếu bị rò rỉ

Khác với mật khẩu có thể đổi, **các thông tin như CMND, ảnh khuôn mặt hay dữ liệu sinh học không thể thay đổi**. Một khi đã bị rò rỉ, cá nhân gần như mất kiểm soát hoàn toàn.

4. Thách thức trong việc bảo vệ dữ liệu cá nhân

4.1 Người dùng thiếu nhận thức

Rất nhiều người chia sẻ công khai thông tin cá nhân trên mạng xã hội mà không lường trước nguy cơ:

- Đăng hình CCCD, thẻ ngân hàng
- Check-in địa điểm thật thời gian thực
- Công khai số điện thoại, địa chỉ trong bài viết cá nhân

Điều này vô tình tạo điều kiện cho kẻ xấu dễ dàng thu thập dữ liệu.

4.2 Hệ thống kỹ thuật yếu kém

Nhiều tổ chức (đặc biệt là doanh nghiệp nhỏ, cơ quan hành chính) không có đủ năng lực bảo mật hệ thống:

- Không mã hóa dữ liệu khi lưu trữ hoặc truyền tải
- Không có chính sách phân quyền truy cập hợp lý
- Không kiểm tra, cập nhật phần mềm định kỳ

4.3 Thiếu quy định pháp lý rõ ràng và chế tài mạnh

Ở một số quốc gia, luật bảo vệ dữ liệu cá nhân còn sơ khai hoặc chưa được thi hành nghiêm túc. Điều này tạo ra khoảng trống pháp lý, khiến các tổ chức thiếu động lực để đầu tư vào bảo mật.

5. Nguyên tắc bảo vệ dữ liệu cá nhân

5.1 Thu thập có mục đích, minh bạch

Chỉ thu thập dữ liệu khi thực sự cần thiết, thông báo rõ mục đích sử dụng cho người dùng, và xin sự đồng ý của họ.

5.2 Giới hạn lưu trữ

Dữ liệu không nên bị giữ lại quá lâu. Sau khi hoàn tất mục đích sử dụng, dữ liệu nên được xóa an toàn.

5.3 Bảo mật và kiểm soát truy cập

Áp dụng các biện pháp kỹ thuật để:

- Mã hóa dữ liệu
- Phân quyền truy cập
- Ghi nhật ký truy cập

5.4 Quyền của người dùng

Người dùng có quyền:

- Biết dữ liệu nào đang được lưu giữ

- Yêu cầu chỉnh sửa, xóa bỏ
- Từ chối chia sẻ dữ liệu cho bên thứ ba

---

6. Vai trò của cá nhân trong việc bảo vệ dữ liệu của chính mình

6.1 Hạn chế chia sẻ thông tin không cần thiết

Không công khai thông tin định danh trên mạng xã hội, không cung cấp dữ liệu cho các ứng dụng không rõ nguồn gốc.

6.2 Sử dụng công cụ bảo mật

- Cài đặt phần mềm chống virus
- Sử dụng xác thực hai yếu tố
- Duyệt web qua VPN
- Đặt mật khẩu mạnh và thay đổi định kỳ

6.3 Luôn cảnh giác trước các dấu hiệu bất thường

Ví dụ:

- Nhận email lạ yêu cầu cung cấp thông tin cá nhân
- Tài khoản ngân hàng bị trừ tiền không rõ lý do
- Thiết bị bị chậm bất thường, xuất hiện ứng dụng lạ

7. Hệ quả khi dữ liệu cá nhân bị xâm phạm

Loại dữ liệu bị rò rỉ	**Hệ quả tiềm ẩn**
Số CMND/CCCD	Mạo danh mở tài khoản, vay tiền
Email, mật khẩu	Truy cập trái phép tài khoản, gửi thư rác
Số thẻ tín dụng	Rút tiền trái phép
Dữ liệu bệnh án	Bị phân biệt đối xử, quấy rối
Dữ liệu định vị	Bị theo dõi, xác định vị trí
Dữ liệu tài chính	Mất tiền, bị lừa đầu tư

8. Kết luận

Dữ liệu cá nhân là phần cốt lõi định danh con người trong thời đại kỹ thuật số. Khi dữ liệu trở thành tài sản quý giá, việc bảo vệ dữ liệu cá nhân không còn là lựa chọn mà là một yêu cầu tất yếu, gắn liền với quyền riêng tư và an toàn thông tin.

Mỗi cá nhân, tổ chức, và cả chính phủ đều có vai trò trong việc đảm bảo an ninh dữ liệu cá nhân. Chỉ khi dữ liệu được bảo vệ đúng mức, xã hội số mới có thể phát triển bền vững, văn minh và an toàn.

PHẦN II: CÁC LOẠI HÌNH TẤN CÔNG DỮ LIỆU CÁ NHÂN VÀ CÁC BIỆN PHÁP BẢO VỆ

1. Tấn Công Mật Khẩu

Trong hầu hết các trường hợp, người dùng khi đăng nhập vào máy tính hoặc một trang web sẽ được yêu cầu tự nhận dạng. Điều này được thực hiện bằng cách nhập một mã định danh được gọi là **username**, chẳng hạn như SListz. Tuy nhiên, vì bất cứ ai cũng có thể nhập tên người dùng này, bước tiếp theo là người dùng phải **xác thực** chính mình bằng cách chứng minh rằng mình thực sự là SListz. Việc cung cấp bằng chứng về tính xác thực của người dùng (một quá trình được gọi là **authentication**) xác nhận danh tính của họ và có thể được sử dụng để bảo vệ các tài sản quan trọng của người dùng bằng cách ngăn chặn sự truy cập của kẻ mạo danh.

Phương tiện xác thực phổ biến nhất là cung cấp thông tin mà chỉ người dùng chính hãng mới biết: vì chỉ SListz thực sự hoặc "đích thực" mới biết duy nhất thông tin này, nó có thể được sử dụng để xác nhận danh tính của cô ấy. Thông tin được biết duy nhất đó được gọi là **mật khẩu**. Mật khẩu là một tổ hợp bí mật của các chữ cái, số và/hoặc ký tự mà – lý tưởng nhất – chỉ người dùng mới biết.

Điểm Yếu của Mật Khẩu

Sức mạnh của mật khẩu – rằng chúng dựa trên trí nhớ con người – cũng chính là điểm yếu của mật khẩu. Đó là vì con người chỉ có thể ghi nhớ một số lượng giới hạn các mục. Mật khẩu đặt gánh nặng lớn lên trí nhớ theo nhiều cách:

- Các mật khẩu hiệu quả nhất thường dài và phức tạp. Tuy nhiên, những mật khẩu này khó cho người dùng ghi nhớ và sau đó nhớ lại chính xác khi cần. Và mỗi mật khẩu được sử dụng nên là duy nhất, điều này càng làm căng thẳng trí nhớ con người hơn.

- Người dùng phải nhớ mật khẩu cho nhiều tài khoản khác nhau. Chúng bao gồm máy tính và thiết bị di động được sử dụng tại nơi làm việc, trường học và ở nhà; nhiều tài khoản web; ngân hàng trực tuyến; tài khoản email; tài khoản mạng xã hội; v.v. Trong một nghiên cứu, 28% người dùng có hơn 13 mật khẩu mỗi người,[1] trong khi trong một nghiên cứu khác, một nhóm 144 người dùng có trung bình 16 mật khẩu mỗi người.[2] Và người dùng từ 16–24 tuổi có trung bình 6,6 tài khoản khác nhau chỉ riêng cho các trang mạng xã hội như Facebook, Twitter và Instagram.[3]

- Nhiều hệ thống kinh doanh có chính sách bảo mật nghiêm ngặt yêu cầu mật khẩu phải hết hạn sau một khoảng thời gian nhất định, chẳng hạn như 45–60 ngày, khi một mật khẩu mới phải được tạo. Một số chính sách bảo mật thậm chí còn ngăn việc sử dụng lại mật khẩu đã sử dụng trước đó, buộc người dùng phải liên tục ghi nhớ mật khẩu mới.

Vì những gánh nặng mà mật khẩu đặt lên trí nhớ con người, người dùng thường đi đường tắt để giúp họ ghi nhớ và nhớ lại mật khẩu của mình. Những đường tắt này tạo ra một mật khẩu yếu, hay một mật khẩu dễ bị kẻ tấn công phá vỡ. Mật khẩu yếu thường sử dụng một từ thông dụng làm mật khẩu (princess), một mật khẩu ngắn (desk), một chuỗi ký tự dễ đoán (abc123) hoặc thông tin cá nhân (Hannah) trong mật khẩu. Một đường tắt phổ biến khác là tái sử dụng cùng một mật khẩu cho nhiều tài khoản. Mặc dù điều này giúp người dùng dễ dàng hơn, nhưng nó cũng giúp kẻ tấn công dễ dàng hơn khi xâm nhập một tài khoản để truy cập vào các tài khoản khác của người dùng.

Việc sử dụng mật khẩu yếu một cách đáng báo động có thể dễ dàng được minh họa. Một số cuộc tấn công gần đây đã dẫn đến hàng trăm triệu mật khẩu người dùng bị đánh cắp, nhiều trong số đó sau đó đã được đăng trên Internet. Một phân tích về một vụ trộm 32 triệu mật khẩu người dùng cho thấy 30% người dùng đã tạo mật khẩu chỉ gồm năm hoặc sáu ký tự, trong khi chỉ 12% mật khẩu người dùng có độ dài chín ký tự, vẫn được coi là quá ngắn để có hiệu quả. Gần một trong năm người dùng đã tạo một mật khẩu thuộc top 5.000 mật khẩu phổ biến nhất, bao gồm tên, từ lóng, từ điển, hoặc các mật khẩu tầm thường (chữ số liên tiếp, các phím liền kề trên bàn phím, v.v.). 10 mật khẩu phổ biến nhất được tìm thấy và số lần xuất hiện của chúng được liệt kê trong Bảng 1-1.

Bảng 1-1 Mười mật khẩu phổ biến nhất

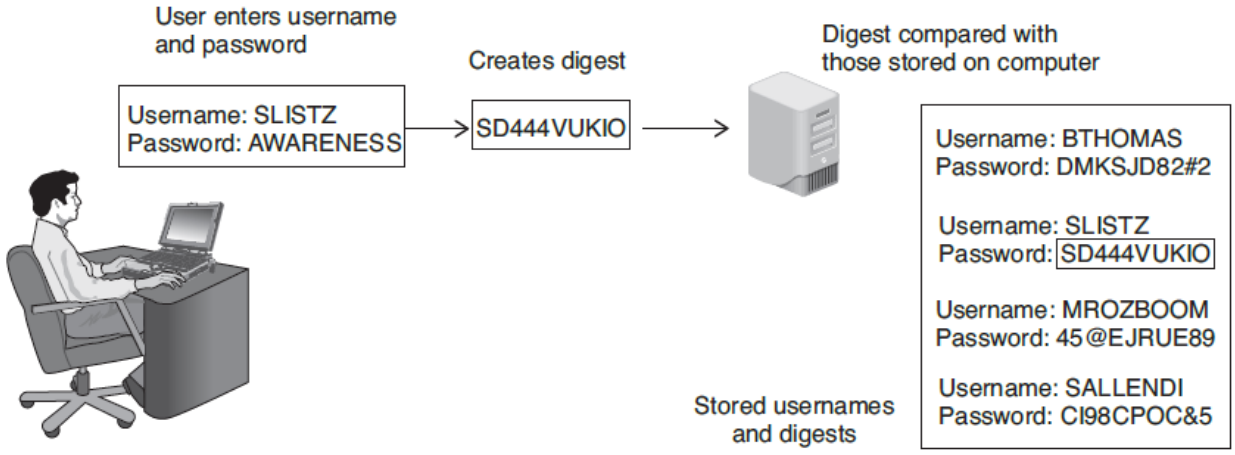
Hạng	Mật khẩu	Số người dùng với mật khẩu
1	123456	290.731
2	12345	79.078
3	123456789	76.790
4	Password	61.958

5	iloveyou	51.622
6	princess	35.231
7	rockyou	22.588
8	1234567	21.726
9	12345678	20.553
10	abc123	17.542

Tấn Công vào Mật Khẩu

Có nhiều loại tấn công có thể được sử dụng để khám phá mật khẩu. Một kỹ thuật tấn công không được sử dụng là **online guessing** (đoán trực tuyến) trong đó kẻ tấn công cố gắng đoán mật khẩu một cách ngẫu nhiên bằng cách gõ các biến thể khác nhau vào ô đăng nhập mật khẩu. Hầu hết các tài khoản đều được cài đặt để vô hiệu hóa tất cả các lần đăng nhập sau một số lần thử sai giới hạn (chẳng hạn như năm lần), do đó khóa kẻ tấn công. Và ngay cả khi kẻ tấn công có số lần thử không giới hạn, vẫn sẽ mất một khoảng thời gian không hợp lý để thử tất cả các tổ hợp khác nhau để đoán đúng mật khẩu.

Vì những hạn chế của đoán trực tuyến, hầu hết các cuộc tấn công mật khẩu ngày nay đều sử dụng **offline cracking** (bẻ khóa ngoại tuyến). Khi mật khẩu lần đầu tiên được người dùng tạo, thông thường một biểu diễn kỹ thuật số của mật khẩu đó được tạo và lưu trữ trên máy tính hoặc trang web (nói về mặt kỹ thuật, quá trình tạo biểu diễn kỹ thuật số này dựa trên một **hash algorithm**, tạo ra một **digest**). Ví dụ, mã hóa (digest) cho mật khẩu jurghbtref có thể được tính toán là 38e6b7cb3b7e66777c625fade02736e9 và sau đó được lưu trữ trên máy tính hoặc trang web. Khi người dùng sau đó nhập lại mật khẩu của mình để đăng nhập, cùng một thuật toán băm sẽ được áp dụng cho những gì cô ấy vừa gõ vào ô đăng nhập mật khẩu và sau đó so sánh với phiên bản đã lưu trữ; nếu khớp, người dùng sẽ được chấp thuận. Điều này được minh họa trong Hình 1-1.

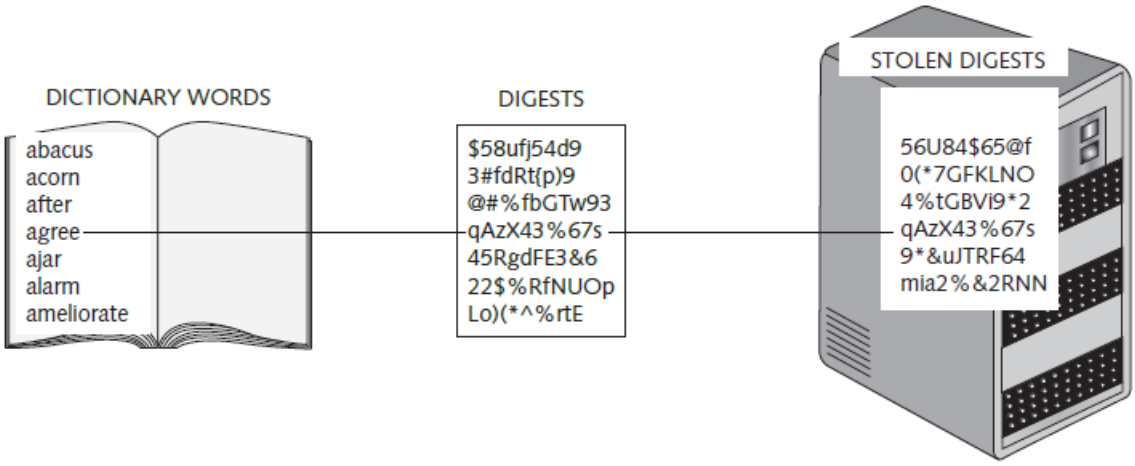


Hình 1-1 So sánh mật khẩu

Với bẻ khóa ngoại tuyến, kẻ tấn công đánh cắp tệp mã hóa mật khẩu và sau đó sử dụng các máy tính mạnh mẽ của riêng chúng để phá vỡ mật khẩu. Kẻ tấn công làm điều này bằng cách đầu tiên tạo mật khẩu của riêng chúng và sau đó tạo các mã hóa (được gọi là **candidates**) cho các mật khẩu này. Sau đó, chúng so sánh các mã hóa của mình với các mã hóa bị đánh cắp: khi các mã hóa khớp nhau, kẻ tấn công sẽ biết mật khẩu đằng sau mã hóa đó.

Một số kỹ thuật bẻ khóa ngoại tuyến cố gắng khớp mã hóa mật khẩu ứng viên đã biết với các mã hóa bị đánh cắp. Trong một **automated brute force attack** (tấn công vét cạn tự động), mọi tổ hợp chữ cái, số và ký tự có thể được sử dụng để tạo mã hóa ứng viên và sau đó được khớp với các mã hóa trong tệp mã hóa bị đánh cắp. Đây là phương pháp chậm nhất nhưng kỹ lưỡng nhất. Sử dụng chương trình tấn công vét cạn tự động, kẻ tấn công nhập vào chương trình các tham số như **password length** (độ dài mật khẩu – độ dài tối thiểu và tối đa của mật khẩu cần tạo, chẳng hạn như từ 1 đến 45), **character set** (tập hợp các chữ cái, ký hiệu và ký tự tạo nên mật khẩu), **language** (ngôn ngữ – chẳng hạn như tiếng Ả Rập, Hà Lan, Anh, Pháp, Đức, Ý, Bồ Đào Nha, Nga, hoặc Tây Ban Nha), **mask** (mặt nạ – nếu một phần của mật khẩu đã biết, một mẫu có thể được nhập để giảm số lượng mật khẩu được tạo ra, chẳng hạn như nếu hai chữ cái đầu tiên của mật khẩu sáu ký tự được biết là sk, mẫu có thể là sk????), và **skips** (bỏ qua – vì hầu hết các mật khẩu là tổ hợp từ giống như chữ, các chương trình có thể được đặt để bỏ qua các tổ hợp ký tự vô nghĩa (wqrghea) để chỉ tạo ra các mật khẩu như elmosworld và carkeys).

Một cuộc tấn công mật khẩu phổ biến khác là **dictionary attack** (tấn công từ điển). Một cuộc tấn công từ điển bắt đầu bằng việc kẻ tấn công tạo các mã hóa của các từ điển thông thường làm ứng viên và sau đó so sánh chúng với các mã hóa trong tệp mã hóa bị đánh cắp. Một cuộc tấn công từ điển được thể hiện trong Hình 2-2.



Hình 1-2 Tấn công từ điển

Tuy nhiên, một khoảnh khắc bước ngoặt trong các cuộc tấn công mật khẩu đã xảy ra vào cuối năm 2009. Một kẻ tấn công đã đột nhập vào một máy chủ thuộc về một nhà phát triển của một số ứng dụng mạng xã hội phổ biến. Máy chủ này chứa hơn 32 triệu mật khẩu người dùng, tất cả đều ở dạng văn bản thuần túy (không phải mã hóa). Những mật khẩu này sau đó đã được đăng trên Internet.

Kẻ tấn công đã tận dụng cơ hội này để kiểm tra các mật khẩu người dùng thực tế. Những mật khẩu này đã cung cấp hai yếu tố quan trọng cho các cuộc tấn công mật khẩu. Thứ nhất, bộ sưu tập mật khẩu "kho báu" này đã cung cấp cho kẻ tấn công, lần đầu tiên, một kho tàng lớn các mật khẩu trong thế giới thực. Bởi vì người dùng lặp lại mật khẩu của họ trên nhiều tài khoản, kẻ tấn công giờ đây có thể sử dụng những mật khẩu này làm mật khẩu ứng viên trong các cuộc tấn công của chúng. Ước tính có hơn hàng trăm triệu mật khẩu đã bị đánh cắp và công bố trực tuyến chỉ trong một năm. Các trang web hiện lưu trữ danh sách các mật khẩu bị rò rỉ này cùng với phân tích thống kê mà kẻ tấn công có thể sử dụng.

Ngoài ra, các bộ sưu tập mật khẩu này đã cung cấp cho kẻ tấn công cái nhìn sâu sắc về tư duy chiến lược của người dùng khi tạo mật khẩu. Ví dụ, trong những trường hợp người dùng kết hợp chữ hoa và chữ thường trong mật khẩu, người dùng có xu hướng viết hoa ở đầu mật khẩu, giống như viết một câu. Tương tự, dấu câu và số có

nhiều khả năng xuất hiện ở cuối mật khẩu, cũng bắt chước cách viết câu thông thường. Và một tỷ lệ cao các mật khẩu bao gồm một tên và ngày, chẳng hạn như Braden2008. Những hiểu biết như vậy có thể có giá trị đối với kẻ tấn công trong việc thiết kế một **mask** (mặt nạ) (chẳng hạn như ?dabcdef -2 ?l?u ?1?1?2?2?2?2?2) để bẻ khóa mật khẩu, vì sử dụng mặt nạ có thể giảm đáng kể thời gian cần thiết để bẻ khóa mật khẩu.

2. Tấn Công Sử Dụng Kỹ Thuật Xã Hội

Hãy xem xét các tình huống sau:

- **Email không mong muốn**. Một email không mong đợi đến từ một người bạn chứa một liên kết đến một trang web với hướng dẫn "Bạn nhất định phải xem cái này!" hoặc có một tệp đính kèm với tin nhắn, “Đây thực sự là ảnh của bạn sao?!?”
- **Lời cầu cứu khẩn cấp**. Một email từ người quen nói rằng cô ấy đang đi du lịch nước ngoài nhưng đã bị cướp và đánh đập. Cô ấy hiện đang hồi phục nhưng rất cần tiền, và cô ấy yêu cầu bạn chuyển tiền ngay lập tức vào tài khoản sau.
- **Tin nhắn cảnh báo**. Bạn nhận được một tin nhắn văn bản trên điện thoại nói rằng nó đến từ ngân hàng của bạn và bạn nên gọi ngay số điện thoại sau. Khi gọi, bạn nghe một tin nhắn tự động nói, “Một tin nhắn văn bản đã được gửi để thông báo rằng thẻ ghi nợ của bạn đã bị giới hạn do vấn đề bảo mật. Để kích hoạt lại, vui lòng nhấn phím 1 ngay bây giờ.” Sau khi nhấn phím 1, bạn sẽ được nhắc nhập bốn chữ số cuối của số An sinh xã hội của mình, và sau đó là số thẻ đầy đủ và ngày hết hạn của thẻ ghi nợ của bạn.
- **Video thảm họa**. Sau một trận lũ lụt gần đây, bạn tìm kiếm trên Internet thông tin về cách quyên góp cho các nạn nhân. Một trang web trông chuyên nghiệp chứa một video có thông tin về thảm họa và cách bạn có thể giúp đỡ, và thông báo cho bạn tải xuống một video và phát nó trên máy tính của bạn.

Mỗi tình huống thực tế này đều sử dụng thủ đoạn để thuyết phục nạn nhân nhanh chóng thực hiện một hành động rủi ro có thể dẫn đến một cuộc tấn công thành công, như được hiển thị trong Bảng 1-2. Điều này được gọi là **social engineering** (kỹ thuật xã hội), hay một phương tiện thao túng người dùng để thực hiện một hành động hoặc thu thập thông tin bí mật mà sau đó kẻ tấn công có thể sử dụng. Không giống như hầu hết các loại tấn công, kỹ thuật xã hội không dựa trực tiếp vào công nghệ, mà thay vào đó dựa vào hành động của nạn nhân.

Bảng 1-2 Các cuộc tấn công kỹ thuật xã hội

Tình huống	Hành động được yêu cầu thực hiện	Kết quả tiềm năng
Email không mong muốn	Nhấp vào liên kết hoặc mở tệp đính kèm	Máy tính có thể bị nhiễm phần mềm độc hại
Lời cầu cứu khẩn cấp	Gửi tiền vào tài khoản	Tiền được gửi đến tài khoản của kẻ tấn công
Tin nhắn cảnh báo	Cung cấp thông tin thẻ ngân hàng	Kẻ tấn công hiện có thông tin thẻ
Video thảm họa	Tải video về máy tính	Video đã tải xuống có thể chứa phần mềm độc hại

Về bản chất, kỹ thuật xã hội dựa vào sự thao túng khéo léo của kẻ tấn công đối với bản chất con người để thuyết phục nạn nhân cung cấp thông tin hoặc thực hiện hành động. Một số "nguyên tắc" cơ bản hoặc lý do khiến loại kỹ thuật xã hội này có hiệu quả. Những điều này được liệt kê trong Bảng 1-3 với ví dụ về một kẻ tấn công giả vờ là giám đốc điều hành (CEO) gọi đến bàn trợ giúp của tổ chức để yêu cầu đặt lại mật khẩu.

