**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**



**CHAPTER 5: E-COMMERCE SECURITY & PAYMENT SYSTEMS**

**Môn học:** Thương mại điện tử

**Mã môn học:** ECOM430984\_23\_1\_02

**Giảng viên hướng dẫn:** Ths.Nguyễn Văn Thành

**Nhóm sinh viên thực hiện:**

*Nhóm 11:*

Nguyễn Thùy Diễm My             21110549

Nguyễn Lê Gia Hân                   21110432

Trần Nguyễn Phương Tây          21110641

Nguyễn Võ Minh Luân              21110899

# PHÂN CÔNG CÔNG VIỆC VÀ ĐÁNH GIÁ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **Họ và tên** | **Công việc** | **Đánh giá** |
| Nguyễn Thùy Diễm My  21110549 | III. TECHNOLOGY SOLUTIONS | 100% |
| Nguyễn Lê Gia Hân  21110432 | II. SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT | 100% |
| Trần Nguyễn Phương Tây  21110641 | 1. THE E-COMMERCE SECURITY ENVIRONMENT VII. CASE STUDY | 100% |
| Nguyễn Võ Minh Luân  21110899 | IV. MANAGEMENT POLICIES, BUSINESS PROCEDURES, AND PUBLIC LAWS V. E-COMMERCE PAYMENT SYSTEMS  VI. ELECTRONIC BILLING PRESENTMENT AND PAYMENT TRÌNH BÀY VÀ THANH TOÁN ĐIỆN TỬ | 100% |

1. **The E-Commerce security environment** (trang 293 - 299 )
2. **THE SCOPE OF THE PROBLEM**

* Internet là một mạng được thiết kế mở, dễ bị tổn thương
* Khả năng ẩn danh trên Internet che giấu nhiều tội phạm bằng danh tính trông có vẻ hợp pháp.
* Tội phạm mạng đang trở thành một vấn đề nghiêm trọng đối với cả tổ chức và người tiêu dùng.

*Theo Symantec, cứ 10 URL thì có 1 URL độc hại, với sự gia tăng đáng kể về hình thức tấn công (sử dụng mã độc để đánh cắp thông tin thẻ tín dụng từ các trang web thanh toán). Các cuộc tấn công web nói chung tiếp tục gia tăng.  
 Cuộc khảo sát do Ponemon Institute thực hiện với 355 công ty thuộc nhiều ngành khác nhau ở 11 quốc gia năm 2019 cho thấy chi phí trung bình hàng năm do tội phạm mạng gây ra đối với tất cả các tổ chức trong nghiên cứu là 13 triệu USD, tăng 12% so với năm trước và tăng 72% trong 5 năm trước đó.  
 Thậm chí các tội phạm còn lập ra Thị trường kinh tế ngầm - còn được gọi là Darkweb hoặc Darknet để bán những thông tin bị đánh cắp.*

* Vì vậy, chúng ta có thể kết luận gì về quy mô tổng thể của tội phạm mạng?
* Tội phạm mạng chống lại các trang thương mại điện tử rất năng động và thay đổi liên tục, với những rủi ro mới xuất hiện gần như hàng ngày.
* Rất khó để ước tính chính xác số lượng tội phạm mạng thực tế.
* Số tiền thiệt hại đối với doanh nghiệp là rất lớn và ngày càng tăng.
* Người quản lý các trang web thương mại điện tử phải chuẩn bị cho các cuộc tấn công tội phạm luôn thay đổi và luôn cập nhật các kỹ thuật bảo mật mới nhất.

1. **WHAT IS GOOD E-COMMERCE SECURITY?**

* Người bán và người tiêu dùng thương mại điện tử cũng phải đối mặt với nhiều rủi ro giống như những người tham gia thương mại truyền thống.  
  → Giảm thiểu rủi ro trong thương mại điện tử là một quá trình phức tạp.
* Bảo mật thương mại điện tử có bản chất gồm nhiều lớp:

Các công nghệ có sẵn nên được sử dụng. Tuy nhiên, những công nghệ này một mình không giải quyết vấn đề. Cần có chính sách và quy trình tổ chức để đảm bảo rằng những công nghệ này không bị phá vỡ. Cuối cùng, cần có các tiêu chuẩn ngành công nghiệp và luật pháp của chính phủ để áp dụng cơ chế thanh toán, cũng như để điều tra và truy cứu người vi phạm luật pháp thiết kế để bảo vệ việc chuyển giao tài sản trong giao dịch thương mại.

➡ Bảo mật thương mại điện tử tốt đòi hỏi một bộ luật, thủ tục, chính sách và công nghệ, trong phạm vi khả thi, bảo vệ các cá nhân và tổ chức khỏi những hành vi không mong muốn trên thị trường thương mại điện tử.

1. **DIMENSIONS OF E-COMMERCE SECURITY**

* *Tính toàn vẹn (Integrity)* đề cập đến khả năng đảm bảo rằng thông tin được hiển thị trên một trang web hoặc được truyền hoặc nhận qua Internet không bị thay đổi dưới bất kỳ hình thức nào bởi một bên trái phép
* *Tính chống chối bỏ (Nonrepudiation)* đề cập đến khả năng đảm bảo rằng những người tham gia thương mại điện tử không từ chối (bác bỏ) các hành động trực tuyến của họ
* *Tính xác thực (Authenticity)* đề cập đến khả năng xác định danh tính của một người hoặc tổ chức mà bạn đang giao dịch trên Internet.
* *Tính bảo mật (Confidentiality)* đề cập đến khả năng đảm bảo rằng tin nhắn và dữ liệu chỉ được cung cấp cho những người được phép xem chúng.
* *Quyền riêng tư (Privacy)* đề cập đến khả năng kiểm soát việc sử dụng thông tin về bản thân.
* *Tính khả dụng (Availability)* đề cập đến khả năng đảm bảo rằng một trang web thương mại điện tử tiếp tục hoạt động như dự định.

➡ Bảo mật thương mại điện tử được thiết kế để bảo vệ sáu khía cạnh này. Khi bất kỳ một trong số chúng bị xâm phạm, an ninh tổng thể sẽ bị ảnh hưởng.

1. **THE TENSION BETWEEN SECURITY AND OTHER VALUES**

Mặc dù bảo mật máy tính được coi là cần thiết để bảo vệ hoạt động thương mại điện tử nhưng không phải là không có nhược điểm. Hai lĩnh vực chính có mâu thuẫn giữa bảo mật và hoạt động của trang web là:

4.1 Security versus Ease of Use ((Bảo mật so với Dễ sử dụng)

* Càng nhiều biện pháp bảo mật được thêm vào một trang web thương mại điện tử thì trang web đó càng khó sử dụng và trang web càng trở nên chậm hơn, cản trở sự truy cập và sử dụng dễ dàng.
* Với người dùng yêu thích sự tiện lợi  
  *Khi người tiêu dùng thấy việc xác thực trên các trang web trở nên dễ dàng, họ sẽ mua nhiều hơn từ 10% đến 20% (theo báo cáo McKinsey, 2016)*
* Với người dùng quan tâm sự bảo mật  
  *Gần 3/4 người tiêu dùng nói rằng họ muốn bảo mật bổ sung, ngay cả khi họ yêu cầu các bước bổ sung để có thể truy cập tài khoản (theo báo cáo của IBM Security, 2018)*

⇒ Một giải pháp là điều chỉnh cài đặt bảo mật theo sở thích của người

dùng.

* Bảo mật được đánh đổi với cái giá là làm chậm bộ xử lý và tăng thêm đáng kể nhu cầu lưu trữ dữ liệu.
* Quá nhiều bảo mật có thể gây tổn hại đến lợi nhuận, trong khi không đủ có thể khiến công ty phá sản.

4.2 Public Safety and the Criminal Uses of the Internet (An toàn công cộng và việc sử dụng internet cho mục đích tội phạm.)

* Ngoài ra còn có mâu thuẫn không thể tránh khỏi giữa mong muốn của các cá nhân hành động ẩn danh (để che giấu danh tính) và nhu cầu của các quan chức trong việc duy trì an toàn công cộng có thể bị bọn tội phạm hoặc khủng bố đe dọa.
* Việc giám sát các thông tin truyền tải Internet có thể gây ra những tranh cãi lớn.
* Sự cân bằng hợp lý giữa an toàn công cộng và quyền riêng tư trong nỗ lực chống khủng bố đã được chứng minh là một vấn đề rất hóc búa đối với chính phủ Hoa Kỳ.

1. **SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT** (trang 300 - trang 323)

Về góc độ công nghệ, có ba lỗ hổng chính dễ bị tấn công khi làm việc với thương mại điện tử: máy khách, máy chủ và đường truyền giao tiếp. Hình 5.2 minh họa một giao dịch thương mại điện tử điển hình với một người tiêu dùng sử dụng thẻ tín dụng để mua sản phẩm. Hình 5.3 minh họa một số vấn đề có thể xảy ra tại mỗi điểm yếu chính trong giao dịch - qua các kênh truyền internet, tại mức máy chủ và mức máy khách.

Trong phần này, chúng tôi mô tả một số dạng phổ biến và có hại nhất của mối đe dọa về bảo mật đối với người tiêu dùng và người điều hành trang web thương mại điện tử: mã độc hại, các chương trình có thể không mong muốn, lừa đảo (phishing), xâm nhập và tấn công cybervandalism, việc xâm nhập vào dữ liệu, trộm cắp thẻ tín dụng, làm giả thông tin (spoofing), tấn công pharming (pharming), website spam và giả danh (identity fraud), tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS), nghe trộm thông tin (sniffing), tấn công từ bên trong, phần mềm máy chủ và máy khách thiết kế kém cỏi, vấn đề bảo mật trên mạng xã hội, vấn đề bảo mật trên nền tảng di động và cuối cùng, vấn đề bảo mật đám mây.