Bảng 1-3 Hiệu quả của kỹ thuật xã hội

Nguyên tắc	Mô tả	Ví dụ
Quyền uy	Bị chỉ đạo bởi người giả danh nhân vật có quyền uy hoặc viện dẫn sai quyền uy của họ	"Tôi là CEO đây."
Đe dọa	Để đe dọa và ép buộc bằng lời đe dọa	"Nếu bạn không đặt lại mật khẩu của tôi, tôi sẽ gọi cho cấp trên của bạn."
Đồng thuận/Bằng chứng xã hội	Bị ảnh hưởng bởi những gì người khác làm	"Tôi đã gọi tuần trước và đồng nghiệp của bạn đã đặt lại mật khẩu của tôi."
Khan hiếm	Có thứ gì đó đang thiếu hụt	"Tôi không thể lãng phí thời gian ở đây."
Khẩn cấp	Cần hành động ngay lập tức	"Cuộc họp với ban giám đốc của tôi bắt đầu sau 5 phút."
Sự quen	Nạn nhân được biết đến và được	"Tôi nhớ đã đọc một đánh giá

thuộc/Mến mộ	đón nhận nồng nhiệt	tốt về bạn."
Niềm tin	Sự tin cậy	"Bạn biết tôi là ai."

Các cuộc tấn công kỹ thuật xã hội bao gồm **phishing** (lừa đảo trực tuyến), **typo squatting** (đánh máy sai), **pretexting** (giả mạo tình huống), **hoaxes** (tin giả), **dumpster diving** (bới thùng rác) và **shoulder surfing** (nhìn trộm).

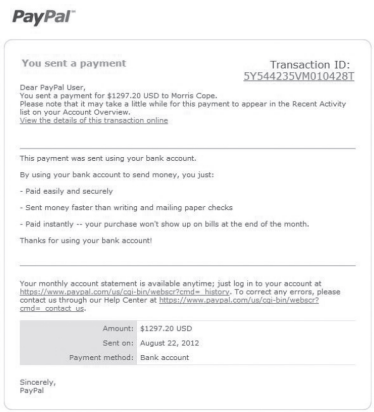
Phishing

Một trong những hình thức kỹ thuật xã hội phổ biến nhất là **phishing**. Phishing là việc gửi email hoặc hiển thị một thông báo web giả mạo đến từ một doanh nghiệp hợp pháp nhằm lừa người dùng tiết lộ thông tin cá nhân. Người dùng được yêu cầu trả lời email hoặc được dẫn đến một trang web nơi họ được yêu cầu cập nhật thông tin cá nhân, như mật khẩu, số thẻ tín dụng, số An sinh xã hội, số tài khoản ngân hàng hoặc thông tin khác. Tuy nhiên, email hoặc trang web đó thực chất là một trang giả mạo được thiết lập để đánh cắp thông tin mà người dùng nhập vào.

LƯU Ý

Từ "phishing" là một biến thể của từ "fishing" (câu cá), với ý tưởng là ném mồi ra ngoài biết rằng mặc dù hầu hết sẽ bỏ qua, nhưng một số sẽ "cắn câu".

Một trong những lý do khiến phishing thành công là các email và trang web giả mạo trông có vẻ hợp pháp. Hình 1-3 minh họa một tin nhắn email phishing thực tế tuyên bố nạn nhân gần đây đã thực hiện một khoản thanh toán lớn cho một cá nhân. Tin nhắn chứa logo, bảng màu và cách diễn đạt được sử dụng bởi trang web hợp pháp để nó trông giống như thật. Nạn nhân đương nhiên sẽ bối rối bởi tin nhắn này và nhấp vào các liên kết, sau đó sẽ yêu cầu tên người dùng và mật khẩu để đăng nhập, nhưng thay vì truy cập một trang web hợp pháp, thông tin này sẽ bị kẻ tấn công thu thập.


PayPal

You sent a payment

Transaction ID: 5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely
- Sent money faster than writing and mailing paper checks
- Paid instantly -- your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

Amount:	$1297.20 USD
Sent on:	August 22, 2012
Payment method:	Bank account

Sincerely,
PayPal

Hình 1-3 Tin nhắn email lừa đảo

Nguồn: PayPal

Một số biến thể của các cuộc tấn công lừa đảo bao gồm:

- **Spear phishing**. Trong khi phishing liên quan đến việc gửi hàng triệu tin nhắn email chung chung cho người dùng, **spear phishing** chỉ nhắm mục tiêu vào những người dùng cụ thể. Các email được sử dụng trong spear phishing được tùy chỉnh cho người nhận, bao gồm tên và thông tin cá nhân của họ, để làm cho tin nhắn trông có vẻ hợp pháp.
- **Whaling**. Một loại spear phishing là **whaling**. Thay vì nhắm vào "những con cá nhỏ", whaling nhắm mục tiêu vào "những con cá lớn", cụ thể là những cá nhân giàu có hoặc các giám đốc điều hành cấp cao trong một doanh nghiệp thường có số tiền lớn hơn trong tài khoản ngân hàng mà kẻ tấn công có thể truy cập nếu cuộc tấn công thành công. Bằng cách tập trung vào nhóm nhỏ hơn này, kẻ tấn công có thể đầu tư nhiều thời gian hơn vào cuộc tấn công và điều chỉnh thông điệp một cách tinh vi để đạt được khả năng thành công cao nhất.
- **Vishing**. Thay vì sử dụng email để liên hệ với nạn nhân tiềm năng, một cuộc gọi điện thoại có thể được sử dụng thay thế. Được gọi là **vishing** (voice phishing), kẻ tấn công gọi cho nạn nhân, người trả lời và nghe một tin nhắn ghi âm giả vờ đến từ ngân hàng của người dùng nói rằng thẻ tín dụng của cô ấy đã có hoạt động gian lận hoặc tài khoản ngân hàng của cô ấy có hoạt động bất thường. Nạn nhân được hướng dẫn gọi đến một số điện thoại cụ thể ngay lập tức (số này đã được kẻ tấn công thiết lập). Khi nạn nhân gọi, một tin nhắn tự động trả lời yêu cầu cô ấy nhập số thẻ tín dụng, số tài khoản ngân hàng, số An sinh xã hội hoặc thông tin khác trên bàn phím điện thoại.

Typo Squatting

Điều gì sẽ xảy ra khi người dùng gõ sai khi nhập địa chỉ URL (uniform resource locator) vào trình duyệt web, chẳng hạn như gõ goggle.com (sai chính tả) hoặc google.net (tên miền không chính xác) thay vì google.com đúng? Thông thường nhất, người dùng sẽ được chuyển hướng đến một trang web giả mạo trông giống hệt. Trang web này có thể chứa một khảo sát khách truy cập hứa hẹn cơ hội giành giải thưởng (nhưng kẻ tấn công thực sự thu thập các địa chỉ email đã nhập để bán cho những kẻ

gửi thư rác) hoặc chứa đầy quảng cáo (mà kẻ tấn công nhận tiền từ lưu lượng truy cập được tạo ra cho trang web). Các trang web giả mạo này tồn tại vì kẻ tấn công mua các tên miền có cách viết tương tự với các trang web thực tế. Điều này được gọi là **typo squatting** (còn gọi là **URL hijacking**). Một trang web nổi tiếng như google.com có thể phải đối phó với hơn 1.000 tên miền typo squatting. Hơn 62% tên miền hoạt động dựa trên các lỗi chính tả phổ biến của facebook.com là các trang web typo squatting.

Trong khi lỗi đánh máy khi nhập URL để truy cập một trang web có thể là một vấn đề, một vấn đề lớn hơn nữa là việc kẻ tấn công cũng nhận được tất cả các tin nhắn email riêng tư có lỗi đánh máy tương tự (chẳng hạn như email gửi đến finances@goggle.com). Các nhà nghiên cứu bảo mật đã thiết lập các tên miền giả mạo dựa trên tên của 500 công ty lớn nhất Hoa Kỳ mà chỉ bỏ sót dấu chấm giữa tên miền và tên miền phụ. Trong sáu tháng, họ đã nhận được hơn 120.000 email riêng tư (hoặc 20 gigabyte email) dựa trên lỗi đánh máy này, nhiều email trong số đó chứa thông tin bí mật và thậm chí cả danh sách mật khẩu.[7]

Pretexting

Social engineering pretexting là việc tạo ra một kịch bản bịa đặt (**pretext**) để thuyết phục nạn nhân thực hiện một hành động hoặc cung cấp thông tin bí mật. Mặc dù liên quan đến việc nói dối, pretexting được coi là nhiều hơn chỉ là tạo ra một lời nói dối; nó có thể tạo ra một danh tính hoàn toàn mới để sử dụng trong cuộc tấn công.

Những kẻ giả mạo sử dụng các chiến thuật khác nhau để thu thập thông tin. Trong một ví dụ, một kẻ giả mạo có thể gọi một người và tự xưng là từ một công ty thực hiện các cuộc khảo sát để hỏi một loạt các câu hỏi có vẻ vô hại. Sau khi kết thúc cuộc gọi đó, kẻ giả mạo lại gọi đến một công ty mà người đó đang kinh doanh. Kẻ giả mạo sau đó tự xưng là người đó và giả vờ rằng mình đã quên số tài khoản hoặc cần thông tin về lịch sử tài khoản của mình. Thông qua cuộc tấn công kỹ thuật xã hội này, kẻ giả mạo có thể thu thập thông tin cá nhân về nạn nhân như Số An sinh xã hội, số tài khoản ngân hàng và thẻ tín dụng, thông tin báo cáo tín dụng và quy mô danh mục đầu tư tiết kiệm và đầu tư.

Hoaxes

Kẻ tấn công có thể sử dụng các **hoaxes** (tin giả) làm bước đầu tiên trong một cuộc tấn công. Hoax là một cảnh báo sai, thường nằm trong một tin nhắn email tuyên

bố đến từ bộ phận công nghệ thông tin (IT). Hoax tuyên bố có một "virus chết người" đang lưu hành trên Internet và rằng người nhận nên xóa các tệp cụ thể hoặc thay đổi cấu hình bảo mật, sau đó chuyển tiếp tin nhắn cho những người dùng khác. Tuy nhiên, việc thay đổi cấu hình có thể cho phép kẻ tấn công xâm phạm hệ thống. Hoặc, việc xóa tệp có thể làm máy tính không ổn định, khiến nạn nhân phải gọi số điện thoại trong tin nhắn email hoax để được giúp đỡ, mà đó thực ra là số điện thoại của kẻ tấn công.

Dumpster Diving

Dumpster diving (bới thùng rác) liên quan đến việc lục lọi các thùng rác để tìm thông tin có thể hữu ích trong một cuộc tấn công. Bảng 1-4 liệt kê các mục khác nhau có thể được lấy từ một doanh nghiệp – nhiều trong số đó dường như vô dụng – và cách chúng có thể được sử dụng.

Bảng 1-4 Các vật dụng có được từ dumpster diving và tính hữu ích của chúng

Mục tìm thấy	Tại sao hữu ích
Lịch	Lịch có thể tiết lộ nhân viên nào vắng mặt vào thời điểm cụ thể.
Phần cứng máy tính không đắt tiền, như ổ đĩa USB hoặc ổ cứng di động	Những thiết bị này thường được xử lý không đúng cách và có thể chứa thông tin có giá trị.
Bản ghi nhớ	Những bản ghi nhớ dường như không quan trọng có thể cung cấp những thông tin nhỏ hữu ích cho kẻ tấn công đang xây dựng một nhân vật mạo danh.
Sơ đồ tổ chức	Xác định các cá nhân trong tổ chức có vị trí quyền lực.
Danh bạ điện thoại	Danh bạ điện thoại có thể cung cấp tên và số điện thoại của các cá nhân trong tổ chức để nhắm mục tiêu hoặc mạo danh.
Sổ tay chính sách	Những cuốn này có thể tiết lộ mức độ bảo mật thực sự trong tổ chức.
Sổ tay hệ thống	Sổ tay hệ thống có thể cho kẻ tấn công biết loại hệ thống máy tính đang được sử dụng để có thể thực hiện nghiên cứu khác nhằm xác định các lỗ hổng.

Dumpster diving không chỉ giới hạn trong kinh doanh. Kẻ tấn công thường lục lọi thùng rác của chủ nhà để đánh cắp các thư mời thẻ tín dụng đã được phê duyệt

trước, các tài liệu chứa số An sinh xã hội, địa chỉ email, thông tin tài khoản ngân hàng và lịch sử việc làm – tất cả đều có thể được sử dụng trong các cuộc tấn công.

Shoulder Surfing

Hãy xem xét kịch bản này: Một người đàn ông bước đến một máy rút tiền tự động (ATM) nằm trên một con phố đông đúc ở trung tâm thành phố để gửi tiền. Sau khi đưa thẻ ATM vào, máy yêu cầu anh ta nhập mã số nhận dạng cá nhân (PIN) trên bàn phím. Khi anh ta gõ bốn chữ số, anh ta nhận thấy một phụ nữ trẻ đã bước đến phía sau anh ta và đang chờ sử dụng ATM. Khi người đàn ông điều hướng qua các menu, người phụ nữ bắt đầu lẩm bẩm, "Nhanh lên, nhanh lên, nhanh lên. Tôi phải đi rồi!" Bị bối rối vì sự thiếu kiên nhẫn của người phụ nữ, người đàn ông nhấp vào một tùy chọn menu không chính xác và sau đó phải quay lại qua một vài tùy chọn bổ sung. Người phụ nữ thở dài lớn tiếng và sau đó nói, "Anh sắp xong chưa?" Người đàn ông vội vàng hoàn thành giao dịch gửi tiền, lấy biên lai và thẻ của mình, rồi nhanh chóng bỏ đi. Tối hôm đó, khi về nhà, anh ta kiểm tra tài khoản ngân hàng trực tuyến của mình và phát hiện ra năm lần rút tiền mặt từ tài khoản của mình đã xảy ra tại cùng một máy ATM với số tiền 200 đô la, 100 đô la, 200 đô la, 100 đô la và 200 đô la, tất cả đều trong vòng một phút kể từ giao dịch ban đầu của anh ta.

Người đàn ông này là nạn nhân của **shoulder surfing** (nhìn trộm), trong đó thông tin được nhập được quan sát bởi một người khác. Trong sự cố này, sau khi người đàn ông hoàn thành giao dịch tại ATM, thông báo "Bạn có muốn thực hiện một giao dịch khác không?" xuất hiện trên màn hình. Bởi vì anh ta đã có thẻ và biên lai của mình, người đàn ông chỉ cần bỏ đi. Tuy nhiên, câu hỏi vẫn còn trên màn hình đủ lâu để người phụ nữ đứng sau anh ta chạm vào phím "CÓ" và nhập lại PIN của anh ta, mà cô ta đã nhìn thấy anh ta nhập. Điều này đã cho cô ta cơ hội thực hiện các lần rút tiền từ tài khoản của anh ta.

Shoulder surfing có thể được thực hiện ở hầu hết mọi địa điểm công cộng nơi một cá nhân được yêu cầu nhập thông tin nhận dạng cá nhân. Điều này bao gồm việc nhập PIN tại ATM, hoàn thành giao dịch mua hàng tại cửa hàng bằng cách nhập PIN thẻ ghi nợ tại quầy thanh toán, viết số An sinh xã hội trên một mẫu giấy hoặc nhập mật khẩu trên bàn phím máy tính tại một quán cà phê hoặc sân bay. Việc quan sát những gì được nhập có thể được thực hiện từ khoảng cách lên đến 15 feet (4,5 mét). Các kỹ

thuật tinh vi hơn bao gồm sử dụng ống nhòm (như trong một toa tàu hoặc nhà ga sân bay lớn) hoặc sử dụng camera truyền hình nhỏ được giấu trong sách hoặc ba lô.

3. Đánh cắp dữ liệu

Chúng ta sẽ tìm hiểu về một trong những mối đe dọa phổ biến và nguy hiểm nhất trong thế giới số hiện nay – đó là đánh **cắp dữ liệu**.

Trộm cắp dữ liệu không phải là chuyện gì quá xa lạ. Nó có thể xảy ra trong nội bộ công ty, qua mạng internet, thậm chí là từ chiếc điện thoại cá nhân của bạn. Điều quan trọng là chúng ta cần hiểu rõ: dữ liệu gì đang bị đánh cắp, ai đang đánh cắp, và họ sử dụng nó vào mục đích gì.

Trước hết, **cần biết dữ liệu nào đang bị đánh cắp**. Không phải lúc nào trộm cắp dữ liệu cũng nhắm vào tài liệu tuyệt mật hay hồ sơ lớn. Có khi chỉ là thông tin cá nhân, danh sách khách hàng, địa chỉ email, lịch sử mua sắm, hay đơn giản là thông tin đăng nhập. Những dữ liệu tưởng chừng nhỏ nhặt này, nếu bị khai thác, vẫn có thể gây thiệt hại nghiêm trọng.

Ví dụ, một tên trộm chỉ cần lấy được địa chỉ email và mật khẩu của bạn ở một trang mua sắm, rồi thử dùng nó để đăng nhập vào tài khoản ngân hàng, mạng xã hội hoặc email công việc. Nếu bạn dùng chung mật khẩu, rủi ro là cực kỳ lớn.

Tiếp theo, chúng ta phải hiểu **dữ liệu bị đánh cắp bằng cách nào**. Có nhiều phương pháp – từ các phần mềm gián điệp, keylogger, email lừa đảo, cho đến việc tấn công vào hệ thống lưu trữ dữ liệu. Thậm chí, việc để lộ thiết bị không được mã hóa, như USB hoặc laptop, cũng có thể dẫn đến mất dữ liệu.

Ngoài ra, nhiều cuộc tấn công lợi dụng **sơ hở từ phía con người**. Một nhân viên gửi nhầm tệp dữ liệu nhạy cảm, hay lưu trữ tài liệu quan trọng ở nơi không an toàn, cũng đủ để kẻ xấu khai thác.

Điểm tiếp theo là **xác định ai là kẻ trộm dữ liệu**. Không phải lúc nào cũng là hacker từ xa. Đôi khi, chính những người bên trong tổ chức – nhân viên cũ, nhân viên bất mãn, hoặc đối tác có quyền truy cập hệ thống – mới là mối nguy lớn nhất.

Ngoài ra, tội phạm mạng chuyên nghiệp cũng rất nguy hiểm. Họ hoạt động theo nhóm, có công cụ tinh vi, và có thể mua bán dữ liệu trên chợ đen một cách kín đáo mà không để lại dấu vết rõ ràng.

Rồi, khi dữ liệu bị đánh cắp, điều quan trọng là **hiểu rõ rủi ro mà người dùng phải đối mặt**. Với dữ liệu cá nhân, nguy cơ là bị mạo danh, bị lừa đảo tài chính, hoặc bị sử dụng để mở tài khoản giả. Với dữ liệu doanh nghiệp, nguy cơ có thể là mất uy tín, rò rỉ chiến lược kinh doanh, hoặc thậm chí là thiệt hại tài chính lớn do khách hàng mất niềm tin.

Một rò rỉ nhỏ – ví dụ như danh sách khách hàng bị công bố – cũng đủ để gây ảnh hưởng nghiêm trọng đến một doanh nghiệp, đặc biệt trong những lĩnh vực như tài chính, y tế, hay công nghệ.

Cuối cùng, chúng ta cần biết **dữ liệu bị đánh cắp được sử dụng vào những mục đích gì**. Có thể là để **bán kiếm lời**, đặc biệt là các thông tin như số thẻ tín dụng, dữ liệu định danh, hay hồ sơ y tế. Cũng có thể là để **tống tiền** – ví dụ như các vụ ransomware, nơi kẻ tấn công mã hóa toàn bộ dữ liệu và yêu cầu doanh nghiệp trả tiền để chuộc lại.

Ngoài ra, trong một số trường hợp, dữ liệu còn được dùng để **gián điệp công nghiệp** hoặc **chiến tranh mạng** – nghĩa là phục vụ cho các mục đích chính trị, thương mại, hay gây ảnh hưởng đến đối thủ.

Tóm lại, trộm cắp dữ liệu không chỉ là hành động đơn lẻ, mà là một chuỗi các nguy cơ liên quan đến công nghệ, con người và cả mục đích khai thác sau đó. Khi chúng ta hiểu rõ dữ liệu nào có giá trị, ai có thể nhắm đến, và họ dùng nó ra sao, thì chúng ta mới có thể xây dựng được các biện pháp bảo vệ hiệu quả và phù hợp.

Trộm Cắp Danh Tính

Identity theft (trộm cắp danh tính) liên quan đến việc sử dụng thông tin cá nhân của người khác, chẳng hạn như tên, số An sinh xã hội, hoặc số thẻ tín dụng, để thực hiện gian lận tài chính. Sử dụng thông tin này để có được thẻ tín dụng, thiết lập tài khoản điện thoại di động, hoặc thậm chí thuê một căn hộ, những kẻ trộm có thể tạo ra các khoản phí quá mức dưới tên nạn nhân. Nạn nhân bị tính phí cho các giao dịch mua và bị hỏng lịch sử tín dụng, điều này có thể là nguyên nhân khiến họ bị từ chối công việc mới hoặc các khoản vay cho trường học, ô tô và nhà ở.

Sau đây là một số hành động mà những kẻ trộm danh tính có thể thực hiện:

- Sản xuất séc giả hoặc thẻ ghi nợ giả và sau đó rút tất cả tiền từ tài khoản ngân hàng

- Thiết lập dịch vụ điện thoại hoặc không dây dưới tên nạn nhân
- Nộp đơn phá sản dưới tên người đó để tránh phải trả nợ hoặc tránh bị trục xuất
- Tiêu xài bằng cách sử dụng số tài khoản tín dụng và ghi nợ được lấy một cách gian lận để mua các mặt hàng đắt tiền như TV màn hình lớn có thể dễ dàng bán lại
- Mở một tài khoản ngân hàng dưới tên người đó và viết séc khống vào tài khoản đó
- Mở một tài khoản thẻ tín dụng mới, sử dụng tên, ngày sinh và số An sinh xã hội của nạn nhân trộm cắp danh tính. Khi kẻ trộm không trả các hóa đơn, tài khoản nợ quá hạn sẽ được báo cáo trên báo cáo tín dụng của nạn nhân.
- Lấy các khoản vay cho các mặt hàng đắt tiền như ô tô và xe máy

Bảng 1-5 tóm tắt một số cách mà kẻ tấn công có thể đánh cắp thông tin cá nhân.

Bảng 1-5 Cách kẻ tấn công đánh cắp thông tin cá nhân

Kỹ thuật	Giải thích
Dumpster diving	Các bản sao kê thẻ tín dụng, biên lai thanh toán và sao kê ngân hàng đã bị loại bỏ có thể được lấy để lấy thông tin cá nhân.
Phishing	Kẻ tấn công thuyết phục nạn nhân nhập thông tin cá nhân vào một trang web giả mạo sau khi nhận được một email giả mạo từ ngân hàng.
Thay đổi địa chỉ	Sử dụng mẫu đơn thay đổi địa chỉ tiêu chuẩn, kẻ tấn công chuyển tất cả thư đến hộp thư bưu điện của chúng để nạn nhân không bao giờ nhìn thấy các khoản phí đã tạo.
Pretexting	Một kẻ tấn công giả vờ là từ một công ty nghiên cứu hợp pháp để yêu cầu thông tin cá nhân.
Stealing	Ví và ví bị đánh cắp chứa thông tin cá nhân có thể được sử dụng để trộm cắp danh tính.

Một trong những lĩnh vực trộm cắp danh tính đang phát triển nhanh nhất liên quan đến việc những kẻ trộm danh tính nộp tờ khai thuế thu nhập giả mạo với Sở Thuế vụ Hoa Kỳ (IRS). Những kẻ trộm danh tính đánh cắp số An sinh xã hội của người nộp thuế sau đó sẽ nộp tờ khai thuế giả mạo yêu cầu một khoản hoàn thuế lớn – thường lớn hơn số tiền mà nạn nhân thực sự được hưởng – được gửi cho kẻ tấn công. Bởi vì IRS

đã gửi các khoản hoàn thuế nhanh hơn trong quá khứ, điều này đã giúp những kẻ trộm dễ dàng nhận được khoản hoàn thuế và sau đó biến mất trước khi nạn nhân nộp tờ khai hợp pháp và phát hiện ra gian lận. Theo IRS, họ đã cấp hơn 5,8 tỷ đô la các khoản hoàn thuế cho những kẻ trộm danh tính đã nộp tờ khai thuế gian lận vào năm 2013, mặc dù đã ngăn chặn khoảng 3 triệu tờ khai gian lận trong năm đó.