1. **MALICIOUS CODE**

Mã độc hại (đôi khi được gọi là “phần mềm độc hại (malware)”) bao gồm nhiều mối đe dọa khác nhau như như virus, worms (Worm máy tính là một loại chương trình độc hại chủ yếu tự lây lan sang các máy tính khác trong khi vẫn hoạt động trên các hệ thống bị nhiễm), phần mềm tống tiền, Trojan horses (chương trình độc hại ngụy trang như một cái gì đó được cho là lành tính) và bot. Một số mã độc, đôi khi được gọi là mã khai thác *exploit*, được thiết kế để lợi dụng các lỗ hổng phần mềm trong hệ điều hành, trình duyệt web, ứng dụng hoặc phần mềm khác của máy tính các thành phần. Trước đây, mã độc thường nhằm mục đích đơn giản là làm hỏng máy tính và thường được tạo ra bởi một hacker đơn độc, nhưng ngày càng nó liên quan đến một nhóm tin tặc hoặc một nhóm được quốc gia hỗ trợ và mục đích là đánh cắp địa chỉ e-mail, thông tin đăng nhập, dữ liệu cá nhân và thông tin tài chính. Đó là sự khác biệt giữa tội phạm nhỏ và tội phạm có tổ chức.

* **Exploit kit**: Bộ công cụ khai thác là tập hợp các khai thác được đóng gói cùng nhau và cho thuê hoặc bán như một sản phẩm thương mại, thường có giao diện người dùng bóng bẩy và chức năng phân tích chuyên sâu. Việc sử dụng bộ công cụ khai thác thường không yêu cầu nhiều kỹ năng kỹ thuật, khiến người mới có thể trở thành tội phạm mạng. Exploit kit thường hướng đến các phần mềm được triển khai rộng rãi, chẳng hạn như Microsoft Windows, Internet Explorer, Adobe Flash và Reader và Oracle Java. Theo Malwarebytes Labs, bộ công cụ khai thác tiếp tục gây ra mối đe dọa, với một số bộ dụng cụ mới được xác định vào năm 2019 phục vụ tải trọng bao gồm ransomware và phần mềm độc hại khác (Malwarebytes Labs, 2020).

Phần mềm độc hại thường được phân phát dưới dạng tệp đính kèm độc hại trong email hoặc được nhúng dưới dạng liên kết trong email. Các liên kết độc hại cũng có thể được đặt trong tài liệu Microsoft Word hoặc Excel trông vô hại. Các liên kết này dẫn trực tiếp đến việc tải về mã độc hại hoặc trang web chứa mã độc hại.

* **malvertising**: Một phương pháp khác để phân phát mã độc hại là nhúng nó vào chuỗi quảng cáo trực tuyến (được gọi là malvertising), bao gồm cả qua Google và các mạng quảng cáo khác. Khi chuỗi mạng quảng cáo trở nên phức tạp hơn,nó sẽ trở nên khó khăn hơn cho các trang web kiểm tra quảng cáo được đặt trên trang web của họ để đảm bảo chúng không chứa mã độc hại.

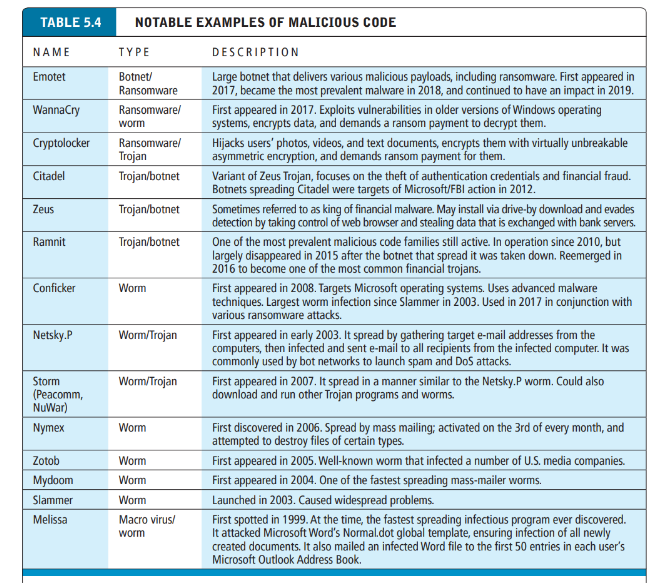
Một trong những cuộc tấn công malvertising lớn nhất xảy ra tại Yahoo, nơi hơn 6,9 triệu người truy cập hàng ngày bị tiếp xúc với các quảng cáo pop-up độc hại. Một cuộc tấn công nổi bật khác liên quan đến quảng cáo được phân phát thông qua nhiều mạng quảng cáo đến trang web của New York Times, BBC, NFL và AOL, đã tấn công vào máy tính khi người dùng nhấp chuột, mã hóa dữ liệu người dùng và đòi tiền chuộc. Vào năm 2020, AdSecure cho biết hơn 27% trong số hơn 1 triệu chiến dịch quảng cáo của họ vào năm 2019 phát hiện có một dạng malvertising nào đó, trong khi Clean.io phát hiện một sự tăng cường trong các chiến dịch malvertising bắt đầu vào giữa tháng 3 năm 2020, trong đợt đại dịch Covid-19 (Knight, 2020; O’Reilly, 2020; Taylor, 2020; Malwarebytes, 2020;). Những quảng cáo độc hại này có thể được ngăn chặn bằng cách sử dụng các chương trình chặn quảng cáo. Google cũng đã đang thực hiện các biện pháp để chặn malvertising và vào năm 2018, họ đã chặn 2,3 tỷ "quảng cáo xấu" mà họ cho rằng vi phạm các chính sách của họ, bao gồm gần 50 triệu quảng cáo lừa đảo (Binder, 2019). Trong những năm trước, nhiều trường hợp malvertising thường bắt nguồn từ tải xuống tự động (drive-by downloads) sử dụng các lỗ hổng zero-day thường xuyên mà Adobe Flash thường gặp phải, mà thường được sử dụng cho quảng cáo trực tuyến. Do đó, Hiệp hội Quảng cáo trực tuyến khuyên người quảng cáo từ bỏ Adobe Flash để sử dụng HTML5, và các trình duyệt Mozilla Firefox, Apple's Safari và Google Chrome hiện nay đã chặn quảng cáo Flash tự động phát lại. Amazon cũng đã ngừng chấp nhận quảng cáo Flash. Adobe đã thông báo rằng họ sẽ ngừng cập nhật và phân phối Flash Player vào cuối năm 2020.

* **drive-by download**: Drive-by download (tải xuống tự động) là phần mềm độc hại đi kèm với một tệp đã được người dùng yêu cầu một cách cố ý hoặc vô tình. Hiện nay, drive-by đã trở thành một trong những phương pháp phổ biến nhất để nhiễm trùng máy tính. Theo Symantec, các bộ công cụ khai thác drive-by download, kèm theo cập nhật và hỗ trợ 24/7, có thể được thuê với giá từ 100 đến 700 đô la mỗi tuần. Mã độc hại nhúng trong các tệp PDF cũng rất phổ biến. Quan trọng không kém, đã có một sự chuyển đổi lớn trong người viết mã độc hại từ các hacker và những người phiêu lưu viên không chuyên thành những nỗ lực tội phạm có tổ chức để lừa đảo các công ty và cá nhân. Nói cách khác, bây giờ đây, nó liên quan đến tiền bạc hơn bao giờ hết.
* **virus**: Một virus là một chương trình máy tính có khả năng nhân bản hoặc tạo ra các bản sao của chính nó và lây lan sang các tệp khác. Ngoài khả năng nhân bản, hầu hết các virus máy tính còn chứa một "gói dữ liệu" (payload). Gói dữ liệu có thể khá vô hại, ví dụ như hiển thị một thông điệp hoặc hình ảnh, hoặc nó có thể rất phá hủy - gây hủy hoại cho các tệp, định dạng lại ổ cứng máy tính hoặc làm cho các chương trình chạy không đúng cách.
* **worm**: Các loại virus thường được kết hợp với sâu máy tính (worm). Thay vì chỉ lây lan từ tệp này sang tệp khác, sâu máy tính được thiết kế để lây lan từ máy tính này sang máy tính khác. Một sâu máy tính không nhất thiết cần phải được kích hoạt bởi người dùng hoặc chương trình để sao chép chính nó. Sâu máy tính Slammer là một trong những loại sâu nổi tiếng nhất. Slammer đã tấn công vào một lỗ hổng đã biết trong phần mềm cơ sở dữ liệu SQL Server của Microsoft và nhiễm trùng hơn 90% máy tính dễ bị tổn thất trên toàn cầu trong vòng 10 phút sau khi xuất hiện trên Internet. Nó gây ra sự cố cho máy rút tiền của Bank of America, đặc biệt ở phần tây nam của Hoa Kỳ, ảnh hưởng đến các máy tính quản lý tiền ở siêu thị như chuỗi Publix ở Atlanta, khiến nhân viên không thể phục vụ người mua một cách thoải mái; và làm đứt kết nối Internet tại Hàn Quốc, gây sụt giảm trên thị trường chứng khoán nơi đó. Sâu máy tính Conficker (còn được gọi là Downad), xuất hiện lần đầu vào năm 2008, là sâu máy tính nguy hiểm nhất kể từ Slammer và đã lây nhiễm khoảng 11 triệu máy tính trên toàn cầu. Ban đầu được thiết kế để thiết lập một mạng botnet toàn cầu, nỗ lực lớn của ngành công nghiệp đã đánh bại nó, nhưng vào năm 2017, Conficker đã được các hacker tái xuất để giúp nhiễm trùng máy tính bằng phần mềm ransomware WannaCry. Nó vẫn là một trong những mối đe dọa malware phổ biến nhất trên Internet.
* **ransomware**: Ransomware là một loại phần mềm độc hại (thường là sâu máy tính) khóa máy tính hoặc tệp tin của bạn để ngăn bạn truy cập chúng. Ransomware thường hiển thị một thông báo thông báo rằng một cơ quan như FBI, Bộ Tư pháp hoặc Cục Thuế (IRS) đã phát hiện hoạt động phi pháp trên máy tính của bạn và đòi bạn phải trả một khoản tiền phạt để mở khóa máy tính và tránh bị truy tố. Một loại ransomware được gọi là CryptoLocker. CryptoLocker mã hóa các tệp của nạn nhân bằng một hệ mã hóa không đối xứng gần như không thể bẻ khóa và đòi tiền chuộc để giải mã chúng, thường trong dạng tiền ảo Bitcoins. Nếu nạn nhân không tuân thủ trong khoảng thời gian cho phép, các tệp sẽ không bao giờ có thể được giải mã. Các biến thể khác bao gồm CryptoDefense và Cryptowall. Sự gia tăng của ransomware cũng liên quan đến sự phát triển của tiền ảo Bitcoin. Các hacker thường yêu cầu nạn nhân trả tiền bằng Bitcoin để giao dịch của họ được che giấu khỏi các cơ quan thụ động. Vào năm 2017, WannaCry, cuộc tấn công ransomware phổ biến nhất đến nay, đã xảy ra. WannaCry đã nhiễm trùng hơn 230.000 máy tính ở hơn 150 quốc gia, bao gồm máy tính trong Dịch vụ Y tế Quốc gia của Anh, Telefónica (hệ thống viễn thông của Tây Ban Nha), FedEx và Deutsche Bahn (hệ thống đường sắt chính của Đức). WannaCry đã tấn công vào các máy tính chạy các phiên bản khác nhau của hệ điều hành Microsoft Windows, mã hóa dữ liệu và sau đó đòi một khoản tiền chuộc bằng Bitcoins (khoảng 300 đô la) để giải mã dữ liệu. WannaCry đã lợi dụng một lỗ hổng phần mềm được gọi là EternalBlue trong các phiên bản cũ của hệ điều hành Windows để sao chép chính nó và lây lan. Theo các công ty bảo mật mạng khác nhau, mã nguồn được sử dụng trong WannaCry có sự tương đồng với mã nguồn trước đây được một nhóm hacker liên quan đến Bắc Triều Tiên sử dụng. Bắc Triều Tiên đã phủ nhận trách nhiệm. Các cuộc tấn công ransomware tiếp tục diễn ra, bao gồm Petya/NotPetya, sử dụng một phương thức tấn công rất giống với WannaCry. Sau khi giảm số lượng vào năm 2018, số lượng cuộc tấn công ransomware, cũng như số tiền trung bình mà nạn nhân trả, đã tăng lên vào năm 2019, và tập trung vào tấn công từ cá nhân chuyển sang các doanh nghiệp nhỏ và vừa cũng như các cơ quan đô thị. Trong nhiều trường hợp, các hacker nhắm vào các nhà cung cấp dịch vụ quản lý xử lý hệ thống máy tính cho các tổ chức như vậy (Popper, 2020; Symantec, 2019; Dudley, 2019).
* **Trojan horse**: Trojan horse trông như là vô hại, nhưng sau đó thực hiện một hành động khác so với dự kiến. Trojan horse không phải là một loại virus vì nó không tự nhân bản, nhưng thường là một cách để virus hoặc mã độc hại khác như bots hoặc rootkits (chương trình mục tiêu là phá vỡ sự kiểm soát của hệ điều hành máy tính) xâm nhập vào hệ thống máy tính. Thuật ngữ "Trojan horse" xuất phát từ con ngựa gỗ khổng lồ trong sử thi Iliad của Homer mà người Hy Lạp tặng cho đối thủ của họ, người Troia - một món quà thực sự chứa đựng hàng trăm lính Hy Lạp. Khi người dân Troia để con ngựa khổng lồ đó vào trong cổng thành, những người lính đã tiết lộ bản thân và bắt giữ thành phố.