4. Bảo vệ quyền riêng tư

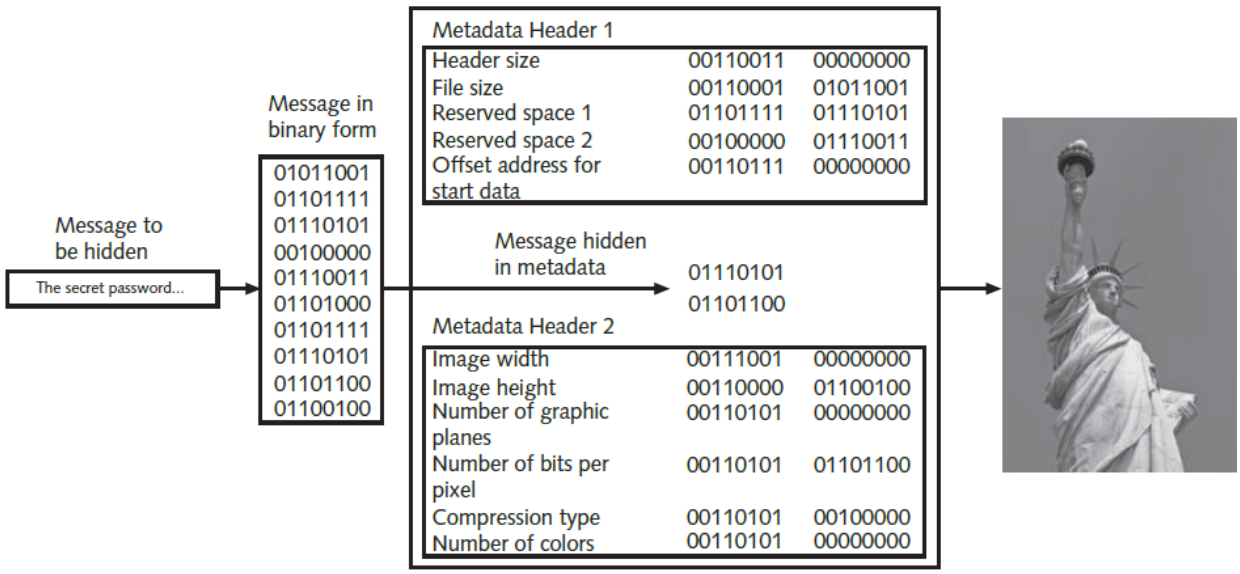
Ngày nay, hầu như không thể ngăn chặn việc thu thập và sử dụng tất cả dữ liệu riêng tư. Tuy nhiên, có một số biện pháp bảo vệ khác nhau có thể được thực hiện để giảm thiểu rủi ro liên quan đến dữ liệu riêng tư. Các biện pháp bảo vệ này bao gồm sử dụng mật mã học và tuân thủ các thực hành tốt nhất. Ngoài ra, các tổ chức thu thập dữ liệu riêng tư cũng có trách nhiệm.

Mật mã học

Việc định nghĩa mật mã học bao gồm việc hiểu nó là gì và nó có thể làm gì. Nó cũng bao gồm việc hiểu cách mật mã học có thể được sử dụng như một công cụ để bảo vệ dữ liệu.

Mật mã học là gì? Việc "xáo trộn" dữ liệu để không thể đọc được là một quá trình được gọi là mật mã học (từ tiếng Hy Lạp có nghĩa là chữ viết ẩn). Mật mã học là khoa học biến đổi thông tin thành một dạng an toàn để người không được ủy quyền không thể truy cập được.

Trong khi mật mã học xáo trộn một thông điệp để không thể hiểu được, thì kỹ thuật che giấu thông tin (steganography) lại ẩn đi sự tồn tại của dữ liệu. Một hình ảnh tưởng chừng vô hại có thể chứa dữ liệu ẩn, thường là một loại thông điệp nào đó, được nhúng trong hình ảnh. Steganography lấy dữ liệu, chia thành các phần nhỏ hơn và ẩn nó vào các phần không sử dụng của tệp, như thể hiện trong Hình 1-4. Steganography có thể ẩn dữ liệu trong các trường tiêu đề tệp mô tả tệp, giữa các phần của metadata (dữ liệu được sử dụng để mô tả nội dung hoặc cấu trúc của dữ liệu thực tế), hoặc trong các vùng của một tệp chứa chính nội dung. Kỹ thuật che giấu thông tin (Steganography) có thể sử dụng nhiều loại tệp khác nhau – tệp hình ảnh, tệp âm thanh, tệp video, v.v. – để ẩn thông điệp và dữ liệu.



Hình 1-4 Dữ liệu được ẩn bằng kỹ thuật che giấu thông tin

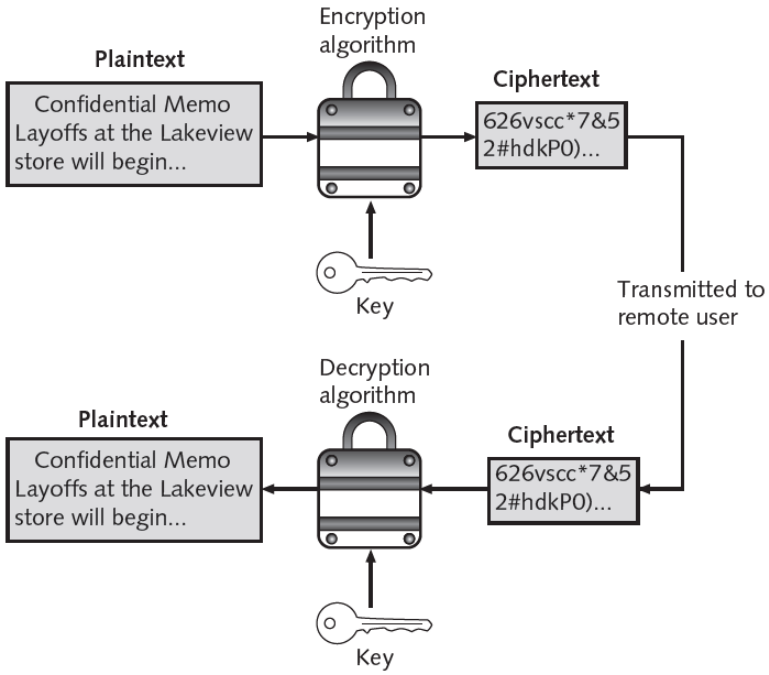
Nguồn gốc của mật mã học có từ hàng thế kỷ trước. Một trong những nhà mật mã học cổ đại nổi tiếng nhất là Julius Caesar. Trong các thông điệp gửi cho các chỉ huy của mình, Caesar đã dịch chuyển mỗi chữ cái trong thông điệp của mình ba vị trí xuống theo bảng chữ cái, sao cho chữ A được thay bằng chữ D, chữ B được thay bằng chữ E, v.v. Việc thay đổi văn bản gốc thành một thông điệp bí mật bằng cách sử dụng mật mã học được gọi là mã hóa. Khi các chỉ huy của Caesar nhận được thông điệp của ông, họ đã đảo ngược quá trình (chẳng hạn như thay thế chữ D bằng chữ A) để thay đổi thông điệp bí mật trở lại dạng ban đầu của nó. Điều này được gọi là giải mã.

Dữ liệu ở dạng không được mã hóa được gọi là dữ liệu cleartext. Dữ liệu cleartext là "rõ ràng" và do đó có thể hiển thị nguyên trạng, không cần giải mã. Dữ liệu plaintext là dữ liệu cleartext sẽ được mã hóa và cũng là kết quả của quá trình giải mã. Plaintext có thể được coi là một trường hợp đặc biệt của cleartext.

Plaintext không nên bị nhầm lẫn với "plain text." Plain text là văn bản không có định dạng (như in đậm hoặc gạch chân).

Dữ liệu plaintext được nhập vào một thuật toán mã hóa, bao gồm các thủ tục dựa trên công thức toán học được sử dụng để mã hóa và giải mã dữ liệu. Một khóa là một giá trị toán học được nhập vào thuật toán để tạo ra ciphertext, hay dữ liệu được mã hóa. Giống như việc một chiếc chìa khóa được đưa vào ổ khóa để khóa cửa, trong mật mã học, một khóa toán học duy nhất được nhập vào thuật toán mã hóa để "khóa" dữ liệu bằng cách tạo ra ciphertext. Khi ciphertext cần được trả về plaintext, quá trình

ngược lại sẽ xảy ra với một thuật toán giải mã và khóa. Quá trình mã hóa được minh họa trong Hình 1-5.



Hình 1-5 Quá trình mật mã học

Mật mã học và Quyền riêng tư Mật mã học có thể cung cấp bảo vệ quyền riêng tư cơ bản cho thông tin vì quyền truy cập vào các khóa có thể bị hạn chế. Mật mã học có thể cung cấp năm biện pháp bảo vệ cơ bản:

- **Bảo mật.** Mật mã học có thể bảo vệ tính bảo mật của thông tin bằng cách đảm bảo rằng chỉ các bên được ủy quyền mới có thể xem thông tin đó. Khi thông tin riêng tư, chẳng hạn như một tài liệu chứa thông tin tài chính của người dùng, được truyền qua Internet hoặc lưu trữ trên ổ đĩa USB, nội dung của nó có thể được mã hóa, điều này chỉ cho phép các cá nhân được ủy quyền có khóa mới có thể xem.
- **Toàn vẹn dữ liệu.** Mật mã học có thể bảo vệ tính toàn vẹn của thông tin. Tính toàn vẹn đảm bảo rằng thông tin là chính xác và không có người không được ủy quyền hoặc phần mềm độc hại nào đã thay đổi dữ liệu đó. Bởi vì ciphertext yêu cầu phải sử dụng khóa để mở dữ liệu trước khi nó có thể bị thay đổi, mật mã học có thể đảm bảo tính toàn vẹn của nó. Tài liệu
- của thông tin tài chính, ví dụ, có thể được bảo vệ để không có dữ liệu nào có thể được thêm hoặc xóa bởi nhân viên không được ủy quyền.

- **Tính sẵn có.** Mật mã học có thể giúp đảm bảo tính sẵn có của dữ liệu để người dùng được ủy quyền có khóa có thể truy cập. Thay vì lưu trữ một tệp quan trọng trên ổ cứng bị khóa trong két sắt để ngăn chặn truy cập trái phép, một tệp được mã hóa có thể được cung cấp ngay lập tức cho các cá nhân được ủy quyền đã được cung cấp khóa. Danh sách tài liệu dữ liệu tài chính có thể được lưu trữ trên máy tính và sẵn sàng cho chuyên gia tài chính xem xét vì cô ấy có khóa thuật toán.
- **Xác thực.** Việc xác thực người gửi có thể được xác minh thông qua mật mã học. Ví dụ, các loại mật mã học cụ thể có thể ngăn chặn tình huống như gửi yêu cầu đến một nhà hoạch định tài chính để rút tiền từ một tài khoản có vẻ như đến từ người dùng nhưng thực tế lại được gửi bởi một kẻ mạo danh.
- **Không từ chối.** Mật mã học có thể thực thi tính không từ chối. Từ chối được định nghĩa là sự phủ nhận; không từ chối là không thể phủ nhận, vì vậy không từ chối là quá trình chứng minh rằng người dùng đã thực hiện một hành động, chẳng hạn như gửi một tin nhắn email. Tính không từ chối ngăn chặn một cá nhân gian lận "nuốt lời" về một hành động. Các tính năng không từ chối của mật mã học có thể ngăn chặn một nhà quản lý tài chính tuyên bố rằng cô ấy chưa bao giờ gửi một bản sao giao dịch dữ liệu tài chính cho bên thứ ba không được ủy quyền.

Bảng 1-6 Các biện pháp bảo vệ thông tin bằng mật mã học

Đặc tính	**Mô tả**	**Bảo vệ**
Bảo mật	Đảm bảo chỉ các bên được ủy quyền mới có thể xem thông tin	Thông tin được mã hóa chỉ có thể được xem bởi những người đã được cung cấp khóa.
Toàn vẹn dữ liệu	Đảm bảo thông tin chính xác và không có người không được ủy quyền hoặc phần mềm độc hại nào đã thay đổi dữ liệu đó	Thông tin được mã hóa không thể thay đổi trừ bởi người dùng được ủy quyền có khóa.
Tính sẵn có	Đảm bảo dữ liệu có thể truy cập được đối với người dùng được ủy quyền	Người dùng được ủy quyền được cung cấp khóa giải mã để truy cập thông tin.
Xác thực	Cung cấp bằng chứng về tính xác thực của người dùng	Có thể thu được bằng chứng rằng người gửi là hợp pháp chứ không phải kẻ mạo danh.

Không từ chối	Chứng minh rằng người dùng đã thực hiện một hành động	Cá nhân bị ngăn chặn gian lận phủ nhận rằng họ đã tham gia vào một giao dịch.

Các loại thuật toán mật mã Có ba loại thuật toán mật mã chính. Đó là thuật toán băm (hash algorithms), thuật toán mật mã đối xứng (symmetric cryptographic algorithms) và thuật toán mật mã bất đối xứng (asymmetric cryptographic algorithms).

Thuật toán băm (Hash Algorithms) Loại thuật toán mật mã cơ bản nhất là thuật toán băm một chiều. Một thuật toán băm tạo ra một "dấu vân tay kỹ thuật số" duy nhất của một tập dữ liệu và thường được gọi là băm. Dấu vân tay này, được gọi là digest (đôi khi được gọi là message digest hoặc hash), đại diện cho nội dung. Mặc dù băm được coi là một thuật toán mật mã, nhưng mục đích của nó không phải là tạo ra ciphertext mà sau này có thể được giải mã. Thay vào đó, băm là "một chiều" ở chỗ nội dung của nó không thể được sử dụng để tiết lộ tập dữ liệu gốc. Băm được sử dụng chủ yếu cho mục đích so sánh.

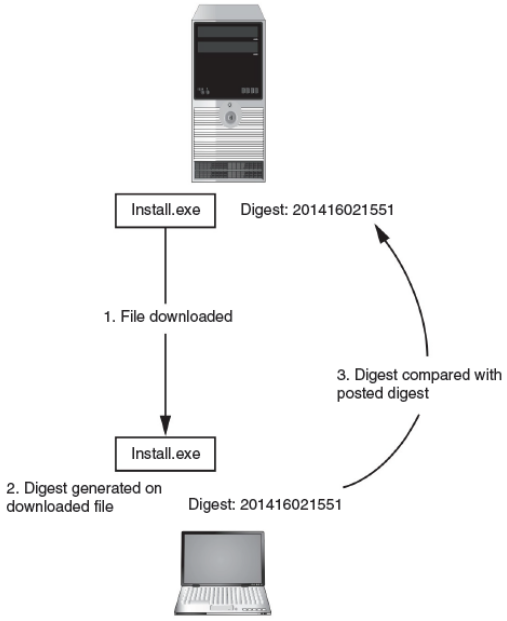
Một hash an toàn được tạo ra từ một tập dữ liệu không thể đảo ngược được. Ví dụ, nếu 12 nhân với 34 thì kết quả là 408. Nếu người dùng được yêu cầu xác định hai số được sử dụng để tạo ra số 408, thì không thể "làm ngược lại" và suy ra các số gốc với độ chắc chắn tuyệt đối vì có quá nhiều khả năng toán học (204 + 204, 204 × 2, 407 + 1, 102 × 4, 361 + 47, v.v.). Hashing cũng tương tự ở chỗ nó được sử dụng để tạo ra một giá trị, nhưng không thể xác định tập dữ liệu gốc.

Một thuật toán băm được coi là an toàn nếu nó có các đặc điểm sau:

- **Kích thước cố định.** Một digest của một tập dữ liệu ngắn nên tạo ra cùng kích thước với một digest của một tập dữ liệu dài. Ví dụ, một digest của chữ cái đơn 'a' là 86be7afa339d0fc7cf-c785e72f578d33, trong khi một digest của 1 triệu lần xuất hiện của chữ cái 'a' là 4a7f5723f954eba1216c9d8f6320431f, cùng độ dài.
- **Duy nhất.** Hai tập dữ liệu khác nhau không thể tạo ra cùng một digest, điều này được gọi là xung đột (collision). Việc thay đổi một chữ cái duy nhất trong một tập dữ liệu sẽ tạo ra một digest hoàn toàn khác. Ví dụ, một digest của Sunday là 0d716e73a2a7910bd4ae634-07056d79b, trong khi một digest của sunday (chữ 's' viết thường) là 3464eb71bd7a4377967a30-32#da798a1b54.

- **Nguyên bản.** Không thể tạo ra một tập dữ liệu có giá trị băm mong muốn hoặc được định nghĩa trước.
- **An toàn.** Giá trị băm tạo ra không thể đảo ngược để xác định plaintext gốc.

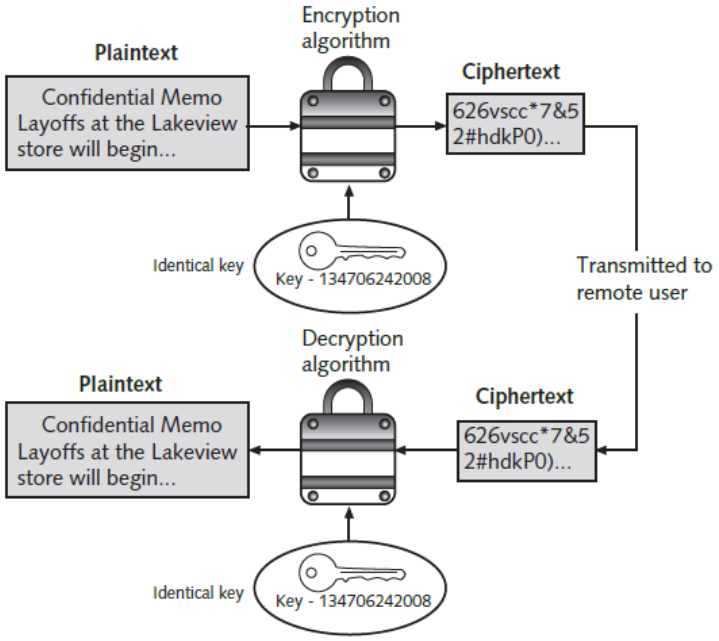
Hashing thường được sử dụng để xác định tính toàn vẹn của một thông điệp hoặc nội dung của một tệp. Trong trường hợp này, digest đóng vai trò là một kiểm tra để xác minh rằng nội dung gốc không bị thay đổi. Ví dụ, các giá trị digest thường được đăng trên các trang web để xác minh tính toàn vẹn của các tệp có thể tải xuống. Người dùng có thể tạo một digest trên một tệp sau khi đã tải xuống và sau đó so sánh giá trị đó với giá trị digest gốc được đăng trên trang web. Một sự trùng khớp cho thấy tính toàn vẹn của tệp đã được bảo toàn. Điều này được thể hiện trong Hình 1-6.



Hình 1-6 Xác minh tính toàn vẹn của tệp bằng digest

Thuật toán mật mã đối xứng Các thuật toán mật mã gốc để mã hóa và giải mã dữ liệu là thuật toán mật mã đối xứng. Thuật toán mật mã đối xứng sử dụng cùng một khóa duy nhất để mã hóa và giải mã tài liệu. Không giống như băm, trong đó hash không nhằm mục đích giải mã, thuật toán đối xứng được thiết kế để mã hóa và giải mã ciphertext. Dữ liệu được Alice mã hóa bằng thuật toán mật mã đối xứng sẽ được Bob giải mã khi nhận được. Do đó, điều cần thiết là khóa phải được giữ riêng tư (bí mật), vì nếu kẻ tấn công có được khóa, hắn có thể đọc tất cả các tài liệu được mã hóa. Vì lý do này, mã hóa đối xứng còn được gọi là khóa riêng tư mật mã học. Mã hóa đối xứng được minh họa trong Hình 1-7, nơi các khóa giống hệt nhau được sử dụng để mã hóa

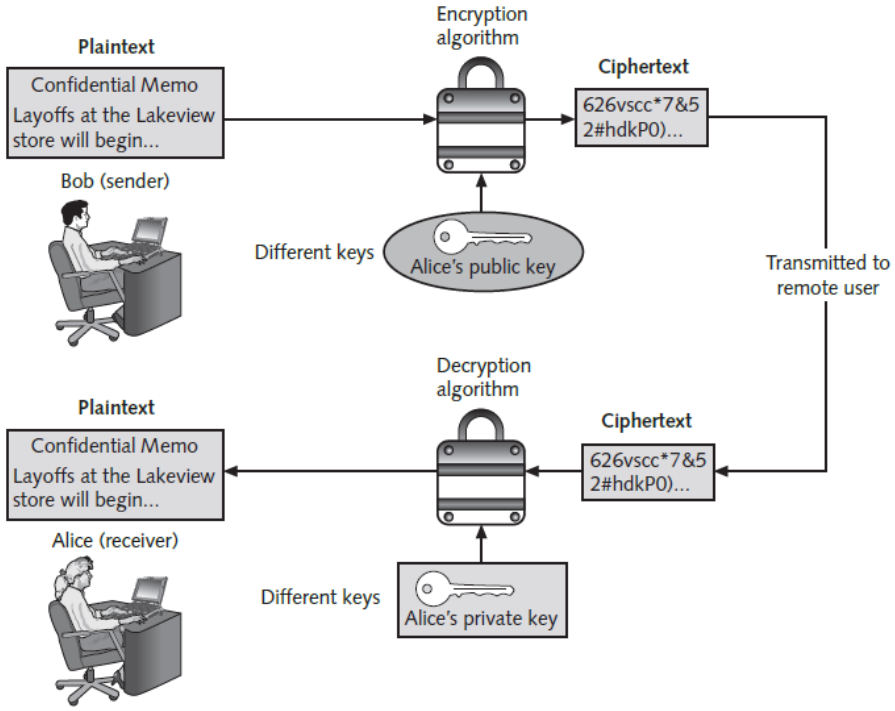
và giải mã tài liệu. Mật mã đối xứng có thể cung cấp các biện pháp bảo vệ mạnh mẽ chống lại các cuộc tấn công miễn là khóa được giữ an toàn.



Hình 1-7 Mật mã đối xứng (khóa riêng tư)

Thuật toán mật mã bất đối xứng Nếu Bob muốn gửi một thông điệp được mã hóa cho Alice bằng cách sử dụng mã hóa đối xứng, anh ta phải đảm bảo rằng cô ấy có khóa để giải mã thông điệp. Nhưng làm thế nào Bob có thể gửi khóa cho Alice? Anh ta không thể gửi nó qua Internet bằng điện tử, vì điều đó sẽ khiến nó dễ bị kẻ tấn công chặn. Anh ta cũng không thể mã hóa khóa và gửi đi, vì Alice sẽ không có cách nào để giải mã khóa đã mã hóa. Ví dụ này minh họa điểm yếu chính của các thuật toán mã hóa đối xứng: việc phân phối và duy trì một khóa đơn an toàn giữa nhiều người dùng, những người thường phân tán về mặt địa lý, đặt ra những thách thức đáng kể.

Một cách tiếp cận hoàn toàn khác với mật mã đối xứng là sử dụng các thuật toán mật mã bất đối xứng, còn được gọi là mật mã khóa công khai. Mã hóa bất đối xứng sử dụng hai khóa thay vì chỉ một. Các khóa này có quan hệ toán học và được gọi là khóa công khai và khóa riêng tư. Khóa công khai được biết đến với mọi người và có thể được phân phối tự do, trong khi khóa riêng tư chỉ được biết đến bởi cá nhân mà nó thuộc về. Khi Bob muốn gửi một thông điệp an toàn cho Alice, anh ta sử dụng khóa công khai của Alice để mã hóa thông điệp. Alice sau đó sử dụng khóa riêng tư của mình để giải mã nó. Mật mã bất đối xứng được minh họa trong Hình 1-8.



Hình 1-8 Mật mã bất đối xứng (khóa công khai)

Một số nguyên tắc quan trọng liên quan đến mật mã bất đối xứng là:

- **Cặp khóa.** Không giống như mật mã đối xứng chỉ sử dụng một khóa, mật mã bất đối xứng yêu cầu một cặp khóa.
- **Khóa công khai.** Khóa công khai theo bản chất được thiết kế là "công khai" và không cần phải bảo vệ. Chúng có thể được tự do cung cấp cho bất kỳ ai hoặc thậm chí được đăng trên Internet.
- **Khóa riêng tư.** Khóa riêng tư phải được giữ bí mật và không bao giờ được chia sẻ.
- **Cả hai chiều.** Khóa mật mã bất đối xứng có thể hoạt động theo cả hai chiều. Một tài liệu được mã hóa bằng khóa công khai có thể được giải mã bằng khóa riêng tư tương ứng. Tương tự, một tài liệu được mã hóa bằng khóa riêng tư có thể được giải mã bằng khóa công khai của nó.

Mật mã bất đối xứng cũng có thể được sử dụng để cung cấp bằng chứng về danh tính của người gửi và rằng dữ liệu không bị chặn hoặc thay đổi. Giả sử Alice nhận được một tài liệu được mã hóa cho biết nó đến từ Bob. Mặc dù Alice có thể chắc chắn rằng thông điệp được mã hóa không bị xem hoặc thay đổi bởi người khác trong quá trình truyền, nhưng làm thế nào cô ấy có thể biết chắc chắn rằng Bob thực sự là người gửi? Vì khóa công khai của Alice được phổ biến rộng rãi, bất kỳ ai cũng có thể

sử dụng nó để mã hóa tài liệu. Một cá nhân khác có thể đã tạo một tài liệu giả, mã hóa nó bằng khóa công khai của Alice, và sau đó gửi cho Alice trong khi giả vờ là Bob. Khóa của Alice có thể xác minh rằng không ai đọc hoặc thay đổi tài liệu trong quá trình truyền, nhưng nó không thể xác minh người gửi.