Trong thế giới hiện đại, một Trojan horse có thể giả dạng thành một trò chơi, nhưng thực chất ẩn chứa một chương trình để đánh cắp mật khẩu của bạn và gửi chúng đến một người khác. Các loại Trojan và các chương trình tải về và triệu chứng Trojan (các Trojan cài đặt các tệp tin độc hại lên máy tính đã bị nhiễm độc thông qua việc tải chúng từ máy tính từ xa hoặc từ một bản sao chứa trong mã của họ) là một loại phổ biến của mã độc hại. Vào năm 2011, Sony đã trải qua vụ vi phạm dữ liệu lớn nhất trong lịch sử vào thời điểm đó khi một Trojan horse tiếp quản máy tính quản trị của Trung tâm trò chơi PlayStation của Sony và tải xuống thông tin cá nhân và thẻ tín dụng liên quan đến 77 triệu người dùng đã đăng ký (Wakabayashi, 2011). Trojan horse thường được sử dụng cho phần mềm độc hại tài chính được phân phối thông qua botnet. Một ví dụ là Zeus, một chương trình đánh cắp thông tin bằng cách ghi nhớ các phím được ấn và đã nhiễm trùng hơn 10 triệu máy tính kể từ khi nó xuất hiện lần đầu vào năm 2007. Các ví dụ khác bao gồm Tinba, một loại ransomware, Ramnit, được thiết kế để đánh cắp thông tin về tài khoản ngân hàng, mật khẩu FTP, cookie phiên và dữ liệu cá nhân; và hai họ con ngựa mộ Trojan, Emotet và Trickbot, đã phát triển từ Trojan ngân hàng thành botnet và theo Malwarebytes Labs, đã là mối đe dọa được phát hiện nhiều nhất ở gần như mọi khu vực trên toàn thế giới (Malwarebytes Labs, 2020; Symantec, 2019; Check Point Software Technologies, Inc., 2017).

* **backdoor**: Một cửa sau (backdoor) là một tính năng của virus, sâu máy tính và Trojan cho phép một kẻ tấn công từ xa truy cập vào máy tính bị nhiễm trùng. Downadup là một ví dụ về một sâu máy tính có cửa sau, trong khi Virut, một loại virus nhiễm trùng nhiều loại tệp tin khác nhau, cũng bao gồm một cửa sau có thể được sử dụng để tải về và cài đặt các mối đe dọa bổ sung.
* **bots and botnets**: Bot (viết tắt của robots) là một loại mã độc hại có thể được cài đặt một cách bí mật trên máy tính của bạn khi kết nối với Internet. Sau khi được cài đặt, bot phản hồi các lệnh bên ngoài gửi bởi kẻ tấn công; máy tính của bạn trở thành một "xác sống" và có thể được kiểm soát bởi một bên thứ ba bên ngoài (người điều khiển "bot-herder"). Botnet là một tập hợp các máy tính bị kiểm soát được sử dụng cho các hoạt động độc hại như gửi thư rác, tham gia vào cuộc tấn công DDoS hoặc chiến dịch stuffing thông tin đăng nhập (các cố gắng đăng nhập độc hại), đánh cắp thông tin từ máy tính và lưu trữ lưu lượng mạng để phân tích sau này. Số lượng botnet hoạt động trên toàn thế giới không biết nhưng được ước tính lên đến hàng ngàn, kiểm soát hàng triệu máy tính. Bot và mạng bot là mối đe dọa quan trọng đối với Internet và thương mại điện tử vì chúng có thể được sử dụng để thực hiện các cuộc tấn công quy mô lớn sử dụng nhiều kỹ thuật khác nhau. Năm 2011, các tư lệnh liên bang đã hỗ trợ các thành viên của đội ngũ tội phạm số của Microsoft trong các cuộc truy quét nhằm tắt botnet Rustock, lúc đó là nguồn gửi thư rác hàng đầu trên thế giới với gần 500.000 máy tính dưới sự kiểm soát của máy chủ điều khiển và điều khiển của nó đặt tại sáu dịch vụ lưu trữ Internet tại Hoa Kỳ. Các quan chức đã tịch thu các máy chủ điều khiển Rustock tại các trang web lưu trữ và cho biết họ không biết máy chủ Rustock đang làm gì. Những thư rác thực sự đã được gửi từ các máy tính dưới sự điều khiển của các máy chủ Rustock (Wingfield, 2011). Năm 2013, Microsoft và FBI đã tham gia vào một cuộc chiến dịch botnet quyết liệt khác, nhắm vào 1.400 botnet Citadel dẫn xuất từ Zeus, đã được sử dụng vào năm 2012 để tấn công vào tài khoản ngân hàng tại các ngân hàng lớn trên khắp thế giới, thu về hơn 500 triệu đô la (Chirgwin, 2013). Năm 2015, một đội ngũ quốc tế đã tắt botnet Beebone, gồm 12.000 máy tính đã nhiễm trùng khoảng 30.000 máy tính mỗi tháng trên khắp thế giới thông qua các lần tải xuống không yêu cầu bằng Changeup, một con sâu biến thể được sử dụng để phân phối Trojan, sâu máy tính, cửa sau và loại mã độc hại khác (Constantin, 2015). FBI và cảnh sát Anh cũng đã ngăn chặn một botnet đã đánh cắp hơn 10 triệu đô la từ các ngân hàng (Pagliery, 2015). Như kết quả của những nỗ lực như vậy, số lượng bot đã giảm đáng kể, đặc biệt là ở Hoa Kỳ, mặc dù chúng vẫn tiếp tục đe dọa (Symantec, 2019).

Mã độc hại là mối đe dọa ở cả hai mức độ máy khách và máy chủ, mặc dù máy chủ thường có lợi thế của bảo vệ chống mã độc hại toàn diện hơn so với người tiêu dùng. Tại mức máy chủ, mã độc hại có thể làm sập toàn bộ một trang web, ngăn cản hàng triệu người sử dụng trang web. Các sự cố như vậy là khá hiếm gặp. Các cuộc tấn công mã độc hại thường xuyên hơn xảy ra tại mức máy khách, và thiệt hại có thể nhanh chóng lan rộng đến hàng triệu máy tính khác kết nối với Internet. Bảng 5.4 liệt kê một số ví dụ nổi tiếng về mã độc hại.



1. **POTENTIALLY UNWANTED PROGRAMS (PUPs)**

Ngoài mã độc hại, môi trường bảo mật thương mại điện tử còn phải đối mặt với các chương trình có thể không mong muốn (PUPs), đôi khi được gọi là các ứng dụng có thể không mong muốn (PUAs), chẳng hạn như phần mềm quảng cáo, phần mềm ký sinh trình duyệt, phần mềm giám sát và các ứng dụng khác, bao gồm phần mềm bảo mật giả mạo, thanh công cụ và các công cụ chẩn đoán PC, tự cài đặt trên máy tính, thường là không cần sự đồng ý được thông báo trước của người dùng. Các chương trình như vậy ngày càng được tìm thấy trên các trang mạng xã hội và trang nội dung do người dùng tạo ra, nơi người dùng bị lừa tải chúng. Sau khi được cài đặt, các ứng dụng này thường rất khó loại bỏ khỏi máy tính. Một ví dụ về một PUP là PCProtect, nó lây nhiễm vào các máy tính chạy hệ thống Windows. PCProtect tỏ ra là một chương trình chống phần mềm độc hại hợp pháp trong khi thực tế nó lại là mã độc hại.