Tuy nhiên, bằng chứng có thể được cung cấp bằng mật mã bất đối xứng, bằng cách tạo ra một chữ ký số, là một xác minh điện tử của người gửi. Một chữ ký viết tay trên một tài liệu giấy đóng vai trò là bằng chứng cho việc người ký đã đọc và đồng ý với tài liệu. Một chữ ký số cũng tương tự nhưng có thể cung cấp thêm lợi ích. Một chữ ký số có thể:

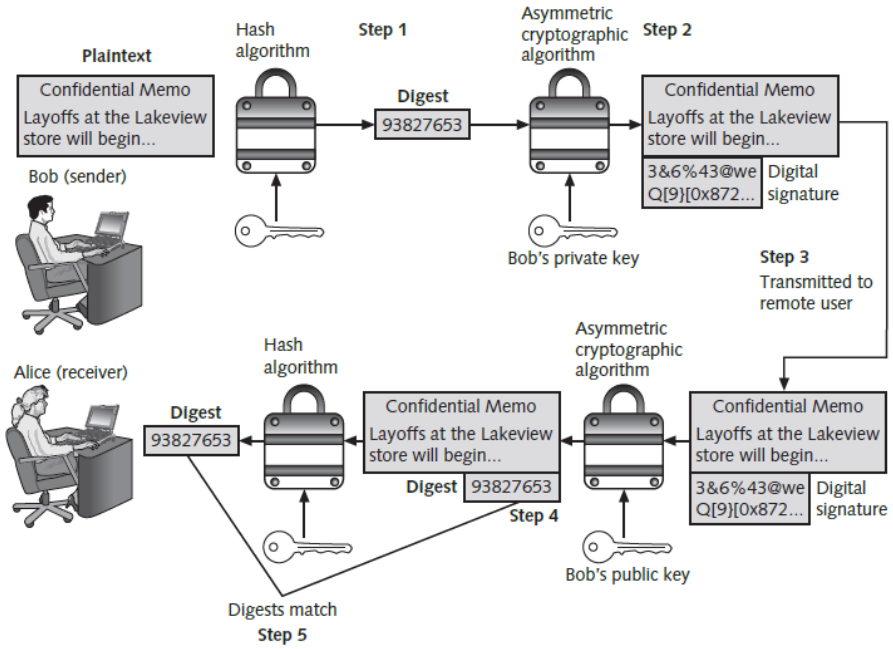
- **Xác minh người gửi.** Một chữ ký số dùng để xác nhận danh tính của người gửi thông điệp điện tử.
- **Ngăn người gửi từ chối tin nhắn.** Người ký không thể sau đó cố gắng từ chối tin nhắn bằng cách tuyên bố chữ ký bị giả mạo (nonrepudiation).
- **Chứng minh tính toàn vẹn của tin nhắn.** Một chữ ký số có thể chứng minh rằng tin nhắn chưa bị thay đổi kể từ khi nó được ký.

Cơ sở của chữ ký số nằm ở khả năng hoạt động theo cả hai hướng của các khóa bất đối xứng (khóa công khai có thể mã hóa tài liệu mà khóa riêng tư có thể giải mã, và khóa riêng tư có thể mã hóa tài liệu mà khóa công khai có thể giải mã). Các bước để Bob gửi một tin nhắn được ký số cho Alice là:

1. Sau khi tạo một bản ghi nhớ, Bob tạo ra một digest trên đó.
2. Bob sau đó mã hóa digest bằng khóa riêng tư của mình. Digest đã mã hóa này là chữ ký số cho bản ghi nhớ.
3. Bob gửi cả bản ghi nhớ và chữ ký số cho Alice.
4. Khi Alice nhận được chúng, cô ấy giải mã chữ ký số bằng khóa công khai của Bob, tiết lộ digest. Nếu cô ấy không thể giải mã chữ ký số, thì cô ấy biết rằng nó không đến từ Bob (vì chỉ khóa công khai của Bob mới có thể giải mã digest được tạo ra bằng khóa riêng tư của anh ấy).
5. Alice sau đó băm bản ghi nhớ bằng cùng thuật toán băm mà Bob đã sử dụng và so sánh kết quả với digest mà cô ấy nhận được từ Bob. Nếu chúng bằng nhau, Alice có thể tin chắc rằng thông điệp không bị thay đổi kể từ khi anh ấy ký. Nếu các digest không bằng nhau, Alice sẽ biết rằng thông điệp đã bị thay đổi kể từ khi nó được ký.

Các bước này được minh họa trong Hình 1-9.

Khóa công khai và khóa riêng tư có thể dẫn đến sự nhầm lẫn về việc sử dụng khóa của ai và khóa nào nên được sử dụng. Bảng 1-7 liệt kê các thực hành cần tuân thủ khi sử dụng mật mã bất đối xứng.



Hình 1-9 Chữ ký số

Bảng 1-7 Thực hành mật mã bất đối xứng

Hành động	**Sử dụng khóa của ai**	**Sử dụng khóa nào**	**Giải thích**
Bob muốn gửi cho Alice một tin nhắn đã mã hóa	Khóa của Alice	Khóa công khai	Khi một tin nhắn được mã hóa được gửi, khóa của người nhận, chứ không phải khóa của người gửi, được sử dụng.
Alice muốn đọc một tin nhắn đã mã hóa do Bob gửi	Khóa của Alice	Khóa riêng tư	Một tin nhắn đã mã hóa chỉ có thể đọc được bằng cách sử dụng khóa riêng tư của người nhận.
Bob muốn gửi cho chính mình một bản sao tin nhắn đã mã	Khóa của Bob	Khóa công khai để mã hóa Khóa	Một tin nhắn được mã hóa chỉ có thể đọc được bằng khóa riêng tư của người nhận. Bob sẽ cần mã hóa nó

hóa mà anh ấy đã gửi cho Alice		riêng tư để giải mã	bằng khóa công khai của mình và sau đó sử dụng khóa riêng tư của mình để giải mã nó.
Bob nhận được một tin nhắn trả lời đã mã hóa từ Alice	Khóa của Bob	Khóa riêng tư	Khóa riêng tư của người nhận được sử dụng để giải mã các tin nhắn đã nhận.
Bob muốn Susan đọc tin nhắn trả lời của Alice mà anh ấy nhận được	Khóa của Susan	Khóa công khai	Tin nhắn nên được mã hóa bằng khóa của Susan để cô ấy có thể giải mã và đọc bằng khóa riêng tư của mình.
Bob muốn gửi cho Alice một tin nhắn có chữ ký số	Khóa của Bob	Khóa riêng tư	Khóa riêng tư của Bob được sử dụng để mã hóa hash.
Alice muốn xem chữ ký số của Bob	Khóa của Bob	Khóa công khai	Vì khóa công khai và khóa riêng tư của Bob hoạt động theo cả hai hướng, Alice có thể sử dụng khóa công khai của anh ấy để giải mã hash.

Sử dụng mật mã học Mật mã học nên được sử dụng để bảo mật tất cả dữ liệu cần được bảo vệ. Điều này bao gồm các tệp cá nhân, cơ sở dữ liệu, phương tiện lưu trữ di động, hoặc dữ liệu trên thiết bị di động. Mật mã học có thể được áp dụng thông qua phần mềm hoặc phần cứng.

Mã hóa bằng phần mềm Mã hóa có thể được thực hiện thông qua phần mềm mật mã chạy trên máy tính để bàn, máy tính xách tay, máy tính bảng hoặc điện thoại thông minh. Có ba phương pháp khác nhau để mã hóa thông qua phần mềm:

- **Các tệp riêng lẻ.** Một phương tiện mã hóa bằng phần mềm là mã hóa hoặc giải mã từng tệp một. Tuy nhiên, đây có thể là một quá trình rườm rà nếu nhiều tệp cần được mã hóa.
- **Hệ thống tệp.** Thay vì bảo vệ từng tệp riêng lẻ, toàn bộ nhóm tệp, chẳng hạn như tất cả các tệp trong một thư mục cụ thể, có thể được mã hóa bằng cách tận dụng

hệ thống tệp của hệ điều hành. Hệ thống tệp là một phương pháp được hệ điều hành sử dụng để lưu trữ, truy xuất và tổ chức các tệp.

- **Mã hóa toàn bộ đĩa.** Mã hóa phần mềm cũng có thể được thực hiện trên quy mô lớn hơn cho toàn bộ đĩa. Điều này được gọi là mã hóa toàn bộ đĩa và bảo vệ tất cả dữ liệu trên ổ cứng. Ngoài việc bảo vệ các tệp và thư mục riêng lẻ, mã hóa toàn bộ đĩa còn ngăn chặn kẻ tấn công truy cập dữ liệu bằng cách khởi động từ một hệ điều hành khác hoặc lấy trộm ổ cứng rồi đặt vào máy tính khác.

Mã hóa phần cứng Mã hóa phần mềm chịu chung số phận với bất kỳ chương trình ứng dụng nào: nó có thể bị tấn công để khai thác các lỗ hổng. Là một lựa chọn khác, mật mã học có thể được nhúng vào phần cứng để cung cấp mức độ bảo mật cao hơn. Mã hóa phần cứng không thể bị khai thác như mã hóa phần mềm.

BÀI 3: BẢO VỆ SỨC KHỎE VÀ AN SINH SỐ

Bước vào thế kỷ 21, trong bối cảnh cuộc Cách mạng Công nghiệp lần thứ tư, không gian số đã trở thành một phần không thể tách rời của đời sống hiện đại. Đối với sinh viên, Internet và các thiết bị công nghệ đã mở ra một hệ sinh thái với những cơ hội vô tận cho việc học tập, nghiên cứu, kết nối và sáng tạo. Tuy nhiên, thế giới số cũng được ví như một con dao hai lưỡi ; bên cạnh những lợi ích to lớn là các thách thức và rủi ro tiềm ẩn đối với sức khỏe, sự an toàn và chất lượng cuộc sống của mỗi cá nhân. Chương này sẽ trang bị cho sinh viên một cái nhìn toàn diện và đa chiều, giúp họ có thể điều hướng một cách an toàn và chủ động trong môi trường phức tạp này.

Nội dung của chương được cấu trúc thành ba phần chính, tương ứng với ba cấp độ nhận thức và hành động khác nhau. Phần đầu tiên, Sức khỏe số, tập trung vào mối quan hệ giữa cá nhân và công nghệ, phân tích các tác động lên sức khỏe thể chất, tâm lý và cung cấp các kỹ năng tự chăm sóc để đạt được sự cân bằng. Tiếp theo, An sinh số, mở rộng góc nhìn ra môi trường bên ngoài, đề cập đến các vấn đề an toàn, an ninh mạng, quyền riêng tư và danh tính số, với mục tiêu trang bị kỹ năng phòng vệ để bảo vệ bản thân trước các mối đe dọa từ bên ngoài. Cuối cùng, Trách nhiệm và Vai trò của sinh viên, chuyển từ tư duy phòng vệ sang chủ động kiến tạo. Mục này nhấn mạnh vai trò của một công dân số và khuyến khích sinh viên không chỉ bảo vệ bản thân mà còn đóng góp tích cực vào việc xây dựng một cộng đồng mạng lành mạnh, văn minh và nhân văn.

Thông qua chương học này, sinh viên sẽ được trang bị đầy đủ hành trang để không chỉ trở thành những người dùng công nghệ thông thái mà còn là những công dân số có trách nhiệm, có khả năng làm chủ cuộc sống số của mình và góp phần tạo ra những thay đổi tích cực cho cộng đồng.

PHẦN I: SỨC KHỎE SỐ

Trong guồng quay của học tập và đời sống xã hội hiện đại, màn hình các thiết bị kỹ thuật số đã trở thành người bạn đồng hành gần như 24/7 của mỗi sinh viên. Sự tương tác liên tục này, dù cho mục đích học tập hay giải trí, đều tạo ra những tác động trực tiếp và sâu sắc đến cả cơ thể và tâm trí của chúng ta. Nhiều câu hỏi được đặt ra: Làm thế nào để duy trì sự tập trung khi học trực tuyến mà không bị mỏi mắt? Làm thế nào để kết nối với bạn bè qua mạng xã hội mà không cảm thấy lo âu hay tự ti? Và làm thế nào để có một giấc ngủ ngon sau một ngày dài tiếp xúc với công nghệ?.

Phần "Sức khỏe số", sẽ đi sâu vào việc trả lời những câu hỏi này. Chúng ta sẽ bắt đầu bằng việc định nghĩa rõ ràng khái niệm "Sức khỏe số" cùng các thành phần cốt lõi của nó, bao gồm sức khỏe thể chất, tâm lý và xã hội. Tiếp theo, mục này sẽ nhận diện và phân tích các vấn đề sức khỏe phổ biến mà sinh viên thường gặp phải, từ hội chứng thị giác máy tính, rối loạn giấc ngủ cho đến các trạng thái căng thẳng, quá tải thông tin và hội chứng sợ bỏ lỡ (FOMO). Quan trọng hơn cả, mục này sẽ cung cấp một bộ kỹ năng và công cụ thực tiễn, giúp sinh viên có thể chủ động quản lý thời gian, chăm sóc bản thân và duy trì một trạng thái cân bằng, lành mạnh trong mối quan hệ với công nghệ.

1. Khái niệm “Sức khỏe số”

Sức khỏe số (Digital Health) được định nghĩa là trạng thái khỏe mạnh về thể chất, tâm lý và xã hội trong mối quan hệ tương tác với công nghệ kỹ thuật số. Đây không phải là một lời kêu gọi từ bỏ công nghệ, mà là một cách tiếp cận chủ động nhằm khai thác lợi ích của thế giới số đồng thời giảm thiểu tác động tiêu cực của nó. Một cá nhân có sức khỏe số tốt là khi họ có khả năng kiểm soát việc sử dụng công nghệ của mình thay vì bị công nghệ kiểm soát. Điều này thể hiện qua việc sử dụng thiết bị số một cách có chủ đích, ý thức về thời gian, nội dung và ảnh hưởng của chúng đến sức khỏe thể chất, tinh thần và các mối quan hệ xã hội. Sức khỏe số là một thành phần quan trọng của kỹ năng công dân số, nhấn mạnh việc sử dụng công nghệ một cách có trách nhiệm và đạo đức. Về bản chất, sức khỏe số là sự cân bằng giữa việc kết nối và ngắt kết nối, giữa thế giới trực tuyến và thế giới thực, giữa việc tiêu thụ thông tin và sáng tạo giá trị, cũng như giữa lợi ích tức thời và sức khỏe bền vững dài hạn.

Tương tự khái niệm sức khỏe toàn diện của Tổ chức Y tế Thế giới (WHO), Sức khỏe số cũng được cấu thành từ ba phương diện chính có tác động qua lại lẫn nhau. Thứ nhất là **sức khỏe thể chất**, liên quan đến ảnh hưởng của việc sử dụng thiết bị kỹ thuật số lên cơ thể. Nó bao gồm các yếu tố như công thái học (Ergonomics) để tránh các bệnh lý cơ xương khớp, sức khỏe thị giác để bảo vệ mắt khỏi ánh sáng xanh và tình trạng mỏi mắt, chất lượng giấc ngủ, và việc duy trì hoạt động thể chất để cân bằng với thời gian ngồi trước màn hình. Thứ hai là **sức khỏe tâm lý và cảm xúc**, liên quan đến trạng thái tinh thần khi tương tác trong môi trường số. Khía cạnh này bao gồm khả năng quản lý căng thẳng trước dòng thông tin vô tận, duy trì sự tập trung, cách thế giới số tác động đến lòng tự trọng qua cơ chế so sánh xã hội, và cảm giác tự chủ, không rơi vào trạng thái nghiện công nghệ. Cuối cùng là **sức khỏe xã hội**, đề cập đến chất lượng các mối quan hệ và tương tác xã hội. Nó bao hàm việc dùng công nghệ để củng cố các mối quan hệ thực, khả năng giao tiếp hiệu quả và đồng cảm trên mạng, cảm giác thuộc về các cộng đồng trực tuyến ý nghĩa, và khả năng tự bảo vệ khỏi các hành vi tiêu cực như bắt nạt trực tuyến. Một trạng thái sức khỏe số lý tưởng là khi cả ba thành phần này được duy trì ở trạng thái cân bằng.

Khái niệm Sức khỏe số không xuất hiện đột ngột mà đã tiến hóa cùng với sự phát triển của công nghệ. Trong những ngày đầu của Internet, mối quan tâm chủ yếu là về các vấn đề thể chất như hội chứng ống cổ tay và mỏi mắt. Với sự ra đời của mạng xã hội và thiết bị di động, trọng tâm bắt đầu chuyển dịch sang các vấn đề sức khỏe tâm lý và xã hội như nghiện Internet, so sánh xã hội và FOMO. Hiện nay, trong kỷ nguyên của Trí tuệ Nhân tạo (AI) và kinh tế chú ý, khái niệm Sức khỏe số còn mở rộng ra cả việc duy trì sự tự chủ về nhận thức và khả năng ra quyết định của con người trước sự thao túng tinh vi của công nghệ.

Thay vì nhìn nhận Sức khỏe số theo kiểu "có hoặc không", sẽ hữu ích hơn nếu xem nó như một phổ liên tục. Một đầu của phổ là trạng thái "sử dụng có vấn đề", đặc trưng bởi sự mất kiểm soát và phụ thuộc. Ở giữa là "sử dụng có ý thức", nơi người dùng nhận thức được hành vi của mình và cố gắng cân bằng. Ở đầu kia của phổ là trạng thái "phát triển mạnh mẽ trong môi trường số", nơi công nghệ không chỉ được quản lý để giảm thiểu tác hại mà còn được chủ động tận dụng như một công cụ để nâng cao chất lượng cuộc sống, học tập suốt đời, và xây dựng các kết nối xã hội ý

nghĩa. Mục tiêu của giáo dục về Sức khỏe số là giúp sinh viên dịch chuyển trên phổ này theo hướng tích cực.

2. Các vấn đề ảnh hưởng đến "Sức khỏe số"

Việc sử dụng công nghệ số thiếu kiểm soát và nhận thức có thể dẫn đến một loạt các vấn đề sức khỏe nghiêm trọng. Về mặt thể chất, một trong những vấn đề phổ biến nhất là Hội chứng thị giác máy tính (CVS), gây ra bởi việc mắt phải liên tục điều tiết và hội tụ khi nhìn vào màn hình có độ sắc nét thấp và ánh sáng chói. Việc giảm tần suất chớp mắt khi tập trung vào màn hình cũng dẫn đến khô mắt. Các triệu chứng bao gồm mỏi mắt, nóng rát, đau đầu, nhìn mờ, và đau vai gáy. Các vấn đề về cơ xương khớp cũng rất phổ biến, điển hình là hiện tượng "Text Neck" (Cổ tin nhắn) do tư thế cúi đầu xem điện thoại trong thời gian dài, làm tăng áp lực lên cột sống cổ một cách đáng kể, cùng với các vấn đề khác như "vai chuột" (mouse shoulder) do căng cơ vai khi dùng chuột và hội chứng ống cổ tay do các chuyển động lặp đi lặp lại. Tình trạng này kéo dài gây mỏi cơ, đau mãn tính và có thể dẫn đến thoái hóa đốt sống sớm. Ngoài ra, ánh sáng xanh từ màn hình ức chế việc sản xuất melatonin, hormone gây ngủ, dẫn đến rối loạn giấc ngủ, khiến chúng ta khó ngủ hơn và mệt mỏi vào ngày hôm sau. Cuối cùng, việc dành hàng giờ cho các hoạt động trên màn hình góp phần tạo ra một lối sống tĩnh tại, là yếu tố nguy cơ của nhiều bệnh mãn tính như béo phì, bệnh tim mạch và tiểu đường tuýp 2.

Về mặt tâm lý và cảm xúc, nghiện Internet và mạng xã hội là một dạng nghiện hành vi, đặc trưng bởi sự thôi thúc không thể kiểm soát việc sử dụng Internet. Các nền tảng này được thiết kế để gây nghiện bằng cách khai thác hệ thống tưởng thưởng dopamine của não bộ, tạo ra cảm giác hài lòng sau mỗi lượt tương tác. Các dấu hiệu nhận biết bao gồm mất kiểm soát về thời gian, cảm thấy cáu kỉnh khi không thể truy cập mạng, và sao lãng các trách nhiệm cá nhân. Song song đó, tình trạng quá tải thông tin từ các nguồn kỹ thuật số gây ra mệt mỏi về mặt nhận thức, làm giảm khả năng tập trung và suy nghĩ sáng tạo. Bên cạnh đó, môi trường số còn tiềm ẩn những thách thức tâm lý mới nổi và tinh vi hơn. Hiện tượng "Doomscrolling" (cuộn trang vô tận trong vô vọng) là hành vi tiêu thụ một lượng lớn tin tức tiêu cực một cách liên tục, được thúc đẩy bởi "thiên kiến tiêu cực" của não bộ, dẫn đến gia tăng cảm giác lo âu và bất lực.

Mạng xã hội còn khuếch đại hiện tượng so sánh xã hội, khi việc liên tục tiếp xúc với những hình ảnh lý tưởng hóa của người khác có thể làm xói mòn lòng tự trọng, gia tăng cảm giác lo âu và góp phần gây ra trầm cảm. Thuật toán có thể tạo ra các "bong bóng lọc" (filter bubble) hoặc "buồng vang" (echo chamber), chỉ cho chúng ta thấy những nội dung phù hợp với niềm tin sẵn có, làm giảm khả năng tiếp xúc với các quan điểm đa chiều và củng cố các định kiến. Đi kèm với đó là Hội chứng sợ bỏ lỡ (FOMO), một dạng lo âu xã hội đặc trưng bởi mong muốn được kết nối liên tục, thúc đẩy hành vi kiểm tra mạng xã hội một cách ám ảnh và có tương quan với tâm trạng tiêu cực. Cuối cùng, bắt nạt trực tuyến (Cyberbullying), hành vi sử dụng công nghệ số để quấy rối, đe dọa người khác, có thể xảy ra 24/7 và có khả năng lan truyền nhanh chóng, gây ra những tổn thương tâm lý nghiêm trọng cho nạn nhân.

3. Kỹ năng và công cụ bảo vệ "Sức khỏe số"

Để đối phó với những thách thức trên, sinh viên cần chủ động trang bị cho mình những kỹ năng và tận dụng các công cụ hỗ trợ để xây dựng một mối quan hệ lành mạnh với công nghệ. Một kỹ năng quan trọng là quản lý thời gian sử dụng thiết bị một cách chủ động bằng cách thiết lập mục tiêu và giới hạn rõ ràng trước khi bắt đầu. Các phương pháp như kỹ thuật Pomodoro, với chu kỳ làm việc 25 phút và nghỉ 5 phút, giúp duy trì sự tập trung và chống lại sự mệt mỏi. Để bảo vệ mắt, quy tắc 20-20-20 (cứ sau 20 phút nhìn vào màn hình, hãy nhìn vào một vật ở xa 20 feet trong 20 giây) là cực kỳ hiệu quả. Việc thiết lập các "vùng không công nghệ" như phòng ngủ, bàn ăn và "thời gian không công nghệ" như một giờ sau khi thức dậy và trước khi đi ngủ, cũng giúp tái cân bằng cuộc sống và cải thiện giấc ngủ.

Thay vì chỉ dựa vào sức mạnh ý chí, sinh viên có thể chủ động xây dựng một "kiến trúc lựa chọn" cho bản thân. Đây là việc thiết kế lại môi trường số và vật lý để khiến các lựa chọn tốt trở nên dễ dàng hơn và các lựa chọn xấu trở nên khó khăn hơn. Ví dụ, bạn có thể xóa các ứng dụng mạng xã hội khỏi màn hình chính, tắt hầu hết các thông báo đẩy, chuyển màn hình sang chế độ xám để giảm sự hấp dẫn thị giác, và đặt điện thoại ở một phòng khác khi học hoặc làm việc.

Bên cạnh quản lý thời gian, việc quản lý thông tin và nhận thức cũng rất cần thiết. Hãy phát triển tư duy phản biện bằng cách luôn đặt câu hỏi về nguồn gốc, mục đích, bằng chứng và thiên kiến của thông tin trên mạng. Sinh viên nên chủ động xây

dựng một "khẩu phần thông tin" lành mạnh bằng cách theo dõi các nguồn uy tín và hủy theo dõi những trang có nội dung tiêu cực hoặc sai sự thật. "Digital Detox", một khoảng thời gian tự nguyện ngắt kết nối khỏi các thiết bị kỹ thuật số, cũng là một công cụ mạnh mẽ để giảm căng thẳng và đánh giá lại mối quan hệ với công nghệ. Việc giải độc số có thể thực hiện ở nhiều cấp độ, từ một buổi tối đến cả một kỳ nghỉ, giúp "thiết lập lại" hệ thống dopamine của não và tìm lại niềm vui từ các hoạt động ngoại tuyến.

Một cách tiếp cận sâu sắc hơn là áp dụng triết lý "Tối giản số" (Digital Minimalism). Triết lý này không chống lại công nghệ, mà là đặt ra một ngưỡng rất cao cho các công cụ số được phép tồn tại trong cuộc sống của bạn. Nó bao gồm việc tạm thời gỡ bỏ các ứng dụng không thiết yếu trong một khoảng thời gian (ví dụ 30 ngày) để tái khám phá các hoạt động ngoại tuyến có giá trị, sau đó chỉ cài đặt lại một cách có chọn lọc những công cụ thực sự hỗ trợ cho các giá trị mà bạn sâu sắc quan tâm.

Công nghệ cũng có thể được sử dụng để chống lại chính những mặt trái của nó. Các hệ điều hành điện thoại thông minh hiện nay đều tích hợp các tính năng quản lý thời gian màn hình như Screen Time (iOS) và Digital Wellbeing (Android), cho phép người dùng theo dõi và đặt giới hạn thời gian cho các ứng dụng. Ngoài ra, các ứng dụng của bên thứ ba như Forest hay Freedom giúp biến việc tập trung thành trò chơi hoặc chặn các trang web gây xao nhãng. Các tiện ích mở rộng trình duyệt như uBlock Origin giúp chặn quảng cáo phiền nhiễu và các trình theo dõi. Cuối cùng, thay vì lướt mạng xã hội trước khi ngủ, các ứng dụng thiền định và hỗ trợ giấc ngủ như Calm hay Headspace cung cấp các bài thiền có hướng dẫn, truyện kể và âm thanh tự nhiên giúp thư giãn tâm trí, chuẩn bị cho một giấc ngủ ngon.

PHẦN II: AN SINH SỐ

Nếu như phần trước tập trung vào việc chăm sóc sức khỏe từ bên trong, thì phần này sẽ hướng sự chú ý ra môi trường số bên ngoài, nơi một cá nhân khó có thể cảm thấy yên tâm nếu "ngôi nhà số" của họ không an toàn. "An sinh số" chính là nghệ thuật xây dựng và bảo vệ "ngôi nhà số" đó, chuyển từ việc tự chăm sóc sang tự vệ. Trong mục này, chúng ta sẽ định nghĩa "An sinh số" và khám phá mối liên hệ mật thiết của nó với "Sức khỏe số". Trọng tâm của mục là nhận diện các rủi ro từ môi trường bên ngoài như các vấn đề về quyền riêng tư, lừa đảo, tin giả, và tác động của dấu chân số. Để đối phó, mục này sẽ trang bị cho sinh viên một "bộ công cụ phòng vệ" toàn diện để xây dựng một pháo đài số vững chắc, giúp họ tự tin và an toàn khi hoạt động trên không gian mạng.

1. Khái niệm “An sinh số”

An sinh số (Digital Well-being) là trạng thái mà một cá nhân có thể tham gia vào môi trường kỹ thuật số một cách an toàn, tự tin và có chủ đích, nơi công nghệ hỗ trợ các mục tiêu xã hội, kinh tế và cá nhân thay vì làm phương hại đến chúng. An sinh số nhấn mạnh đến các yếu tố môi trường bên ngoài, bao gồm cảm giác được an toàn và an ninh khỏi các mối đe dọa như lừa đảo và tấn công mạng ; quyền riêng tư để có quyền kiểm soát thông tin cá nhân của mình ; sự tự chủ để đưa ra lựa chọn sáng suốt về cách thức và thời điểm sử dụng công nghệ mà không bị các thiết kế gây nghiện thao túng ; và sự hòa nhập cùng khả năng quản lý danh tính số một cách tích cực trong các cộng đồng trực tuyến. Nói một cách đơn giản, nếu Sức khỏe số là "chăm sóc bản thân", thì An sinh số là "đảm bảo ngôi nhà kỹ thuật số của bạn an toàn và đáng sống".

An sinh số và Sức khỏe số là hai khái niệm có mối quan hệ cộng sinh, không thể tách rời. An sinh số được xem là nền tảng cho Sức khỏe số ; rất khó để một người có sức khỏe tâm lý tốt nếu họ liên tục sống trong lo sợ bị đánh cắp danh tính hay bị bắt nạt trực tuyến, vốn là các vấn đề của an sinh số. Một môi trường số an toàn là điều kiện tiên quyết để người dùng có thể duy trì trạng thái tinh thần khỏe mạnh. Ngược lại, Sức khỏe số cũng củng cố An sinh số ; một người có kỹ năng quản lý thời gian và nhận thức tốt sẽ ít có khả năng trở thành nạn nhân của các chiêu trò lừa đảo. Ví dụ, một sinh viên có thể có sức khỏe thể chất tốt, nhưng nếu tài khoản mạng xã hội của họ

bị xâm nhập, an sinh số của họ sẽ bị tổn hại nghiêm trọng, điều này chắc chắn sẽ gây ra căng thẳng và lo âu, ảnh hưởng ngược lại đến sức khỏe số của họ. Do đó, việc tiếp cận cả hai khía cạnh là cần thiết để có một cuộc sống số toàn diện và lành mạnh.

An sinh số không chỉ là trách nhiệm của người dùng mà còn phụ thuộc rất lớn vào thiết kế của các nền tảng công nghệ. Các khái niệm như "Thiết kế Nhân văn" (Humane Design) ngày càng được nhấn mạnh, yêu cầu các nhà thiết kế có trách nhiệm đạo đức trong việc tạo ra các sản phẩm tôn trọng sự chú ý của người dùng, giảm thiểu các yếu tố gây nghiện, và cung cấp các cài đặt quyền riêng tư minh bạch. Sinh viên cần được trang bị kiến thức để nhận diện các "mẫu thiết kế đen tối" (dark patterns) - những giao diện người dùng được cố tình thiết kế để lừa hoặc ép người dùng thực hiện những hành động mà họ không mong muốn.

2. Các vấn đề ảnh hưởng đến “An sinh số”

Môi trường số tiềm ẩn nhiều rủi ro có thể gây tổn hại đến tài chính, danh tiếng và sự an toàn của sinh viên. Một trong những vấn đề hàng đầu là quyền riêng tư và bảo mật dữ liệu cá nhân, vốn được xem là "vàng" trong nền kinh tế số. Các vụ tấn công mạng có thể làm rò rỉ dữ liệu cá nhân, tạo điều kiện cho kẻ xấu thực hiện hành vi đánh cắp danh tính như mở tài khoản ngân hàng hoặc vay tiền dưới tên của nạn nhân. Đồng thời, hầu hết các dịch vụ miễn phí trên Internet đều theo dõi và giám sát người dùng thông qua các công cụ như cookies để xây dựng hồ sơ chi tiết về sở thích và thói quen của họ, chủ yếu nhằm mục đích quảng cáo nhắm mục tiêu. Dữ liệu này còn có thể được các nhà môi giới dữ liệu bán cho các bên thứ ba cho các mục đích thương mại và chính trị, điển hình là vụ bê bối Cambridge Analytica. Một hiện tượng tâm lý đáng chú ý là "Nghịch lý Quyền riêng tư" (The Privacy Paradox), trong đó người dùng bày tỏ sự lo ngại về quyền riêng tư nhưng hành động của họ lại không phản ánh điều đó. Bên cạnh đó, vấn đề "Sharenting", chỉ việc các bậc cha mẹ chia sẻ quá nhiều thông tin về con cái, cũng vô tình tạo ra một "dấu chân số" cho đứa trẻ trước khi chúng có thể đồng ý.

Về an toàn và an ninh mạng, lừa đảo trực tuyến (phishing, scams) là hình thức tấn công phổ biến nhất, khai thác yếu tố con người. Phishing là hành vi giả mạo các đơn vị uy tín để lừa người dùng cung cấp thông tin đăng nhập. Các chiêu trò lừa đảo khác cũng ngày càng tinh vi, từ "việc nhẹ lương cao" đến lừa đảo tình cảm, thậm chí là

các hình thức mới như lừa đảo "Mổ lợn" (Pig Butchering Scams) kết hợp giữa lừa đảo tình cảm và đầu tư, hay các cuộc gọi lừa đảo sử dụng công nghệ sao chép giọng nói bằng AI. Bên cạnh đó, sự lan tràn của tin tức giả (fake news) và thông tin sai lệch là một mối đe dọa lớn. Cần phân biệt "misinformation" (lan truyền thông tin sai nhưng không có ác ý) và "disinformation" (cố tình tạo và lan truyền thông tin sai sự thật để trục lợi hoặc gây hoang mang). Ngoài ra, cần cảnh giác với "Malinformation" (thông tin ác ý), là việc lan truyền thông tin có thật nhưng với mục đích gây hại. Tin giả thường khai thác cảm xúc và lan truyền với tốc độ chóng mặt, gây hậu quả khôn lường. Không gian mạng cũng chứa đựng nhiều nội dung độc hại như ngôn từ thù hận, bạo lực cực đoan, và các thử thách nguy hiểm có thể tác động tiêu cực lâu dài đến sức khỏe tâm thần.

Cuối cùng, dấu chân số (digital footprint) và danh tiếng trực tuyến có những tác động lâu dài. Mỗi hành động của bạn trên mạng đều góp phần tạo nên dấu chân số, vốn tồn tại gần như vĩnh viễn và dễ dàng được tìm kiếm. Các nhà tuyển dụng và ban tuyển sinh ngày nay thường tìm kiếm tên ứng viên trên mạng, và một bình luận thiếu suy nghĩ hay hình ảnh không phù hợp từ quá khứ có thể ảnh hưởng tiêu cực đến cơ hội trong tương lai. Do đó, việc quản lý danh tiếng cá nhân trên mạng, bao gồm những gì bạn đăng và những gì người khác đăng về bạn, đã trở thành một kỹ năng quan trọng. Xây dựng một hình ảnh cá nhân tích cực và chuyên nghiệp là một kỹ năng thiết yếu, trong khi việc bị bôi nhọ danh dự trên mạng có thể gây ra khủng hoảng cá nhân nghiêm trọng.

3. Kỹ năng và công cụ bảo vệ “An sinh số”

Để điều hướng an toàn trong môi trường số phức tạp, sinh viên cần trang bị một bộ kỹ năng phòng vệ chủ động và tận dụng các công nghệ hỗ trợ. Kỹ năng quản lý quyền riêng tư và bảo mật là nền tảng. Hãy luôn sử dụng mật khẩu mạnh—dài, phức tạp và duy nhất cho mỗi tài khoản quan trọng—và bật xác thực hai yếu tố (2FA) bất cứ khi nào có thể. Dành thời gian để xem lại và tùy chỉnh các cài đặt quyền riêng tư trên các nền tảng mạng xã hội, giới hạn người có thể xem bài đăng của bạn và gỡ bỏ quyền truy cập của các ứng dụng không còn sử dụng. Hãy phát triển một "phản xạ hoài nghi" để nhận diện các hình thức lừa đảo, cảnh giác với các thông điệp tạo cảm giác khẩn cấp hoặc đưa ra lời đề nghị quá tốt, và không bao giờ nhấp vào các liên kết đáng ngờ.

Đối với các cuộc trò chuyện nhạy cảm, hãy ưu tiên sử dụng các dịch vụ có mã hóa đầu cuối như Signal hoặc WhatsApp.

Sinh viên nên hình thành thói quen thực hiện "Kiểm toán Quyền riêng tư" (Privacy Audit) định kỳ hàng quý hoặc nửa năm một lần. Các bước thực hiện bao gồm: tìm kiếm tên của bạn trên Internet để xem thông tin công khai; kiểm tra chi tiết cài đặt quyền riêng tư trên mạng xã hội; quản lý quyền của các ứng dụng bên thứ ba đang truy cập vào tài khoản của bạn; và kiểm tra quyền của các ứng dụng trên điện thoại (truy cập micro, máy ảnh, vị trí, v.v.).

Kỹ năng đánh giá thông tin và truyền thông cũng cực kỳ quan trọng. Hãy thực hành phương pháp kiểm chứng thông tin SIFT: Dừng lại (Stop), Điều tra nguồn tin (Investigate the source), Tìm các nguồn tin khác (Find better coverage), và Truy tìm lại các trích dẫn (Trace claims). Việc này giúp bạn không vội vàng tin và chia sẻ thông tin gây cảm xúc mạnh, đồng thời có được cái nhìn đa chiều và xác thực hơn. Hãy học cách nhận diện các đặc điểm của tin tức giả như tiêu đề giật gân, ngôn ngữ kích động, hình ảnh sai ngữ cảnh, và không có nguồn trích dẫn rõ ràng. Các thuyết âm mưu thường đưa ra những lời giải thích đơn giản cho các vấn đề phức tạp và cho rằng có một "nhóm tinh hoa" nào đó đang che giấu sự thật. Để hỗ trợ kỹ năng này, bạn có thể sử dụng các công cụ kiểm chứng nâng cao như tìm kiếm hình ảnh ngược (Google Images, TinEye) để phát hiện hình ảnh sai ngữ cảnh, hoặc các trang lưu trữ web (Wayback Machine) để xem các phiên bản cũ của một trang web.

Để hỗ trợ các kỹ năng trên, có nhiều công cụ và phần mềm hữu ích. Trình quản lý mật khẩu như Bitwarden hoặc 1Password là công cụ nền tảng để có thói quen bảo mật tốt, giúp tạo và lưu trữ an toàn hàng chục mật khẩu mạnh và duy nhất. Mạng riêng ảo (VPN) tạo ra một "đường hầm" mã hóa, bảo vệ lưu lượng truy cập của bạn khỏi sự theo dõi, đặc biệt khi dùng Wi-Fi công cộng. Đương nhiên, việc cài đặt và cập nhật một phần mềm diệt virus uy tín là thiết yếu trên máy tính để ngăn chặn các phần mềm độc hại mới nhất. Cuối cùng, các tiện ích mở rộng cho trình duyệt như HTTPS Everywhere (tự động chuyển sang kết nối mã hóa), Privacy Badger (chặn trình theo dõi), và uBlock Origin (chặn quảng cáo độc hại) có thể giúp tăng cường bảo mật và sự riêng tư khi duyệt web.

PHẦN III: TRÁCH NHIỆM VÀ VAI TRÒ CỦA SINH VIÊN TRONG XÂY DỰNG MÔI TRƯỜNG SỐ LÀNH MẠNH

Sau khi được trang bị kỹ năng để bảo vệ Sức khỏe số và An sinh số cá nhân, chúng ta bước vào phần then chốt: chuyển từ vai trò của một người dùng được bảo vệ sang một công dân số có trách nhiệm và chủ động. Môi trường số không phải là một vùng đất vô chủ, mà là một xã hội mở rộng và chất lượng của nó phụ thuộc vào hành vi của mỗi thành viên. Mục này sẽ phân tích sâu sắc về các khía cạnh của trách nhiệm công dân số. Chúng ta sẽ cùng nhau khám phá các quy tắc ứng xử văn minh trên mạng, tìm hiểu sức mạnh của việc lan tỏa những giá trị tích cực, và học cách nhận biết, hỗ trợ bạn bè khi họ gặp khó khăn về tâm lý. Cuối cùng, mục này sẽ khuyến khích sinh viên tham gia vào các cộng đồng an toàn số, trở thành những tác nhân thay đổi, góp phần định hình một môi trường mạng nhân văn và tiến bộ.

1. Hành xử có văn hóa trên mạng (Netiquette)

"Netiquette", là sự kết hợp giữa "Network" (Mạng lưới) và "Etiquette" (Quy tắc ứng xử), là một bộ các quy tắc không chính thức về hành vi được chấp nhận trong giao tiếp trực tuyến. Việc tuân thủ Netiquette không chỉ thể hiện sự tôn trọng người khác mà còn là nền tảng để xây dựng một môi trường giao tiếp hiệu quả và văn minh. Quy tắc vàng của Netiquette là ghi nhớ yếu tố con người (Remember the Human); đằng sau mỗi tài khoản là một con người thật với những cảm xúc riêng. Trước khi đăng bất cứ điều gì, hãy tự hỏi: "Liệu mình có dám nói điều này trực tiếp với họ không?". Điều này giúp ngăn chặn các hành vi công kích vốn dễ xảy ra hơn trong môi trường ẩn danh tương đối của Internet. Không gian mạng là nơi hội tụ của vô số quan điểm và văn hóa, do đó cần tôn trọng sự đa dạng và khác biệt. Hãy tập trung phản biện vào lập luận chứ không công kích cá nhân, và chấp nhận rằng việc "bất đồng quan điểm" là bình thường. Đồng thời, hãy sử dụng ngôn ngữ phù hợp, tránh viết in hoa toàn bộ (vì nó được xem như đang la hét) và sử dụng ngữ pháp đúng mực để đảm bảo thông điệp được truyền tải rõ ràng.

Các quy tắc ứng xử này cần được áp dụng một cách linh hoạt tùy theo từng bối cảnh cụ thể. Ví dụ, trong email học thuật/công việc, luôn sử dụng tiêu đề rõ ràng, lời chào và kết thúc trang trọng, đồng thời kiểm tra lỗi chính tả kỹ lưỡng. Trong các cuộc họp trực tuyến, hãy vào đúng giờ, chọn không gian yên tĩnh, tắt micro khi không phát

biểu và sử dụng tính năng giơ tay. Khi thảo luận trên các diễn đàn học tập, hãy giữ bình luận liên quan đến chủ đề, trích dẫn nguồn và tôn trọng ý kiến của người khác.

Mỗi lượt bình luận và chia sẻ của bạn đều có sức ảnh hưởng, vì đó là một hành động khuếch đại thông điệp đến với mạng lưới của bạn. Hãy luôn tư duy trước khi hành động (Think Before You Post/Share), cân nhắc xem nội dung có chính xác không, có làm tổn thương ai không, hay có ảnh hưởng đến hình ảnh của mình và người khác không. Thay vì chỉ trích tiêu cực, hãy đưa ra góp ý mang tính xây dựng để làm cho cuộc thảo luận trở nên có giá trị hơn. Khi bạn nhấn nút "chia sẻ", bạn đang bảo chứng cho thông tin đó với mạng lưới của mình, vì vậy đừng trở thành một mắt xích trong chuỗi lây lan tin giả và ngôn từ thù hận. Hãy áp dụng các kỹ năng kiểm chứng thông tin để đảm bảo bạn chỉ lan tỏa những nội dung chính xác và có giá trị.

Dấu chân số của bạn đang dần trở thành một phần quan trọng trong sơ yếu lý lịch (CV) của bạn, do đó, việc quản lý hình ảnh cá nhân trực tuyến một cách có chủ đích là một kỹ năng thiết yếu. Mỗi sinh viên đều đang xây dựng một "thương hiệu cá nhân", dù có chủ đích hay không. Hãy suy nghĩ về hình ảnh bạn muốn người khác nhìn nhận về mình và để các hoạt động trực tuyến của bạn phản ánh những giá trị đó. Hành xử trên các nền tảng khác nhau cần có sự điều chỉnh—chuyên nghiệp trên LinkedIn, cá nhân hơn trên Facebook—nhưng luôn phải duy trì một chuẩn mực văn minh chung. Thay vì chỉ lo xóa bỏ dấu vết tiêu cực, hãy chủ động xây dựng một dấu chân số tích cực bằng cách chia sẻ các bài viết học thuật, các dự án bạn tham gia, và tham gia bình luận một cách thông minh trong các nhóm chuyên ngành. Một hồ sơ trực tuyến tích cực và chuyên nghiệp là một lợi thế cạnh tranh lớn.

2. Ủng hộ, chia sẻ nội dung tích cực

Trong một môi trường số thường bị chi phối bởi những tin tức tiêu cực và các cuộc tranh cãi, việc chủ động lan tỏa những điều tích cực là một hành động có sức mạnh to lớn. Việc làm này không chỉ đơn thuần là chia sẻ những câu chuyện vui vẻ. Nó đóng vai trò quan trọng trong việc chống lại sự tiêu cực và tin giả bằng cách làm loãng đi dòng chảy của thông tin độc hại. Khi bạn tích cực tương tác với những nội dung có giá trị, bạn đang "dạy" cho các thuật toán của nền tảng mạng xã hội biết rằng đây là loại nội dung mà cộng đồng quan tâm, từ đó giúp các nội dung tương tự được hiển thị nhiều hơn. Hơn nữa, một kiến thức hữu ích, một câu chuyện về lòng tốt, hay

một dự án vì cộng đồng được lan tỏa có thể truyền cảm hứng và tạo ra những tác động tích cực ngoài đời thực. Sinh viên có thể áp dụng nhiều chiến lược để đóng góp, như chia sẻ tri thức chuyên ngành, lan tỏa các sáng kiến cộng đồng, công khai chúc mừng thành công của người khác, và tự tạo ra các nội dung gốc mang tính xây dựng nếu có khả năng.

Một khía cạnh quan trọng của việc ủng hộ nội dung tích cực là thực hành vai trò "Đồng minh số" (Digital Allyship). Đây là việc một người sử dụng vị thế và tiếng nói của mình để ủng hộ và bảo vệ các cá nhân hoặc nhóm người yếu thế trên không gian mạng. Trở thành một đồng minh tích cực bao gồm việc lắng nghe và học hỏi về trải nghiệm của các cộng đồng khác, khuếch đại tiếng nói của họ bằng cách chia sẻ bài viết của họ, và can thiệp một cách an toàn khi thấy một người bị công kích. Hành động đồng minh cần xuất phát từ sự chân thành và mong muốn tạo ra thay đổi, chứ không phải để biểu diễn đạo đức.

3. Hỗ trợ bạn bè khi thấy dấu hiệu bị ảnh hưởng tâm lý

Môi trường số cũng là nơi các dấu hiệu bất ổn tâm lý có thể bộc lộ, và việc trở thành một người bạn biết quan sát và hỗ trợ đúng cách là một kỹ năng xã hội vô cùng quan trọng. Mặc dù bạn không phải là một nhà chuyên môn để chẩn đoán, bạn có thể nhận ra những thay đổi trong hành vi của bạn bè. Các dấu hiệu này có thể bao gồm sự thay đổi trong nội dung đăng tải (nhiều hơn về cảm giác cô đơn, tuyệt vọng), thay đổi trong tần suất hoạt động (biến mất hoặc hoạt động ám ảnh), rút lui khỏi các tương tác xã hội, hoặc chia sẻ các nội dung nhạy cảm về ý định tự hại. Khi nhận thấy các dấu hiệu trên, hãy tiếp cận một cách riêng tư và tế nhị, tuyệt đối không bình luận công khai. Hãy gửi một tin nhắn riêng, bắt đầu một cách nhẹ nhàng để bày tỏ sự quan tâm và sẵn sàng lắng nghe. Nếu họ chia sẻ, nhiệm vụ quan trọng nhất của bạn là lắng nghe không phán xét và xác thực cảm xúc của họ, thay vì đưa ra những lời sáo rỗng. Hãy thử đề nghị những sự giúp đỡ cụ thể thay vì hỏi chung chung.

Điều quan trọng nhất cần nhớ là bạn là một người bạn, không phải một nhà trị liệu. Do đó, vai trò thiết yếu của bạn là kết nối họ với những người có chuyên môn. Hãy chủ động tìm hiểu và lưu lại thông tin liên lạc của các nguồn lực hỗ trợ như Phòng Tư vấn Tâm lý của trường hoặc các đường dây nóng uy tín. Bạn có thể gợi ý một cách khéo léo và đề nghị đi cùng nếu họ muốn. Trong trường hợp khẩn cấp, nếu

bạn có lý do để tin rằng bạn của mình đang có nguy cơ tự hại tức thời, đừng giữ bí mật. Hãy liên hệ ngay với các dịch vụ khẩn cấp, phòng công tác sinh viên của trường hoặc một người lớn mà bạn tin tưởng. Việc lắng nghe và hỗ trợ một người bạn đang gặp khó khăn có thể rất nặng nề về mặt cảm xúc. Vì vậy, người hỗ trợ cũng phải biết cách chăm sóc bản thân bằng cách đặt ra ranh giới, tìm kiếm sự hỗ trợ cho chính mình và dành thời gian cho các hoạt động tái tạo năng lượng để tránh bị kiệt sức.

4. Tham gia cộng đồng an toàn số

Hành động cá nhân là quan trọng, nhưng sức mạnh tập thể mới có thể tạo ra những thay đổi bền vững. Việc tham gia các câu lạc bộ, diễn đàn về An toàn thông tin hay Truyền thông số mang lại nhiều lợi ích : giúp nâng cao kiến thức và kỹ năng, có cơ hội thực hành qua các sự kiện, và xây dựng mạng lưới với những người cùng mối quan tâm. Sinh viên có một lợi thế đặc biệt là hiểu rõ ngôn ngữ và các kênh giao tiếp hiệu quả nhất với bạn bè đồng trang lứa. Các bạn có thể tạo ra các sản phẩm truyền thông sáng tạo và dễ tiếp cận như infographic, video TikTok để truyền tải các thông điệp về an toàn số một cách hấp dẫn, hoặc tổ chức các sự kiện ngang hàng (peer-to-peer) để nâng cao nhận thức. Sinh viên có thể chủ động đề xuất và thực hiện các dự án cụ thể như tổ chức "Tuần lễ An toàn số" với chuỗi workshop và buổi nói chuyện, xây dựng chương trình "Đại sứ An toàn số" để tư vấn cho các bạn khác, hoặc phát triển bộ "Cẩm nang Sinh tồn số" với các tài liệu trực quan.

Cấp độ cao nhất của vai trò công dân số là trở thành một người ủng hộ (advocate) cho một môi trường số an toàn, không chỉ bảo vệ bản thân và bạn bè mà còn hành động vì một môi trường chung tốt đẹp hơn. Khi chứng kiến điều sai trái như bắt nạt trực tuyến, đừng im lặng. Bạn có thể hành động bằng cách báo cáo (Report) nội dung vi phạm cho nền tảng, gửi tin nhắn riêng để hỗ trợ và động viên nạn nhân, hoặc lên tiếng phản đối hành vi đó một cách văn minh nếu cảm thấy an toàn. Hơn nữa, hãy tham gia và ủng hộ các chiến dịch, ký tên vào các bản kiến nghị nhằm yêu cầu các công ty công nghệ và các nhà hoạch định chính sách phải có trách nhiệm hơn trong việc bảo vệ người dùng.