* **adware**: Phần mềm quảng cáo thường được sử dụng để hiển thị quảng cáo pop-up khi người dùng truy cập vào một số trang web cụ thể. Nó ngày càng được sử dụng như một công cụ bởi các tội phạm mạng. Theo Malwarebytes Labs, phần mềm quảng cáo đã là mục đe dọa hàng đầu đối với người tiêu dùng vào năm 2019 (Malwarebytes Labs, 2020).
* **browser parasite**: Một ký sinh trình duyệt (còn được gọi là một công cụ áp đặt cài đặt trình duyệt) là một chương trình có khả năng theo dõi và thay đổi các cài đặt của trình duyệt của người dùng, ví dụ, thay đổi trang chủ của trình duyệt hoặc gửi thông tin về các trang web đã truy cập đến một máy tính từ xa. Ký sinh trình duyệt thường là một phần của phần mềm quảng cáo. Năm 2015, Lenovo đã đối mặt với một loạt chỉ trích khi có thông tin rò rỉ rằng hãng đã gửi các laptop chạy hệ điều hành Windows với phần mềm quảng cáo Superfish được cài đặt sẵn. Superfish đã tiêm kết quả mua sắm riêng vào trình duyệt của máy tính khi người dùng tìm kiếm trên Google, Amazon hoặc các trang web khác. Trong quá trình này, Superfish đã tạo ra một rủi ro bảo mật bằng cách cho phép người khác trên mạng Wi-Fi chiếm quyền điều khiển trình duyệt mà không để lại dấu vết và thu thập bất cứ thứ gì được gõ vào đó. Cuối cùng, Lenovo đã phát hành một công cụ gỡ bỏ để cho phép khách hàng xóa phần mềm quảng cáo. Microsoft và các công ty bảo mật chính thống đã định nghĩa lại các chương trình phần mềm quảng cáo là mã độc hại và khuyến cáo các nhà sản xuất không nên gửi sản phẩm kèm các chương trình phần mềm quảng cáo (Loeb, 2016).
* **cryptojacking**: Cryptojacking cài đặt một loại ký sinh trình duyệt hút sức mạnh xử lý của máy tính để đào tiền điện tử mà không có sự hiểu biết hoặc sự đồng ý của người dùng. Theo Webroot, vào năm 2019, gần 9 triệu URL đã lưu trữ một kịch bản cryptojacking (Webroot, 2020).
* **spyware**: Phần mềm giám sát có thể được sử dụng để thu thập thông tin như các phím người dùng bấm, bản sao của thư điện tử và tin nhắn tức thời của họ, và thậm chí chụp ảnh màn hình (và từ đó lấy được mật khẩu hoặc dữ liệu tài khoản bí mật khác).