Bằng cách đảm nhận những vai trò này, mỗi sinh viên đang từ một người dùng thụ động trở thành một tác nhân thay đổi tích cực, góp phần xây dựng một hệ sinh thái số nhân văn, an toàn và phát triển bền vững. Khi công nghệ tiếp tục phát triển, vai trò

của công dân số sẽ càng trở nên phức tạp hơn. Sinh viên cần chuẩn bị cho một tương lai nơi ranh giới giữa thực và ảo ngày càng mờ nhạt với sự xuất hiện của Trí tuệ Nhân tạo và Metaverse. Các vấn đề mới sẽ nảy sinh liên quan đến đạo đức AI, bản dạng trong thế giới ảo, và quyền sở hữu dữ liệu. Trở thành một công dân số có trách nhiệm trong tương lai không chỉ là về việc sử dụng công nghệ một cách an toàn, mà còn là tham gia tích cực vào các cuộc đối thoại xã hội để định hình các quy tắc, chuẩn mực và luật lệ cho những công nghệ mới này, đảm bảo chúng phục vụ cho lợi ích chung của con người.

BÀI 4: BẢO VỆ MÔI TRƯỜNG

Trong kỷ nguyên mà từng ngóc ngách cuộc sống đều được số hóa, từ cách chúng ta giao tiếp, làm việc cho đến giải trí, công nghệ đã trở thành một phần không thể thiếu. Sự phát triển vũ bão của nó mang đến vô vàn lợi ích, định hình một thế giới hiện đại đầy tiện nghi. Tuy nhiên, đằng sau bức tranh rực rỡ ấy, một câu hỏi cấp bách đang dần nổi lên: Mối quan hệ giữa công nghệ số và môi trường thực sự là gì? Liệu tiến bộ công nghệ có đang vô tình đánh đổi bằng sức khỏe của hành tinh chúng ta? Hay ngược lại, nó chính là chìa khóa để giải quyết những thách thức môi trường lớn nhất của thời đại?

Tài liệu này được biên soạn nhằm mang đến một cái nhìn toàn diện và sâu sắc về mối liên hệ phức tạp này. Chúng ta sẽ không chỉ nhận diện những khái niệm cơ bản của công nghệ số, mà còn đi sâu phân tích những đóng góp tích cực mà nó mang lại trong việc bảo vệ môi trường, cũng như đối mặt với những thách thức và hệ lụy tiêu cực cần được giải quyết. Với cấu trúc dạng sách giáo trình, tài liệu này hy vọng sẽ là một nguồn tham khảo hữu ích, khơi gợi tư duy và hành động cho sinh viên, nhà nghiên cứu, các nhà hoạch định chính sách và bất kỳ ai quan tâm đến tương lai bền vững của Trái Đất trong bối cảnh công nghệ không ngừng phát triển.

PHẦN I: NHẬN DIỆN CÔNG NGHỆ SỐ

Chào mừng bạn đến với phần đầu tiên của bộ tài liệu, nơi chúng ta sẽ đặt nền móng cho việc hiểu rõ mối quan hệ giữa công nghệ và môi trường. Trước khi đi sâu vào những tác động cụ thể, điều quan trọng là phải có một cái nhìn rõ ràng về bản chất của công nghệ số – một khái niệm tưởng chừng quen thuộc nhưng lại vô cùng rộng lớn và đa diện. phần này sẽ đưa bạn qua định nghĩa cơ bản, khám phá các thành phần cốt lõi tạo nên hệ sinh thái số phức tạp mà chúng ta đang sống, từ phần cứng vật lý, phần mềm vô hình, đến mạng lưới kết nối toàn cầu và khối lượng dữ liệu khổng lồ. Chúng ta cũng sẽ điểm qua những xu hướng công nghệ số nổi bật nhất hiện nay như Trí tuệ Nhân tạo, IoT, Điện toán đám mây và Blockchain, những xu hướng đang định hình tương lai và mang theo những tiềm năng cũng như thách thức không nhỏ đối với môi trường. Hiểu rõ "chất liệu" của cuộc cách mạng số này chính là bước khởi đầu để chúng ta đánh giá được dấu chân môi trường của nó.

1. Định nghĩa và đặc điểm

Công nghệ số (Digital Technology) là tập hợp các công nghệ sử dụng tín hiệu số, được biểu diễn bằng các giá trị rời rạc 0 và 1, để xử lý, lưu trữ, truyền tải và hiển thị thông tin. Khác với tín hiệu tương tự (analog) liên tục, công nghệ số chuyển đổi mọi loại dữ liệu – từ âm thanh, hình ảnh, video đến văn bản – thành dạng số hóa, cho phép chúng được xử lý và quản lý hiệu quả hơn bằng các thiết bị điện tử. Sự chuyển đổi này là nền tảng cho mọi tiến bộ công nghệ hiện đại mà chúng ta đang chứng kiến, từ chiếc điện thoại thông minh trong túi đến các siêu máy tính phức tạp.

Các đặc điểm nổi bật của công nghệ số đã tạo nên cuộc cách mạng trong nhiều lĩnh vực. Thứ nhất, nó mang lại tính chính xác và độ tin cậy cao; do sử dụng tín hiệu rời rạc, thông tin số ít bị nhiễu và méo mó hơn so với tín hiệu tương tự, giúp duy trì chất lượng dữ liệu trong quá trình truyền tải và xử lý. Ví dụ, khi bạn gửi một bức ảnh kỹ thuật số qua mạng, bức ảnh đó sẽ đến người nhận với chất lượng y hệt bản gốc, không bị "mờ nhòe" hay "nhiễu" như khi truyền tín hiệu analog qua khoảng cách xa. Thứ hai, thông tin số dễ dàng sao chép và phân phối mà không làm giảm chất lượng, đồng thời có thể truyền tải nhanh chóng qua mạng internet, tạo điều kiện cho sự lan truyền tri thức và thông tin chưa từng có. Điển hình là một bài báo điện tử có thể được hàng triệu người đọc cùng lúc trên khắp thế giới mà không tốn giấy mực hay thời gian

vận chuyển. Thứ ba, công nghệ số có khả năng xử lý tự động cao; các thuật toán và phần mềm có thể được lập trình để xử lý lượng lớn dữ liệu một cách tự động và với tốc độ vượt trội. Chẳng hạn, một phần mềm kế toán có thể xử lý hàng nghìn giao dịch tài chính trong vài giây, hoặc một hệ thống nhận diện khuôn mặt có thể quét hàng triệu bức ảnh để tìm kiếm thông tin mong muốn. Cuối cùng, tính tương thích và kết nối là một ưu điểm vượt trội, cho phép các thiết bị và hệ thống số khác nhau dễ dàng kết nối và tương tác với nhau, tạo thành các mạng lưới phức tạp và mở ra tiềm năng ứng dụng không giới hạn trong tương lai. Điển hình là điện thoại thông minh của bạn có thể kết nối với loa Bluetooth, đồng hồ thông minh, TV và thậm chí là hệ thống chiếu sáng trong nhà, tạo nên một hệ sinh thái kết nối liền mạch.

2. Các thành phần chính của công nghệ số

Công nghệ số không phải là một thực thể đơn lẻ mà là một hệ thống phức tạp bao gồm nhiều thành phần cốt lõi, hoạt động đồng bộ để tạo nên các hệ thống và ứng dụng đa dạng mà chúng ta sử dụng hàng ngày. Hiểu rõ các thành phần này là điều cần thiết để đánh giá toàn diện tác động của chúng đến môi trường.

2.1. Phần cứng (Hardware)

Phần cứng là các thiết bị vật lý, bộ phận hữu hình tạo nên hệ thống công nghệ số, đóng vai trò nền tảng cho việc xử lý, lưu trữ và truyền tải dữ liệu. Đây là các thành phần vật chất mà chúng ta có thể nhìn thấy và chạm vào. Các loại phần cứng phổ biến bao gồm máy tính cá nhân (PC) và máy tính xách tay (Laptop), những thiết bị đa năng phục vụ cả mục đích cá nhân và công việc, từ xử lý văn bản đến chơi game. Máy chủ (Servers) là những máy tính mạnh mẽ hơn, được thiết kế để cung cấp dịch vụ và tài nguyên cho các máy tính khác trong mạng, thường đặt tại các trung tâm dữ liệu. Thiết bị di động (Smartphones, Tablets) là các thiết bị cầm tay nhỏ gọn, tích hợp nhiều chức năng như giao tiếp, truy cập internet, chụp ảnh và là cổng kết nối chính của hàng tỷ người dùng với thế giới số. Thiết bị mạng (Routers, Switches) là những thành phần thiết yếu để kết nối các máy tính và thiết bị khác trong một mạng lưới, đảm bảo luồng dữ liệu thông suốt. Đặc biệt, sự phát triển của thiết bị IoT (Internet of Things) đã mở rộng khái niệm phần cứng sang các cảm biến và thiết bị thông minh được kết nối internet để thu thập và trao đổi dữ liệu tự động, từ camera an ninh đến thiết bị nhà thông minh. Ví dụ cụ thể về phần cứng bao gồm một chiếc iPhone, một máy chủ của

Google đặt tại trung tâm dữ liệu, hoặc một cảm biến độ ẩm đất được gắn trên cánh đồng nông nghiệp. Tất cả những thiết bị này, dù lớn hay nhỏ, đều cần được sản xuất, sử dụng năng lượng và cuối cùng trở thành rác thải, tạo nên dấu chân môi trường đáng kể.

2.2. Phần mềm (Software)

Phần mềm là các chương trình và ứng dụng chạy trên phần cứng, cung cấp các hướng dẫn và chức năng cho thiết bị, cho phép người dùng tương tác và thực hiện các tác vụ cụ thể. Nếu phần cứng là bộ não và cơ thể, thì phần mềm là trí tuệ và linh hồn của hệ thống số. Các loại phần mềm chính bao gồm: Hệ điều hành (Operating Systems) như Windows, macOS, Android, iOS, chúng quản lý tài nguyên phần cứng và cung cấp môi trường để các ứng dụng khác hoạt động. Đây là nền tảng cơ bản nhất mà mọi thiết bị số đều cần có. Ví dụ, hệ điều hành Android trên điện thoại của bạn quản lý mọi thứ từ màn hình cảm ứng đến kết nối Wi-Fi. Ứng dụng (Applications) là các chương trình được thiết kế để thực hiện các chức năng cụ thể, từ trình duyệt web, phần mềm xử lý văn bản, đến ứng dụng chỉnh sửa ảnh và trò chơi điện tử. Chúng là những công cụ mà người dùng tương tác trực tiếp để hoàn thành công việc hoặc giải trí. Điển hình là ứng dụng Zalo để nhắn tin, trình duyệt Google Chrome để lướt web, hay phần mềm Microsoft Word để soạn thảo văn bản. Cuối cùng, phần mềm nhúng (Embedded Software) là các chương trình được tích hợp trực tiếp vào phần cứng để điều khiển các thiết bị cụ thể, thường là các thiết bị không phải máy tính đa năng, ví dụ như phần mềm trong tủ lạnh thông minh, đồng hồ thông minh hoặc hệ thống điều khiển trong ô tô. Bạn có thể thấy phần mềm nhúng điều khiển nhiệt độ chính xác trong tủ lạnh thông minh hoặc giúp đồng hồ thông minh đo nhịp tim của bạn. Mặc dù phần mềm không có tác động vật lý trực tiếp, nhưng việc phát triển, duy trì và chạy phần mềm đòi hỏi tài nguyên tính toán và năng lượng, góp phần gián tiếp vào dấu chân môi trường của công nghệ số.

2.3. Mạng và kết nối (Networks and Connectivity)

Mạng và kết nối là yếu tố cốt lõi giúp các thiết bị số giao tiếp và trao đổi thông tin với nhau, tạo nên một thế giới kết nối không ngừng. Không có mạng, các thiết bị phần cứng sẽ chỉ là những cỗ máy đơn độc. Internet, mạng máy tính toàn cầu, là xương sống của mọi hoạt động số hóa hiện đại, cho phép hàng tỷ thiết bị kết nối và

trao đổi thông tin xuyên biên giới. Mỗi khi bạn truy cập một trang web hoặc gửi email, bạn đang sử dụng mạng Internet. Sự phát triển của mạng di động (3G, 4G, 5G) đã cách mạng hóa cách chúng ta truy cập internet, cho phép kết nối không dây tốc độ cao qua các thiết bị di động ở hầu hết mọi nơi. Điển hình là việc bạn xem video trực tuyến mượt mà trên điện thoại khi đang di chuyển nhờ kết nối 4G hoặc 5G. Wi-Fi cung cấp khả năng kết nối mạng không dây cục bộ, tiện lợi cho các thiết bị trong nhà hoặc văn phòng. Laptop của bạn kết nối internet tại nhà thông qua Wi-Fi router. Đặc biệt, công nghệ đám mây (Cloud Computing) đã thay đổi cách chúng ta lưu trữ và truy cập dữ liệu; thay vì sở hữu và duy trì cơ sở hạ tầng vật lý tại chỗ, người dùng và doanh nghiệp có thể thuê tài nguyên điện toán (máy chủ, lưu trữ, cơ sở dữ liệu, phần mềm) từ các nhà cung cấp dịch vụ thông qua internet. Google Drive, Dropbox, và iCloud là những ví dụ về dịch vụ đám mây nơi bạn lưu trữ ảnh và tài liệu mà không cần tải về máy tính. Mạng lưới này tiêu thụ một lượng lớn năng lượng để vận hành các thiết bị chuyển mạch, router và đặc biệt là các trung tâm dữ liệu khổng lồ, nơi lưu trữ "đám mây", đây là một trong những điểm tác động môi trường đáng kể của công nghệ số.

2.4. Dữ liệu (Data)

Dữ liệu là nguyên liệu thô, là máu của công nghệ số. Mọi hoạt động số đều tạo ra, xử lý, lưu trữ và sử dụng dữ liệu, biến nó thành một trong những tài sản quan trọng nhất trong kỷ nguyên hiện đại. Ngày nay, chúng ta đang chứng kiến sự bùng nổ của dữ liệu lớn (Big Data) – thuật ngữ chỉ các tập dữ liệu có khối lượng cực lớn, đa dạng về định dạng (văn bản, hình ảnh, video, âm thanh) và tốc độ cập nhật nhanh, đến mức các công cụ xử lý dữ liệu truyền thống không thể xử lý hiệu quả. Ví dụ, dữ liệu về hàng tỷ giao dịch mua sắm trực tuyến mỗi ngày trên Amazon, hay hàng triệu tin nhắn và hình ảnh được chia sẻ trên Facebook, đều là Big Data. Việc thu thập, lưu trữ và phân tích Big Data đòi hỏi cơ sở hạ tầng mạnh mẽ và tiêu tốn nhiều tài nguyên. Để quản lý lượng dữ liệu khổng lồ này một cách có hệ thống, cơ sở dữ liệu (Databases) được sử dụng. Đây là các hệ thống được tổ chức để lưu trữ, quản lý và truy xuất dữ liệu một cách hiệu quả và an toàn. Một ví dụ về cơ sở dữ liệu là hệ thống lưu trữ thông tin khách hàng của một ngân hàng, hay danh sách sản phẩm trên một trang thương mại điện tử. Mặc dù dữ liệu tự thân không phải là vật chất, nhưng vòng đời của dữ liệu – từ việc tạo ra, truyền tải, lưu trữ đến phân tích và xóa bỏ – đều liên quan mật thiết đến

việc tiêu thụ năng lượng và tài nguyên của các thành phần phần cứng và mạng lưới, từ đó góp phần vào dấu chân môi trường của công nghệ số.

3. Các xu hướng công nghệ số nổi bật

Sự phát triển không ngừng của công nghệ số đã tạo ra nhiều xu hướng nổi bật, định hình tương lai của chúng ta và mang theo những tác động sâu sắc, đa chiều đến môi trường. Việc nắm bắt các xu hướng này giúp chúng ta hình dung rõ hơn về những cơ hội và thách thức phía trước.

3.1. Trí tuệ nhân tạo (Artificial Intelligence - AI)

Trí tuệ nhân tạo (AI) là khả năng của máy móc học hỏi, suy luận, nhận thức và giải quyết vấn đề tương tự như con người. AI không chỉ là một công nghệ đơn lẻ mà là một lĩnh vực rộng lớn bao gồm học máy (Machine Learning), học sâu (Deep Learning), xử lý ngôn ngữ tự nhiên (Natural Language Processing) và nhiều nhánh khác. AI đang được ứng dụng rộng rãi từ xe tự lái, nhận diện khuôn mặt, hệ thống khuyến nghị trên các nền tảng số, đến việc phân tích dữ liệu phức tạp trong y học và khoa học khí hậu. Ví dụ, trợ lý ảo Siri hoặc Google Assistant sử dụng AI để hiểu và phản hồi yêu cầu của bạn. Trong ngành y tế, AI giúp chẩn đoán bệnh chính xác hơn qua phân tích hình ảnh y tế. Mặc dù AI có tiềm năng to lớn trong việc tối ưu hóa tài nguyên và dự báo môi trường (như sẽ được thảo luận ở phần 2), nhưng quá trình huấn luyện các mô hình AI lớn, đặc biệt là các mô hình học sâu, đòi hỏi sức mạnh tính toán khổng lồ và tiêu thụ một lượng năng lượng đáng kể, tạo ra một dấu chân carbon không nhỏ.

3.2. Internet vạn vật (Internet of Things - IoT)

Internet vạn vật (IoT) là một mạng lưới rộng lớn của các thiết bị vật lý được nhúng cảm biến, phần mềm và các công nghệ khác, cho phép chúng kết nối và trao đổi dữ liệu với các hệ thống và thiết bị khác qua internet. Từ các thiết bị gia dụng thông minh, thiết bị đeo tay, đến các cảm biến công nghiệp và hệ thống thành phố thông minh, IoT đang biến mọi vật thể xung quanh chúng ta thành một phần của mạng lưới số. Ví dụ, một chiếc tủ lạnh thông minh có thể thông báo cho bạn khi hết sữa, hay một vòng đeo tay thông minh theo dõi nhịp tim và hoạt động thể chất của bạn. IoT giúp thu thập dữ liệu theo thời gian thực về môi trường, hiệu suất hoạt động và hành vi người dùng, từ đó cho phép tối ưu hóa tài nguyên và đưa ra quyết định thông minh hơn. Tuy

nhiên, sự bùng nổ của các thiết bị IoT cũng đặt ra thách thức về sản xuất hàng loạt thiết bị, tiêu thụ năng lượng cho việc truyền tải và xử lý dữ liệu, cũng như vấn đề rác thải điện tử khi các thiết bị này lỗi thời.

3.3. Điện toán đám mây (Cloud Computing)

Điện toán đám mây (Cloud Computing) là một mô hình cung cấp tài nguyên điện toán (máy chủ, lưu trữ, cơ sở dữ liệu, mạng, phần mềm, phân tích) theo yêu cầu qua internet, thay vì người dùng phải sở hữu và duy trì cơ sở hạ tầng vật lý cục bộ. Các nhà cung cấp dịch vụ đám mây lớn như Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform quản lý và vận hành các trung tâm dữ liệu khổng lồ, cho phép các doanh nghiệp và cá nhân truy cập tài nguyên một cách linh hoạt và hiệu quả về chi phí. Khi bạn sử dụng Google Docs để soạn thảo văn bản trực tuyến, hoặc xem phim trên Netflix, bạn đang sử dụng dịch vụ đám mây. Điện toán đám mây giúp giảm nhu cầu về phần cứng cục bộ, tối ưu hóa việc sử dụng tài nguyên và mở rộng quy mô dễ dàng. Tuy nhiên, bản thân các trung tâm dữ liệu đám mây lại là những "người khổng lồ" về tiêu thụ năng lượng, đặt ra áp lực lớn trong việc tìm kiếm các nguồn năng lượng sạch và giảm thiểu dấu chân carbon của chúng.

3.4. Chuỗi khối (Blockchain)

Chuỗi khối (Blockchain) là một công nghệ sổ cái phân tán, phi tập trung và an toàn, nơi các giao dịch được ghi lại thành các "khối" và liên kết với nhau bằng mật mã. Mỗi khối chứa một dấu thời gian và liên kết đến khối trước đó, tạo thành một chuỗi không thể thay đổi. Công nghệ này thường được biết đến nhiều nhất thông qua các loại tiền điện tử như Bitcoin và Ethereum. Bitcoin là ví dụ nổi bật nhất về ứng dụng của Blockchain, nơi mọi giao dịch được ghi lại công khai và không thể thay đổi. Tuy nhiên, Blockchain có tiềm năng ứng dụng trong nhiều lĩnh vực khác ngoài tài chính, bao gồm quản lý chuỗi cung ứng minh bạch, theo dõi nguồn gốc sản phẩm, và quản lý năng lượng tái tạo. Ví dụ, một công ty có thể dùng Blockchain để theo dõi nguồn gốc cà phê từ nông trại đến tách cà phê trên bàn bạn, đảm bảo tính bền vững và công bằng. Mặc dù hứa hẹn về tính minh bạch và bảo mật, nhưng các cơ chế đồng thuận của một số Blockchain, đặc biệt là Proof of Work (PoW) được sử dụng bởi Bitcoin, đòi hỏi sức mạnh tính toán cực lớn và tiêu thụ một lượng năng lượng điện khổng lồ, gây ra lo ngại đáng kể về tác động môi trường.

3.5. Thực tế ảo (Virtual Reality - VR) và Thực tế tăng cường (Augmented Reality - AR)

Thực tế ảo (VR) và Thực tế tăng cường (AR) là hai công nghệ đang cách mạng hóa cách chúng ta tương tác với thế giới kỹ thuật số. VR tạo ra một môi trường mô phỏng hoàn toàn, tách biệt người dùng khỏi thế giới thực (ví dụ: qua kính VR), mang lại trải nghiệm nhập vai sâu sắc. Với VR, bạn có thể "du hành" đến một rừng mưa nhiệt đới hoặc tham quan bảo tàng ảo ngay tại nhà. Trong khi đó, AR chồng các yếu tố ảo (hình ảnh, thông tin kỹ thuật số) lên thế giới thực thông qua camera của điện thoại thông minh hoặc kính AR, tăng cường trải nghiệm thực tại. Trò chơi Pokémon Go là một ví dụ phổ biến về AR, nơi bạn thấy các nhân vật hoạt hình xuất hiện trong môi trường thực của mình qua màn hình điện thoại. Các công nghệ này có tiềm năng ứng dụng trong giáo dục, đào tạo (ví dụ: mô phỏng các thảm họa môi trường), du lịch ảo (giảm nhu cầu di chuyển vật lý), và thậm chí là thiết kế sản phẩm bền vững. Tuy nhiên, việc sản xuất các thiết bị VR/AR phức tạp đòi hỏi nhiều vật liệu và năng lượng, và việc sử dụng chúng cũng tiêu tốn điện năng, đặt ra yêu cầu về thiết kế và sử dụng bền vững để tối thiểu hóa tác động môi trường.

PHẦN II: CÔNG NGHỆ SỐ TÁC ĐỘNG TÍCH CỰC ĐẾN MÔI TRƯỜNG

Trong bối cảnh biến đổi khí hậu và suy thoái môi trường đang là những thách thức toàn cầu cấp bách, câu hỏi đặt ra là liệu công nghệ có thể là một phần của giải pháp? phần này sẽ đưa bạn vào một hành trình khám phá những khía cạnh tích cực, nơi công nghệ số vươn lên trở thành một công cụ mạnh mẽ, mang tính đột phá trong cuộc chiến bảo vệ và phục hồi hành tinh của chúng ta. Chúng ta sẽ cùng nhau tìm hiểu cách các giải pháp số hóa đang cách mạng hóa khả năng giám sát và quản lý môi trường, giúp tối ưu hóa việc sử dụng tài nguyên và giảm thiểu phát thải, đồng thời nâng cao nhận thức và thúc đẩy hành động vì một tương lai bền vững. Từ những cảm biến nhỏ bé đến dữ liệu vệ tinh khổng lồ, công nghệ số đang mở ra những cánh cửa mới để chúng ta hiểu, bảo vệ và chung sống hài hòa hơn với thiên nhiên.

1. Giám sát và quản lý môi trường hiệu quả

Khả năng thu thập và xử lý dữ liệu theo thời gian thực của công nghệ số đã cách mạng hóa việc giám sát và quản lý môi trường. Những công cụ này cung cấp cái nhìn sâu sắc và kịp thời về tình trạng hành tinh của chúng ta.

1.1. Giám sát chất lượng không khí và nước

Công nghệ số đã biến đổi hoàn toàn cách chúng ta theo dõi và phản ứng với ô nhiễm không khí và nước. Việc triển khai các cảm biến thông minh và hệ thống IoT đã cho phép thu thập dữ liệu chi tiết về chất lượng môi trường ở quy mô lớn. Các cảm biến này có thể được lắp đặt tại các thành phố, khu công nghiệp, dọc theo sông hồ để liên tục đo lường các chỉ số như nồng độ PM2.5, CO2, SO2, NOx trong không khí hoặc pH, oxy hòa tan, nhiệt độ, và sự hiện diện của hóa chất trong nước. Dữ liệu thu thập được truyền về trung tâm để phân tích bằng các thuật toán tiên tiến, cung cấp thông tin theo thời gian thực về mức độ ô nhiễm, giúp các cơ quan chức năng đưa ra cảnh báo kịp thời và áp dụng biện pháp xử lý phù hợp. Ví dụ, ở Seoul (Hàn Quốc) hoặc Bắc Kinh (Trung Quốc), các ứng dụng di động hiển thị chỉ số chất lượng không khí theo thời gian thực dựa trên dữ liệu từ mạng lưới cảm biến dày đặc, giúp người dân biết khi nào nên đeo khẩu trang hoặc hạn chế ra ngoài. Ngoài ra, việc sử dụng drone và vệ tinh đã mở rộng khả năng giám sát lên quy mô rộng lớn hơn nhiều. Drone được trang bị camera độ phân giải cao và cảm biến chuyên dụng có thể bay qua các khu vực

xa xôi, khó tiếp cận như rừng sâu, đất ngập nước hoặc bãi biển để phát hiện nạn phá rừng, ô nhiễm dầu tràn hay tình trạng suy thoái môi trường ở cấp độ vi mô. Chẳng hạn, các tổ chức bảo tồn như WWF sử dụng drone để theo dõi các khu rừng Amazon, phát hiện sớm các hoạt động khai thác gỗ trái phép. Đồng thời, dữ liệu vệ tinh cung cấp cái nhìn vĩ mô, toàn cảnh về các hiện tượng môi trường lớn như biến đổi khí hậu, sự nóng lên toàn cầu, mực nước biển dâng, sự thay đổi của thảm thực vật hay sự di chuyển của khối không khí ô nhiễm, cho phép các nhà khoa học xây dựng mô hình dự báo và đánh giá tác động dài hạn. NASA và ESA (Cơ quan Vũ trụ châu Âu) liên tục cung cấp dữ liệu vệ tinh giúp các nhà khoa học theo dõi sự tan chảy của sông băng và biến đổi khí hậu toàn cầu.

1.2. Quản lý rừng và đa dạng sinh học

Trong lĩnh vực bảo tồn rừng và đa dạng sinh học, công nghệ số đã trở thành một đồng minh không thể thiếu. Việc kết hợp Hệ thống Thông tin Địa lý (GIS) với công nghệ Viễn thám (Remote Sensing) từ vệ tinh và drone đã cho phép lập bản đồ chi tiết, theo dõi sự thay đổi của diện tích rừng, phát hiện sớm các đám cháy rừng và nạn phá rừng trái phép với độ chính xác cao. Một ví dụ là Global Forest Watch, một nền tảng trực tuyến sử dụng dữ liệu vệ tinh để cung cấp cảnh báo về nạn phá rừng theo thời gian thực cho các quốc gia và tổ chức trên thế giới. Các thuật toán AI có thể phân tích hàng triệu hình ảnh vệ tinh để tự động nhận diện các khu vực bị ảnh hưởng, dự đoán nguy cơ cháy rừng và hỗ trợ công tác quy hoạch bảo tồn. Đối với việc bảo vệ động vật hoang dã, các thiết bị theo dõi gắn GPS trên động vật hoặc camera bẫy kết nối IoT giúp các nhà bảo tồn theo dõi hành vi, lộ trình di cư, tình trạng sức khỏe của các loài nguy cấp theo thời gian thực. Tổ chức Wildlife Conservation Society (WCS) sử dụng vòng cổ GPS gắn cho voi để theo dõi đường di cư và bảo vệ chúng khỏi những kẻ săn trộm ở châu Phi. Điều này cung cấp dữ liệu quý giá để đưa ra các biện pháp bảo vệ phù hợp, xác định các khu vực sinh sống quan trọng và ngăn chặn nạn săn bắn trộm. Thậm chí, AI còn có khả năng phân tích âm thanh trong rừng để phát hiện tiếng cưa máy hoặc tiếng súng săn, cảnh báo kịp thời về các hoạt động khai thác trái phép. Dự án "Guardian" của Rainforest Connection sử dụng điện thoại thông minh cũ lắp đặt trong rừng để nghe lén tiếng cưa máy và cảnh báo lực lượng bảo vệ.

1.3. Dự báo và cảnh báo thiên tai

Công nghệ số đóng vai trò then chốt trong việc cải thiện khả năng dự báo và cảnh báo thiên tai, giảm thiểu thiệt hại về người và của. Các mô hình dự báo thời tiết và khí hậu dựa trên Big Data và AI sử dụng sức mạnh của siêu máy tính và thuật toán phức tạp để xử lý lượng lớn dữ liệu khí tượng thủy văn lịch sử và hiện tại. Từ đó, chúng có thể đưa ra dự báo chính xác hơn về các hiện tượng thời tiết cực đoan như bão, lũ lụt, hạn hán, hoặc sóng thần. Trung tâm Dự báo Khí tượng Thủy văn Quốc gia Việt Nam sử dụng các mô hình số và dữ liệu vệ tinh để dự báo đường đi của bão, giúp các tỉnh ven biển sơ tán dân kịp thời. Độ chính xác được nâng cao này giúp các cộng đồng có thời gian chuẩn bị, sơ tán kịp thời và triển khai các biện pháp phòng ngừa. Bên cạnh đó, các hệ thống cảnh báo sớm dựa trên IoT và công nghệ di động đã được phát triển để gửi cảnh báo trực tiếp đến người dân ở các khu vực có nguy cơ cao. Ví dụ, ở Nhật Bản, hệ thống cảnh báo sớm động đất tự động gửi thông báo đến điện thoại di động và kích hoạt hệ thống dừng tàu điện trước khi sóng địa chấn mạnh nhất đến. Khả năng cung cấp thông tin kịp thời và chính xác này giúp cứu sống nhiều người và giảm thiểu tác động tàn phá của thiên tai.

2. Tối ưu hóa tài nguyên và giảm phát thải

Một trong những đóng góp quan trọng nhất của công nghệ số là khả năng tối ưu hóa việc sử dụng tài nguyên và giảm thiểu phát thải trong nhiều lĩnh vực, từ năng lượng đến nông nghiệp và giao thông.

2.1. Năng lượng thông minh và lưới điện thông minh

Công nghệ số là nền tảng cho sự chuyển đổi sang một hệ thống năng lượng hiệu quả và bền vững hơn. Lưới điện thông minh (Smart Grid) ứng dụng công nghệ số để quản lý và phân phối điện hiệu quả hơn bằng cách tích hợp các cảm biến, hệ thống điều khiển và công nghệ thông tin. Hệ thống này giúp cân bằng cung cầu điện năng theo thời gian thực, giảm tổn thất trong quá trình truyền tải, đồng thời tích hợp năng lượng tái tạo (như điện mặt trời và gió) vào lưới điện một cách ổn định và đáng tin cậy hơn, khắc phục tính không liên tục của chúng. Ở Đức, dự án Energiewende đã triển khai lưới điện thông minh để tích hợp thành công lượng lớn năng lượng tái tạo, giảm sự phụ thuộc vào nhiên liệu hóa thạch. Trong các đô thị, tòa nhà thông minh (Smart Buildings) sử dụng hệ thống quản lý năng lượng dựa trên IoT để tự động điều khiển ánh sáng, điều hòa không khí và hệ thống sưởi ấm dựa trên sự hiện diện của người

dùng, điều kiện môi trường bên ngoài và lịch trình hoạt động. Tòa nhà The Edge ở Amsterdam là một ví dụ điển hình, nơi hệ thống thông minh giúp giảm 70% mức tiêu thụ năng lượng so với các tòa nhà văn phòng thông thường. Điều này giúp giảm đáng kể lượng năng lượng tiêu thụ không cần thiết. Ngoài ra, công nghệ số còn giúp tối ưu hóa sản xuất năng lượng tái tạo bằng cách dự đoán chính xác hơn sản lượng điện từ các trang trại năng lượng mặt trời và gió dựa trên dữ liệu thời tiết, từ đó tăng cường hiệu quả và mức độ phụ thuộc vào các nguồn năng lượng sạch này.

2.2. Nông nghiệp thông minh

Nông nghiệp thông minh là một ví dụ điển hình về cách công nghệ số có thể cải thiện hiệu quả tài nguyên trong một lĩnh vực truyền thống. Việc sử dụng cảm biến đất và hệ thống IoT cho phép nông dân thu thập dữ liệu chính xác và liên tục về độ ẩm, pH, dinh dưỡng và nhiệt độ của đất. Dựa vào những dữ liệu này, hệ thống tưới tiêu tự động và bón phân chính xác có thể được áp dụng, chỉ cung cấp đúng lượng nước và phân bón cần thiết cho từng khu vực hoặc từng cây trồng. Ví dụ, công ty CropX cung cấp các cảm biến đất thông minh và phần mềm dựa trên AI giúp nông dân Israel tiết kiệm đến 50% lượng nước tưới tiêu. Điều này giúp tiết kiệm đáng kể lượng nước, phân bón và thuốc trừ sâu, giảm thiểu ô nhiễm nguồn nước và đất. Hơn nữa, drone kết hợp với AI trong quản lý cây trồng có thể bay qua các cánh đồng để chụp ảnh đa phổ, phát hiện sớm dấu hiệu sâu bệnh, tình trạng thiếu nước hoặc dinh dưỡng ở từng phần của cánh đồng. AI phân tích hình ảnh để xác định chính xác khu vực cần can thiệp, giúp nông dân phun thuốc hoặc bón phân cục bộ, giảm lượng hóa chất sử dụng và tăng năng suất cây trồng. Công ty PrecisionHawk sử dụng drone để thu thập dữ liệu về sức khỏe cây trồng, giúp nông dân Mỹ tối ưu hóa việc sử dụng thuốc bảo vệ thực vật và tăng năng suất. Công nghệ số cũng góp phần giảm thiểu chất thải thực phẩm thông qua các ứng dụng và nền tảng số giúp kết nối người bán và người mua, tối ưu hóa chuỗi cung ứng và phân phối để giảm lượng thực phẩm thừa bị vứt bỏ, từ đó giảm áp lực lên bãi chôn lấp và tài nguyên. Ứng dụng Too Good To Go cho phép người dùng mua thực phẩm sắp hết hạn từ các nhà hàng và cửa hàng với giá rẻ, giúp giảm lượng thực phẩm lãng phí.

2.3. Giao thông thông minh và giảm phát thải

Trong lĩnh vực giao thông, công nghệ số đóng vai trò quan trọng trong việc giảm ùn tắc và khí thải. Hệ thống giao thông thông minh (ITS) sử dụng mạng lưới cảm biến, camera và thuật toán AI để điều khiển đèn giao thông, quản lý luồng xe và cung cấp thông tin giao thông theo thời gian thực. Bằng cách tối ưu hóa luồng di chuyển, ITS giúp giảm ùn tắc, rút ngắn thời gian di chuyển và trực tiếp làm giảm lượng khí thải carbon từ các phương tiện giao thông. Ví dụ, tại Singapore, hệ thống giao thông thông minh quản lý luồng xe hiệu quả, giúp giảm đáng kể thời gian di chuyển và ô nhiễm không khí đô thị. Sự phát triển của xe điện (EV) và xe tự lái cũng là minh chứng rõ nét cho vai trò của công nghệ số. Xe điện, được vận hành hoàn toàn bằng năng lượng điện, không phát thải tại chỗ, góp phần làm sạch không khí đô thị. Các thành phố lớn như Oslo (Na Uy) đã đạt được những bước tiến lớn trong việc điện hóa giao thông công cộng và cá nhân, nhờ các ứng dụng công nghệ số hỗ trợ sạc và quản lý đội xe điện. Xe tự lái, dựa trên các hệ thống AI và cảm biến phức tạp, có tiềm năng tối ưu hóa lộ trình, giảm thiểu các hành vi lái xe tiêu tốn nhiên liệu như phanh gấp và tăng tốc đột ngột, từ đó giảm tiêu thụ năng lượng. Ngoài ra, các ứng dụng chia sẻ phương tiện như Uber hay Grab sử dụng nền tảng số để tối ưu hóa việc sử dụng xe, giảm số lượng xe cá nhân lưu thông trên đường, góp phần giảm ùn tắc, tiêu thụ nhiên liệu và khí thải.

3. Nâng cao nhận thức và hành động vì môi trường

Công nghệ số không chỉ cung cấp công cụ kỹ thuật mà còn là phương tiện mạnh mẽ để giáo dục, nâng cao nhận thức và thúc đẩy hành động vì môi trường trong cộng đồng.

3.1. Giáo dục và thông tin

Công nghệ số đã mở rộng đáng kể khả năng tiếp cận thông tin và giáo dục về môi trường. Các nền tảng học trực tuyến (e-learning) và MOOCs (Massive Open Online Courses) cung cấp hàng ngàn khóa học về biến đổi khí hậu, phát triển bền vững, đa dạng sinh học và các chủ đề môi trường khác đến hàng triệu người trên toàn cầu, vượt qua rào cản địa lý và chi phí. Coursera và edX cung cấp các khóa học miễn phí hoặc có phí về môi trường từ các trường đại học hàng đầu thế giới, tiếp cận hàng triệu học viên. Phương tiện truyền thông số và mạng xã hội đóng vai trò quan trọng trong việc lan truyền thông điệp về môi trường một cách nhanh chóng và rộng rãi, tạo ra các chiến dịch nâng cao nhận thức, khuyến khích thảo luận và thúc đẩy hành động

tập thể. Chiến dịch #Trashtag trên Instagram đã lan truyền mạnh mẽ, khuyến khích hàng ngàn người tham gia dọn rác ở các khu vực công cộng. Các tổ chức môi trường và cá nhân có thể dễ dàng chia sẻ thông tin, hình ảnh và video để thu hút sự chú ý của công chúng. Hơn nữa, Thực tế ảo (VR) và Thực tế tăng cường (AR) đang được ứng dụng để tạo ra những trải nghiệm nhập vai, giúp người học hiểu rõ hơn về các hệ sinh thái, tác động của ô nhiễm và biến đổi khí hậu một cách trực quan và sống động. Ví dụ, tour VR "Our Planet" của Netflix cho phép người xem khám phá các hệ sinh thái đa dạng và chứng kiến tác động của biến đổi khí hậu một cách chân thực.

3.2. Kinh tế tuần hoàn và tái chế

Công nghệ số đang đóng vai trò quan trọng trong việc thúc đẩy mô hình kinh tế tuần hoàn, nơi tài nguyên được sử dụng tối đa và chất thải được giảm thiểu. Các nền tảng số kết nối người tái chế và người sử dụng vật liệu đã xuất hiện, tạo ra các thị trường trực tuyến cho vật liệu tái chế. Điều này giúp các doanh nghiệp dễ dàng tìm kiếm nguồn nguyên liệu đầu vào từ rác thải, thay vì phải khai thác tài nguyên mới, đồng thời giúp giảm lượng chất thải chôn lấp. Ví dụ, các ứng dụng như "Recycle Bank" (Mỹ) thưởng điểm cho người dùng tái chế, khuyến khích hành vi xanh. Ngoài ra, Blockchain cho chuỗi cung ứng minh bạch là một công nghệ đầy hứa hẹn. Bằng cách ghi lại mọi giao dịch và di chuyển của sản phẩm trên một sổ cái phân tán, Blockchain giúp theo dõi nguồn gốc sản phẩm và vật liệu, đảm bảo tính bền vững và đạo đức trong sản xuất. IBM Food Trust sử dụng Blockchain để theo dõi chuỗi cung ứng thực phẩm, giúp giảm lãng phí và đảm bảo nguồn gốc sản phẩm bền vững. Điều này khuyến khích các nhà sản xuất áp dụng các quy trình thân thiện với môi trường và giảm thiểu chất thải, đồng thời cho phép người tiêu dùng đưa ra lựa chọn mua hàng có trách nhiệm hơn.

3.3. Khoa học công dân và sự tham gia cộng đồng

Công nghệ số đã dân chủ hóa việc thu thập dữ liệu và thúc đẩy sự tham gia của cộng đồng vào công tác bảo vệ môi trường thông qua khoa học công dân. Các ứng dụng di động thu thập dữ liệu môi trường cho phép người dân tham gia vào việc giám sát môi trường bằng cách báo cáo các vấn đề như ô nhiễm, nạn phá rừng, hoặc thu thập dữ liệu về đa dạng sinh học thông qua điện thoại thông minh của họ. Dự án iNaturalist cho phép người dùng chụp ảnh và định danh các loài thực vật, động vật, đóng góp vào

cơ sở dữ liệu đa dạng sinh học toàn cầu. Dữ liệu này, khi được tổng hợp và phân tích, có thể cung cấp thông tin quý giá cho các nhà khoa học và cơ quan quản lý. Hơn nữa, các nền tảng gây quỹ cộng đồng (crowdfunding) cho các dự án môi trường đã giúp các tổ chức phi lợi nhuận và cá nhân dễ dàng huy động nguồn lực tài chính cho các sáng kiến bảo vệ môi trường, từ trồng rừng đến làm sạch bãi biển. Kickstarter và GoFundMe thường xuyên có các dự án gây quỹ thành công cho các sáng kiến môi trường, như phát triển công nghệ lọc rác thải nhựa đại dương. Những nền tảng này không chỉ cung cấp tài chính mà còn nâng cao nhận thức và thu hút sự ủng hộ rộng rãi từ công chúng.

PHẦN III: CÔNG NGHỆ SỐ TÁC ĐỘNG TIÊU CỰC ĐẾN MÔI TRƯỜNG

Bên cạnh những hứa hẹn về một tương lai xanh, công nghệ số cũng mang trong mình những góc khuất, những tác động tiêu cực đáng kể đến môi trường mà chúng ta không thể bỏ qua. phần này sẽ là một cái nhìn thẳng thắn và toàn diện vào "dấu chân môi trường" của ngành công nghệ. Chúng ta sẽ khám phá cách mà lượng năng lượng khổng lồ được tiêu thụ bởi các trung tâm dữ liệu và các hoạt động như khai thác tiền điện tử đang góp phần vào phát thải khí nhà kính. Đặc biệt, vấn đề rác thải điện tử – một "núi rác" độc hại ngày càng chồng chất – sẽ được phân tích sâu về khối lượng, thành phần độc hại và những hệ lụy nguy hiểm. Cuối cùng, chúng ta cũng sẽ tìm hiểu về áp lực từ việc khai thác tài nguyên thiên nhiên và dấu chân carbon của chuỗi cung ứng toàn cầu. Việc nhận diện rõ ràng những mặt trái này là cực kỳ quan trọng để chúng ta có thể đưa ra các giải pháp hiệu quả và bền vững.

1. Tiêu thụ năng lượng và phát thải carbon

Một trong những lo ngại lớn nhất về tác động môi trường của công nghệ số là lượng năng lượng khổng lồ mà nó tiêu thụ, dẫn đến phát thải khí nhà kính đáng kể.

1.1. Trung tâm dữ liệu (Data Centers)

Trung tâm dữ liệu là trái tim của thế giới số, nơi lưu trữ, xử lý và quản lý hàng tỷ tỷ byte dữ liệu mỗi ngày, từ các ứng dụng di động, trang web đến các dịch vụ đám mây và trí tuệ nhân tạo. Những cơ sở vật chất khổng lồ này, chứa hàng ngàn máy chủ và thiết bị mạng, tiêu thụ một lượng năng lượng khổng lồ không chỉ để vận hành các máy chủ liên tục 24/7 mà còn để duy trì hệ thống làm mát phức tạp, kiểm soát nhiệt độ và độ ẩm. Ước tính, trung tâm dữ liệu toàn cầu có thể chiếm tới 1-3% tổng lượng điện tiêu thụ của thế giới, và con số này dự kiến sẽ tiếp tục tăng lên nhanh chóng cùng với sự gia tăng nhu cầu về dữ liệu và các dịch vụ số. Ví dụ, một trung tâm dữ liệu lớn của Google có thể tiêu thụ lượng điện bằng cả một thành phố nhỏ. Vấn đề trở nên nghiêm trọng hơn khi phần lớn năng lượng tiêu thụ bởi trung tâm dữ liệu vẫn đến từ các nguồn năng lượng hóa thạch (than đá, dầu mỏ, khí đốt), dẫn đến việc phát thải lượng lớn khí nhà kính (CO2) vào khí quyển, làm trầm trọng thêm vấn đề biến đổi khí hậu. Mặc dù nhiều công ty công nghệ lớn đang nỗ lực chuyển đổi sang sử dụng năng lượng tái tạo và áp dụng các công nghệ làm mát hiệu quả hơn, nhưng quá trình chuyển đổi này vẫn

còn chậm và không đồng đều trên toàn cầu, khiến trung tâm dữ liệu trở thành một điểm nóng về phát thải carbon. Chẳng hạn, mặc dù Google và Facebook đã đầu tư lớn vào năng lượng tái tạo cho các trung tâm dữ liệu của họ, nhưng nhu cầu điện năng vẫn liên tục tăng.

1.2. Mạng lưới truyền tải dữ liệu và thiết bị người dùng

Ngoài các trung tâm dữ liệu, toàn bộ mạng lưới truyền tải dữ liệu cũng tiêu thụ một lượng năng lượng đáng kể. Internet toàn cầu, bao gồm hệ thống cáp quang dưới biển, các trạm phát sóng di động, router, switch và các thiết bị mạng khác, phải hoạt động liên tục để đảm bảo dữ liệu được truyền tải thông suốt giữa các thiết bị và trung tâm dữ liệu. Việc duy trì hoạt động 24/7 của mạng lưới này đòi hỏi một nguồn cung cấp điện ổn định và liên tục, góp phần vào tổng lượng năng lượng tiêu thụ của ngành công nghệ. Mỗi khi bạn xem một video trực tuyến chất lượng cao hoặc tham gia cuộc họp video, lượng dữ liệu truyền tải qua mạng sẽ tăng lên, đòi hỏi nhiều năng lượng hơn. Bên cạnh đó, hàng tỷ thiết bị điện tử cá nhân mà chúng ta sử dụng hàng ngày như smartphone, máy tính xách tay, TV thông minh và máy tính bảng, mặc dù mỗi thiết bị có mức tiêu thụ điện năng không lớn, nhưng với số lượng khổng lồ, tổng lượng tiêu thụ lại trở nên đáng kể. Quá trình sạc pin, duy trì kết nối mạng và hoạt động của các thiết bị này góp phần vào nhu cầu năng lượng chung và gián tiếp gây ra phát thải carbon từ các nhà máy điện. Một hộ gia đình hiện đại với nhiều thiết bị thông minh kết nối mạng có thể tiêu thụ điện năng lớn hơn nhiều so với trước đây, ngay cả khi các thiết bị đang ở chế độ chờ. Hơn nữa, việc sản xuất các thiết bị này cũng tiêu tốn năng lượng và tài nguyên, tạo nên một chuỗi tác động môi trường từ khâu khai thác đến sử dụng và thải bỏ.

1.3. Khai thác tiền điện tử

Một trong những vấn đề gây tranh cãi nhất về tác động môi trường của công nghệ số là hoạt động khai thác tiền điện tử, đặc biệt là Bitcoin. Quá trình khai thác Bitcoin, được gọi là "đào" Bitcoin, đòi hỏi các máy tính chuyên dụng phải thực hiện các phép tính mật mã cực kỳ phức tạp để xác minh giao dịch và thêm các khối mới vào chuỗi khối (Blockchain). Cơ chế này, được gọi là Proof of Work (PoW), được thiết kế để yêu cầu một lượng lớn năng lượng tính toán, nhằm đảm bảo tính bảo mật và phi tập trung của mạng lưới. Tuy nhiên, chính yêu cầu này đã dẫn đến việc tiêu thụ một lượng

năng lượng cực kỳ lớn, thường được so sánh với mức tiêu thụ điện của cả một quốc gia nhỏ như Argentina hoặc Thụy Điển trong một năm. Theo Đại học Cambridge, mức tiêu thụ điện của Bitcoin trong năm 2021 có lúc vượt qua cả quốc gia Hà Lan. Vấn đề nghiêm trọng hơn là phần lớn năng lượng được sử dụng cho khai thác tiền điện tử thường đến từ các nguồn hóa thạch, đặc biệt là than đá ở một số khu vực, dẫn đến lượng khí thải carbon đáng kể và làm trầm trọng thêm vấn đề biến đổi khí hậu. Nghiên cứu chỉ ra rằng lượng carbon footprint của Bitcoin có thể cao hơn của ngành khai thác vàng. Mặc dù đang có những nỗ lực chuyển đổi sang các cơ chế đồng thuận tiết kiệm năng lượng hơn (ví dụ: Proof of Stake) và sử dụng năng lượng tái tạo trong khai thác, nhưng tác động môi trường hiện tại của việc khai thác tiền điện tử vẫn là một mối lo ngại lớn.

2. Rác thải điện tử

Rác thải điện tử là một trong những hệ quả tiêu cực rõ ràng và đáng báo động nhất của sự phát triển nhanh chóng của công nghệ số, gây ra những vấn đề nghiêm trọng về môi trường và sức khỏe.

2.1. Khối lượng rác thải khổng lồ

Một đặc điểm cố hữu của ngành công nghệ số là tốc độ lỗi thời nhanh chóng của các thiết bị điện tử. Các nhà sản xuất liên tục tung ra các mẫu mã mới với công nghệ cải tiến, tính năng vượt trội, khuyến khích người tiêu dùng nâng cấp điện thoại, máy tính, TV hoặc các thiết bị thông minh khác chỉ sau vài năm sử dụng. Chu kỳ nâng cấp ngắn ngủi này tạo ra một lượng lớn rác thải điện tử hàng năm. Hàng chục triệu tấn thiết bị điện tử cũ bị vứt bỏ mỗi năm trên toàn cầu, và con số này không ngừng tăng lên. Theo Báo cáo Giám sát Rác thải Điện tử Toàn cầu (Global E-waste Monitor) của Liên Hợp Quốc, thế giới đã tạo ra 53,6 triệu tấn rác thải điện tử vào năm 2019, và con số này được dự báo sẽ đạt 74 triệu tấn vào năm 2030. Vấn đề trở nên trầm trọng hơn bởi thiếu quy trình tái chế hiệu quả và phổ biến. Tỷ lệ tái chế rác thải điện tử trên toàn cầu còn rất thấp, nghĩa là phần lớn trong số hàng triệu tấn thiết bị cũ này không được xử lý đúng cách, mà thường kết thúc ở các bãi chôn lấp hoặc được xuất khẩu sang các nước đang phát triển, nơi chúng được tháo dỡ thủ công trong điều kiện không an toàn. Chỉ khoảng 17,4% lượng e-waste toàn cầu được thu gom và tái chế đúng cách trong năm 2019.

2.2. Độc hại và ô nhiễm môi trường

Sự nguy hiểm của rác thải điện tử nằm ở thành phần hóa học của chúng. Các thiết bị điện tử chứa nhiều kim loại nặng và hóa chất độc hại như chì (trong bảng mạch, màn hình CRT), thủy ngân (trong màn hình LCD, pin), cadmium (trong pin, chip), crom, brominated flame retardants (chất chống cháy có brom), và nhiều chất khác. Khi không được xử lý đúng cách, đặc biệt là khi bị chôn lấp hoặc đốt thủ công, các chất độc hại này có thể rò rỉ vào đất, nước và không khí, gây ô nhiễm nghiêm trọng cho hệ sinh thái. Tại Agbogbloshie, Ghana, một trong những bãi phế liệu điện tử lớn nhất thế giới, người dân đốt dây điện để lấy đồng, giải phóng khói độc chứa dioxin và furan gây ung thư. Chì có thể gây tổn thương thần kinh, thủy ngân ảnh hưởng đến hệ thần kinh và thận, cadmium gây ung thư và các bệnh về xương. Môi trường bị ô nhiễm bởi e-waste sẽ ảnh hưởng trực tiếp đến chuỗi thức ăn và nguồn nước sinh hoạt. Hơn nữa, những người làm việc trong các bãi phế liệu điện tử, đặc biệt là ở các nước đang phát triển nơi quy trình tái chế thiếu an toàn, thường xuyên tiếp xúc trực tiếp với các chất độc hại này, dẫn đến các vấn khỏe con người nghiêm trọng như tổn thương thần kinh, ung thư, dị tật bẩm sinh, các bệnh về đường hô hấp và da liễu, biến e-waste trở thành một vấn đề nhân đạo và môi trường cấp bách.

3. Khai thác tài nguyên thiên nhiên

Để sản xuất ra hàng tỷ thiết bị điện tử mỗi năm, ngành công nghệ số đòi hỏi một lượng lớn tài nguyên thiên nhiên, đặc biệt là các kim loại và khoáng sản. Quá trình khai thác này thường đi kèm với những tác động tiêu cực đáng kể đến môi trường và xã hội.

3.1. Nhu cầu nguyên vật liệu thô

Việc sản xuất các thiết bị điện tử đòi hỏi một danh mục dài các kim loại quý hiếm và đất hiếm, bao gồm vàng, bạc, platin, paladi (trong các mạch điện tử), đồng, nhôm, sắt (cho dây dẫn và vỏ thiết bị), và các nguyên tố đất hiếm như neodymium, dysprosium (cho nam châm trong loa, động cơ, ổ cứng). Việc khai thác những tài nguyên này thường diễn ra ở những vùng nhạy cảm về môi trường và có thể gây ra phá hủy môi trường sống nghiêm trọng. Các hoạt động khai thác mỏ có thể dẫn đến nạn phá rừng trên diện rộng để mở đường cho mỏ và cơ sở hạ tầng, gây xói mòn đất, làm suy thoái chất lượng đất và mất khả năng hấp thụ carbon của rừng. Nước thải từ các

mỏ thường chứa hóa chất độc hại và kim loại nặng, làm ô nhiễm nguồn nước mặt và nước ngầm, ảnh hưởng đến hệ sinh thái thủy sinh và nguồn nước sinh hoạt của cộng đồng địa phương. Chẳng hạn, việc khai thác lithium cho pin điện thoại và xe điện đang gây ra lo ngại về thiếu nước và ô nhiễm ở các khu vực khô hạn như Chile và Bolivia. Hơn nữa, toàn bộ quá trình khai thác và tinh chế kim loại là một quy trình tiêu tốn nhiều năng lượng và nước, góp phần vào phát thải khí nhà kính và gây áp lực lên nguồn tài nguyên nước sạch.

3.2. Xung đột và các vấn đề xã hội

Mối liên hệ giữa công nghệ và khai thác tài nguyên còn phức tạp hơn khi xét đến khía cạnh xã hội. Một số khoáng sản quan trọng cho sản xuất thiết bị điện tử, điển hình là coltan (columbite-tantalite, được sử dụng trong tụ điện cho điện thoại di động và các thiết bị điện tử khác) và cassiterite (nguyên liệu cho thiếc), thường được khai thác ở các vùng có xung đột vũ trang, đặc biệt là ở miền đông Cộng hòa Dân chủ Congo. Những khoáng sản này được gọi là "kim loại xung đột" vì việc buôn bán chúng có thể tài trợ cho các nhóm vũ trang, kéo dài các cuộc xung đột, gây ra bạo lực và bất ổn khu vực. Báo cáo của Liên Hợp Quốc đã nhiều lần chỉ ra mối liên hệ giữa việc khai thác khoáng sản như coltan và các nhóm vũ trang tại Congo. Ngoài ra, việc khai thác những khoáng sản này thường liên quan đến lao động trẻ em và các điều kiện làm việc cực kỳ tồi tệ, không an toàn và không có các biện pháp bảo vệ sức khỏe, gây ra những hậu quả nghiêm trọng về nhân quyền. Tổ chức Ân xá Quốc tế đã ghi nhận các trường hợp trẻ em làm việc trong các mỏ cobalt ở Congo, đối mặt với nguy hiểm và điều kiện sống khắc nghiệt. Mặc dù các công ty công nghệ đang nỗ lực để đảm bảo nguồn cung cấp khoáng sản không liên quan đến xung đột, nhưng việc truy xuất nguồn gốc và đảm bảo chuỗi cung ứng minh bạch vẫn là một thách thức lớn trong ngành.

4. Dấu chân carbon của chuỗi cung ứng và sản xuất

Quá trình sản xuất và vận chuyển các sản phẩm công nghệ số cũng để lại một dấu chân carbon đáng kể, thường bị bỏ qua khi chỉ tập trung vào giai đoạn sử dụng.

4.1. Sản xuất và lắp ráp

Việc sản xuất các linh kiện điện tử tinh vi như chip bán dẫn, màn hình, bo mạch chủ và sau đó là lắp ráp chúng thành sản phẩm hoàn chỉnh là một quy trình cực kỳ phức tạp và tiêu tốn tài nguyên. Các nhà máy sản xuất trong ngành công nghệ thường

tiêu thụ một lượng lớn năng lượng và nước để vận hành máy móc, duy trì môi trường sản xuất sạch sẽ (phòng sạch) và thực hiện các quy trình hóa học. Quá trình này không chỉ góp phần vào nhu cầu điện năng toàn cầu mà còn thường xuyên phát thải khí nhà kính và các chất ô nhiễm khác vào môi trường, nếu không có các biện pháp kiểm soát chặt chẽ. Các nhà máy sản xuất chip bán dẫn (ví dụ: TSMC hay Samsung Foundry) là những cơ sở tiêu thụ nước và điện khổng lồ, tạo ra lượng khí thải lớn. Hơn nữa, việc sử dụng hóa chất độc hại trong quá trình sản xuất (ví dụ: các dung môi, axit, kim loại nặng trong quá trình khắc, làm sạch, và mạ) là một mối lo ngại lớn. Nếu các chất này không được quản lý, xử lý và thải bỏ đúng cách, chúng có thể gây ô nhiễm nghiêm trọng cho đất, nước và không khí xung quanh các khu công nghiệp, ảnh hưởng đến sức khỏe của người lao động và cộng đồng địa phương.

4.2. Vận chuyển và hậu cần

Trong một chuỗi cung ứng toàn cầu phức tạp, các linh kiện và sản phẩm công nghệ thường được sản xuất ở nhiều quốc gia khác nhau và sau đó được vận chuyển khắp thế giới để lắp ráp và phân phối đến tay người tiêu dùng. Quá trình vận chuyển toàn cầu này, sử dụng các phương tiện như tàu biển, xe tải và máy bay, tiêu thụ một lượng lớn nhiên liệu hóa thạch và phát thải CO2 cùng các chất gây ô nhiễm khác vào khí quyển. Một chiếc iPhone được sản xuất tại Trung Quốc có thể chứa linh kiện từ hàng chục quốc gia khác nhau và được vận chuyển bằng đường hàng không đến các thị trường chính, tạo ra một dấu chân carbon đáng kể trước khi đến tay người dùng. Ví dụ, một chiếc điện thoại thông minh có thể có chip sản xuất ở Đài Loan, màn hình ở Hàn Quốc, lắp ráp ở Trung Quốc, và sau đó được vận chuyển đến châu Âu hoặc Mỹ để bán. Mỗi bước trong chuỗi cung ứng này đều có dấu chân carbon riêng. Với khối lượng sản phẩm khổng lồ được sản xuất và luân chuyển hàng ngày, tác động từ vận chuyển và hậu cần đóng góp đáng kể vào tổng lượng khí thải của ngành công nghệ. Việc tối ưu hóa chuỗi cung ứng, giảm quãng đường vận chuyển và chuyển đổi sang các phương thức vận tải xanh hơn là những thách thức lớn đối với các công ty công nghệ.

5. Mối lo ngại về hiệu ứng "Rebound Effect"

Mặc dù công nghệ số thường được ca ngợi vì khả năng tăng cường hiệu quả sử dụng tài nguyên, nhưng có một mối lo ngại tiềm ẩn được gọi là hiệu ứng "Rebound

Effect", hay còn gọi là "hiệu ứng Jevons". Hiệu ứng này mô tả hiện tượng khi việc cải thiện hiệu quả sử dụng một tài nguyên lại dẫn đến việc tăng tổng mức tiêu thụ tài nguyên đó. Ví dụ, công nghệ số có thể giúp tối ưu hóa việc quản lý năng lượng trong một tòa nhà, giảm lượng điện tiêu thụ cho mỗi đơn vị diện tích. Tuy nhiên, nếu sự tiết kiệm này làm giảm chi phí vận hành, nó có thể khuyến khích việc xây dựng thêm nhiều tòa nhà hoặc sử dụng năng lượng cho các tiện ích khác, cuối cùng dẫn đến việc tăng tổng lượng tiêu thụ năng lượng của hệ thống.

Một ví dụ khác là việc sử dụng các ứng dụng hội nghị trực tuyến có thể làm giảm nhu cầu di chuyển bằng máy bay cho các cuộc họp kinh doanh, từ đó tiết kiệm nhiên liệu và giảm khí thải. Tuy nhiên, chính sự tiện lợi và chi phí thấp của việc giao tiếp trực tuyến lại khuyến khích việc tổ chức nhiều cuộc họp hơn, tăng cường sử dụng internet và các dịch vụ đám mây (email, lưu trữ tài liệu trực tuyến), điều này lại dẫn đến tăng nhu cầu về trung tâm dữ liệu và mạng lưới truyền tải, qua đó tăng lượng năng lượng tiêu thụ tổng thể của ngành công nghệ. Các nghiên cứu đã chỉ ra rằng mặc dù hội nghị trực tuyến giảm phát thải từ di chuyển, nhưng việc tăng cường sử dụng dịch vụ video trực tuyến đã làm tăng đáng kể mức tiêu thụ năng lượng của các trung tâm dữ liệu và hạ tầng mạng. Hiệu ứng Rebound cho thấy rằng việc cải thiện hiệu quả công nghệ tự nó không đảm bảo sẽ dẫn đến việc giảm tổng mức tiêu thụ tài nguyên. Để đạt được sự bền vững thực sự, cần phải có sự kết hợp giữa các giải pháp công nghệ hiệu quả với các chính sách quản lý, nâng cao nhận thức và thay đổi hành vi tiêu dùng để tránh tình trạng "tăng trưởng xanh" chỉ là một ảo ảnh.

PHẦN IV: GIẢI PHÁP

Sau khi đã nhận diện những thách thức môi trường do công nghệ số gây ra, câu hỏi quan trọng tiếp theo là: Chúng ta có thể làm gì để giảm thiểu những tác động tiêu cực này và hướng tới một tương lai bền vững hơn? phần này sẽ tập trung vào các giải pháp thiết thực có thể được áp dụng ở nhiều cấp độ khác nhau. Chúng ta sẽ bắt đầu từ những hành động cá nhân nhỏ nhưng ý nghĩa mà mỗi người dùng công nghệ có thể thực hiện hàng ngày, sau đó mở rộng ra các chính sách và sáng kiến mang tầm quốc gia. Từ việc kéo dài vòng đời thiết bị đến việc xây dựng các nền kinh tế tuần hoàn, mỗi giải pháp đều đóng góp vào việc tạo ra một hệ sinh thái số thân thiện hơn với hành tinh. Đây là lúc chúng ta biến nhận thức thành hành động để công nghệ thực sự phục vụ cho sự phát triển bền vững.

1. Giải pháp với mỗi cá nhân (người dùng công nghệ)

Mỗi người dùng công nghệ đều có thể đóng góp vào việc giảm thiểu tác động tiêu cực của công nghệ số thông qua những lựa chọn và thói quen hàng ngày. Những thay đổi nhỏ trong hành vi cá nhân, khi được nhân rộng, sẽ tạo ra hiệu ứng tích cực đáng kể.

Đầu tiên và quan trọng nhất là kéo dài vòng đời sử dụng của thiết bị điện tử. Thay vì chạy theo xu hướng và nâng cấp thiết bị mới mỗi khi có phiên bản ra mắt, người dùng nên tìm cách sử dụng điện thoại thông minh, máy tính, máy tính bảng và các thiết bị điện tử khác càng lâu càng tốt. Điều này không chỉ giúp tiết kiệm chi phí mà còn trực tiếp giảm nhu cầu sản xuất thiết bị mới, từ đó giảm khai thác tài nguyên và lượng rác thải điện tử phát sinh. Ví dụ, thay vì mua điện thoại mới mỗi năm, hãy cân nhắc giữ chiếc điện thoại hiện tại của bạn thêm 2-3 năm nữa, hoặc thay pin, sửa chữa màn hình nếu cần. Khi thiết bị cũ không còn đáp ứng nhu cầu, hãy xem xét các lựa chọn sửa chữa, tái sử dụng (bán lại hoặc tặng cho người khác) thay vì vứt bỏ. Các cửa hàng sửa chữa điện thoại độc lập đang ngày càng phổ biến, và các nền tảng trao đổi đồ cũ như Chợ Tốt (Việt Nam) hay Craigslist (quốc tế) giúp tái sử dụng thiết bị.

Thứ hai, việc tái chế rác thải điện tử đúng cách là cực kỳ cần thiết. Khi một thiết bị điện tử thực sự không thể sử dụng hay sửa chữa được nữa, việc vứt bỏ chúng vào thùng rác thông thường là một hành động gây hại nghiêm trọng cho môi trường do các hóa chất độc hại và kim loại nặng chứa trong đó. Thay vào đó, mỗi cá nhân cần

tìm hiểu và đưa rác thải điện tử đến các điểm thu gom, trung tâm tái chế chuyên dụng hoặc tham gia các chương trình thu hồi của nhà sản xuất. Tại Việt Nam, một số nhà mạng hoặc siêu thị điện máy lớn có chương trình thu hồi điện thoại, pin cũ để tái chế. Ở các nước phát triển, có nhiều điểm thu gom e-waste được chính quyền địa phương thiết lập. Điều này giúp đảm bảo rằng các vật liệu quý giá và độc hại được xử lý an toàn, tái chế hiệu quả.

Thứ ba, người dùng nên ưu tiên sử dụng năng lượng hiệu quả cho các thiết bị công nghệ. Điều này bao gồm việc rút phích cắm sạc khi thiết bị đã đầy pin hoặc không sử dụng, tắt các thiết bị khi không cần thiết (máy tính, màn hình, bộ định tuyến Wi-Fi vào ban đêm), và kích hoạt các chế độ tiết kiệm năng lượng trên thiết bị. Ví dụ, bật chế độ tiết kiệm pin trên điện thoại, tắt Wi-Fi router khi đi ngủ, hoặc sử dụng tính năng "Sleep" thay vì để máy tính hoạt động liên tục. Việc lựa chọn các thiết bị có chứng nhận tiết kiệm năng lượng (như Energy Star) cũng là một quyết định thông minh. Ngoài ra, hãy xem xét việc sử dụng dịch vụ đám mây một cách có trách nhiệm. Mặc dù đám mây mang lại nhiều tiện ích, nhưng việc lưu trữ dữ liệu không cần thiết, phát trực tuyến video chất lượng siêu cao liên tục, hoặc chạy các ứng dụng ngốn tài nguyên trên đám mây đều góp phần vào mức tiêu thụ năng lượng của trung tâm dữ liệu. Bạn có thể dọn dẹp các tệp cũ không dùng đến trên Google Drive hoặc Dropbox, và chọn cài đặt chất lượng video phù hợp thay vì luôn xem ở độ phân giải 4K trên Netflix nếu không cần thiết. Người dùng nên dọn dẹp các tệp không cần thiết, tối ưu hóa cài đặt chất lượng video và cân nhắc mức độ sử dụng các dịch vụ trực tuyến.

Cuối cùng, việc nâng cao nhận thức và chia sẻ thông tin về tác động môi trường của công nghệ số là một hành động thiết thực. Mỗi cá nhân có thể tự tìm hiểu sâu hơn về vấn đề này, sau đó chia sẻ kiến thức và kinh nghiệm của mình với gia đình, bạn bè và cộng đồng thông qua mạng xã hội hoặc các cuộc trò chuyện hàng ngày. Tham gia các nhóm môi trường trên Facebook, chia sẻ bài viết về e-waste hoặc pin năng lượng tái tạo là những cách để lan tỏa thông điệp. Việc tạo ra một cộng đồng người dùng có ý thức môi trường sẽ thúc đẩy sự thay đổi tích cực từ dưới lên, khuyến khích các nhà sản xuất và chính phủ hành động có trách nhiệm hơn.

2. Giải pháp cấp quốc gia

Ở cấp độ quốc gia, các chính phủ đóng vai trò then chốt trong việc định hình một khuôn khổ pháp lý và chính sách để giảm thiểu tác động tiêu cực của công nghệ số đến môi trường. Những giải pháp này đòi hỏi sự phối hợp đa ngành và tầm nhìn dài hạn.

Một trong những ưu tiên hàng đầu là xây dựng và thực thi các chính sách quản lý rác thải điện tử hiệu quả. Điều này bao gồm việc ban hành các luật về Trách nhiệm mở rộng của nhà sản xuất (Extended Producer Responsibility - EPR), yêu cầu các nhà sản xuất phải chịu trách nhiệm về toàn bộ vòng đời của sản phẩm, từ thiết kế thân thiện với môi trường đến việc thu gom và tái chế khi sản phẩm hết hạn sử dụng. Liên minh Châu Âu đã áp dụng chỉ thị WEEE (Waste Electrical and Electronic Equipment) yêu cầu các nhà sản xuất tài trợ cho việc thu gom và tái chế thiết bị điện tử cũ. Cần thiết lập các điểm thu gom rác thải điện tử dễ tiếp cận trên toàn quốc, đồng thời đầu tư vào công nghệ và cơ sở hạ tầng tái chế hiện đại, an toàn để chiết xuất các vật liệu quý giá và xử lý các chất độc hại một cách hiệu quả. Việc cấm xuất khẩu rác thải điện tử sang các nước đang phát triển cũng là một biện pháp quan trọng để ngăn chặn ô nhiễm và các vấn đề sức khỏe.

Thứ hai, quốc gia cần có chính sách khuyến khích sử dụng năng lượng tái tạo và tăng cường hiệu quả năng lượng trong ngành công nghệ. Chính phủ có thể đưa ra các ưu đãi thuế, trợ cấp hoặc các khoản vay ưu đãi cho các công ty công nghệ đầu tư vào các trung tâm dữ liệu xanh, sử dụng năng lượng mặt trời, gió hoặc các nguồn năng lượng sạch khác. Ireland đã thu hút nhiều trung tâm dữ liệu lớn của Google và Microsoft bằng cách khuyến khích họ sử dụng năng lượng gió và các nguồn tái tạo khác. Đồng thời, cần thiết lập các tiêu chuẩn hiệu quả năng lượng bắt buộc cho các thiết bị điện tử và trung tâm dữ liệu, khuyến khích đổi mới công nghệ để giảm mức tiêu thụ điện. chương trình Energy Star của Mỹ đặt ra các tiêu chuẩn hiệu quả năng lượng cho nhiều loại thiết bị điện tử, giúp người tiêu dùng dễ dàng lựa chọn sản phẩm tiết kiệm điện. Các chương trình nghiên cứu và phát triển (R&D) về công nghệ xanh, như hệ thống làm mát hiệu quả hơn cho trung tâm dữ liệu hay công nghệ pin bền vững, cũng cần được ưu tiên và tài trợ.

Thứ ba, việc thúc đẩy kinh tế tuần hoàn trong lĩnh vực công nghệ là một giải pháp chiến lược. Chính phủ có thể hỗ trợ các sáng kiến thiết kế sản phẩm điện tử theo

hướng dễ dàng sửa chữa, nâng cấp và tháo rời để tái chế. Điều này bao gồm việc yêu cầu các nhà sản xuất cung cấp linh kiện thay thế, tài liệu sửa chữa và công cụ cần thiết cho người tiêu dùng và các cửa hàng sửa chữa độc lập. Pháp đã ban hành "chỉ số khả năng sửa chữa" cho các sản phẩm điện tử, khuyến khích người tiêu dùng lựa chọn các sản phẩm dễ sửa chữa hơn. Ngoài ra, việc tạo ra các thị trường cho vật liệu tái chế và khuyến khích các doanh nghiệp sử dụng nguyên liệu thứ cấp trong sản xuất sẽ giảm áp lực khai thác tài nguyên mới. Chính phủ cũng có thể hỗ trợ các nền tảng số hóa giúp kết nối các chuỗi cung ứng tái chế, tối ưu hóa việc thu gom và phân phối vật liệu.

Thứ tư, kiểm soát chuỗi cung ứng và khai thác tài nguyên một cách có trách nhiệm là điều cần thiết. Quốc gia cần thiết lập các quy định nghiêm ngặt về truy xuất nguồn gốc khoáng sản, đảm bảo rằng các nguyên vật liệu được sử dụng trong sản xuất thiết bị công nghệ không liên quan đến xung đột vũ trang, lao động trẻ em hoặc các hoạt động khai thác gây hại môi trường. Luật Dodd-Frank Act (Mỹ) có điều khoản yêu cầu các công ty công khai thông tin về nguồn gốc khoáng sản xung đột, mặc dù việc thực thi vẫn còn nhiều thách thức. Việc tham gia và thúc đẩy các hiệp định quốc tế về khai thác khoáng sản có trách nhiệm cũng là một phần quan trọng của giải pháp này.

Cuối cùng, việc đầu tư vào giáo dục và nâng cao nhận thức cộng đồng là nền tảng cho mọi giải pháp. Chính phủ cần tích hợp kiến thức về tác động môi trường của công nghệ số vào chương trình giáo dục, từ cấp phổ thông đến đại học. Các chương trình giáo dục quốc gia có thể bao gồm các bài học về "công dân số xanh" (green digital citizen) từ sớm. Các chiến dịch truyền thông quốc gia có thể được triển khai để nâng cao nhận thức của người dân về tầm quan trọng của việc sử dụng công nghệ có trách nhiệm, cách tái chế đúng cách và lợi ích của việc kéo dài vòng đời thiết bị. Điều này sẽ tạo ra một nền tảng xã hội vững chắc, nơi người dân hiểu rõ vai trò của mình trong việc bảo vệ môi trường trong kỷ nguyên số.