1. **PHISHING**

* **social engineering**: kỹ thuật xã hội dựa vào sự tò mò, lòng tham, tính dễ bị đánh lừa và sợ hãi của con người để đánh lừa họ thực hiện một hành động dẫn đến việc tải xuống phần mềm độc hại. Kevin Mitnick, cho đến khi bị bắt và giam giữ vào năm 1999, là một trong những tội phạm máy tính nổi tiếng nhất của Hoa Kỳ. Mitnick đã sử dụng các kỹ thuật lừa dối đơn giản để lấy mật khẩu, số An Sinh Xã Hội và hồ sơ cảnh sát, tất cả đều không cần sử dụng bất kỳ công nghệ phức tạp nào (Mitnick, 2011). Đầu năm 2020, số lượng tấn công sử dụng các kỹ thuật xã hội dựa trên sự bùng nổ lo sợ về đại dịch Covid-19 cũng như sự quan tâm đến các chương trình kích thích liên quan đã tăng mạnh, Ví dụ, một cuộc tấn công ẩn phần mềm độc hại trong một bản đồ hiển thị thống kê về virus corona; một cuộc tấn công khác liên quan đến một email giả mạo từ Tổ chức Y tế Thế giới, khuyến khích người nhận tải xuống một cuốn sách điện tử giả mạo chứa nghiên cứu về đại dịch cũng như thông tin về cách bảo vệ trẻ em (Pipikaite và Davis, 2020; Đội Thông tin đe doạ, 2020).
* phishing: Lừa đảo thông qua mạng phishing là bất kỳ nỗ lực trực tuyến gian lận của bên thứ ba để thu thập thông tin mật cho mục đích tài chính. Các cuộc tấn công lừa đảo thông qua mạng phishing thường không liên quan đến mã độc hại mà thay vào đó dựa vào biểu dị và gian lận trực tiếp, các kỹ thuật "xã hội hóa". Một trong những cuộc tấn công lừa đảo thông qua mạng phishing phổ biến nhất là thư lừa đảo qua email. Cuộc lừa đảo bắt đầu bằng một email: một cựu bộ trưởng dầu mỏ giàu có của Nigeria đang tìm kiếm một tài khoản ngân hàng để lưu trữ hàng triệu đô la trong một thời gian ngắn, và yêu cầu số tài khoản ngân hàng của bạn để tiền có thể được gửi vào đó. Đáp ứng, bạn sẽ nhận được một triệu đô la. Loại lừa đảo qua email này thường được biết đến với tên "cuộc lừa đảo qua thư Nigeria" (xem Hình 5.4). Theo nhóm nghiên cứu đe doạ của Palo Alto Networks, các cuộc tấn công qua email Nigeria, đặc biệt là những cuộc tấn công qua email Nigeria từ một nhóm tội phạm mạng Nigeria được biết đến với tên SilverTerrier, đã trở nên phức tạp hơn nhiều và nguy hiểm hơn. Trong suốt năm 2019, dịch vụ phân tích phần mềm độc hại Wildfire của Palo Alto đã phát hiện hơn 27.000 trường hợp phần mềm độc hại SilverTerrier (Scroxton, 2020).
* BEC (business e-mail compromise) phishing: Hàng ngàn cuộc tấn công qua mạng lừa đảo thông qua mạng khác sử dụng các chiêu trò khác, một số giả vờ là eBay, PayPal hoặc Citibank gửi email yêu cầu bạn xác minh tài khoản của bạn (được gọi là spear phishing, hoặc nhắm vào khách hàng biết đang gửi tiền cho một ngân hàng cụ thể hoặc loại hình kinh doanh khác). Bấm vào liên kết trong email và bạn sẽ được đưa đến một trang web do kẻ lừa đảo kiểm soát và bắt bạn nhập thông tin mật về tài khoản của bạn, chẳng hạn như số tài khoản và mã PIN cá nhân. Trong bất kỳ ngày nào, hàng triệu email tấn công lừa đảo này được gửi, và không may thay, một số người bị lừa và tiết lộ thông tin tài khoản cá nhân của họ. Theo công ty nghiên cứu bảo mật Check Point Research, trong quý đầu năm 2020, Apple là thương hiệu được hacker mô phỏng nhiều nhất trong các cuộc tấn công lừa đảo thông qua mạng, theo sau bởi Netflix (Check Point Software Technologies, Inc., 2020).
* Người lừa đảo dựa vào các kỹ thuật của "kẻ lừa dối" truyền thống, nhưng sử dụng email hoặc các hình thức truyền thông trực tuyến khác, chẳng hạn như mạng xã hội hoặc tin nhắn văn bản, để lừa người nhận tự nguyện cung cấp mã truy cập tài chính, số tài khoản ngân hàng, số thẻ tín dụng và thông tin cá nhân khác. Thường xuyên, người lừa đảo tạo ra (hoặc "giả mạo") một trang web giả mạo với tạo tượng là một tổ chức chính thống và lừa dối người dùng nhập thông tin tài chính, hoặc trang web tải xuống phần mềm độc hại như một trình theo dõi phím tự động vào máy tính của nạn nhân. Ví dụ, công ty nghiên cứu bảo mật Venafi đã phát hiện ra rằng có tới bốn lần số lượng trang web bán lẻ giả mạo thiết kế để thu thập thông tin của khách hàng so với trang web bán lẻ thực và số lượng trang web giả mạo như vậy đã tăng gấp đôi kể từ năm 2018 (Vaas, 2019). Người lừa đảo sử dụng thông tin họ thu thập để thực hiện các hành vi gian lận như trừ tiền từ thẻ tín dụng của bạn hoặc rút tiền từ tài khoản ngân hàng của bạn, hoặc theo cách khác "ăn cắp danh tính" của bạn (gian lận danh tính). Một cuộc khảo sát của Webroot cho biết gần một nửa trong số 4.000 người được khảo sát nói rằng dữ liệu cá nhân hoặc tài chính của họ đã bị lộ thông qua tin nhắn lừa đảo qua email (Webroot, 2019). Symantec báo cáo rằng vào năm 2018, khoảng 1 trong mỗi 3.207 email chứa cuộc tấn công lừa đảo qua email, một sự giảm sút nhẹ về tỷ lệ so với năm 2017. (Symantec, 2019). Tuy nhiên, một số loại lừa đảo thông qua mạng, chẳng hạn như lừa đảo qua email kinh doanh BEC và lừa đảo qua mạng spear phishing, vẫn tiếp tục tăng lên, và đầu năm 2020, các nhà nghiên cứu về an ninh cảnh báo về sự gia tăng của lừa đảo qua email kinh doanh BEC cụ thể, đặc biệt là khi có quá nhiều người làm việc từ xa tại nhà và do đó không thể dễ dàng xác minh tính chính xác của người gửi email, cũng như sự gia tăng của email lừa đảo với chủ đề về virus corona (Moffitt, 2020; Culafi, 2020). Để chống lại lừa đảo qua email, vào năm 2012, các nhà cung cấp dịch vụ email hàng đầu, bao gồm Google, Microsoft, Yahoo và AOL, cùng với các công ty dịch vụ tài chính như PayPal, Ngân hàng Mỹ và các công ty khác, đã hợp tác để thành lập DMARC.org, một tổ chức nhằm giảm đáng kể việc giả mạo địa chỉ email, trong đó những người tấn công sử dụng địa chỉ email thật để gửi email lừa đảo cho những nạn nhân có thể bị đánh lừa vì email dường như có nguồn gốc từ một nguồn mà người nhận tin cậy. DMARC (Domain-based Message Authentication, Reporting, and Conformance) cung cấp một phương thức xác thực nguồn gốc của email và cho phép người nhận cách ly, báo cáo hoặc từ chối các thông điệp không vượt qua bài kiểm tra của nó. Yahoo và AOL đã báo cáo thành công đáng kể trong việc chống lừa đảo qua email như một kết quả của việc sử dụng DMARC, và vào năm 2016, Google đã tham gia với họ để triển khai một phiên bản nghiêm ngặt hơn của DMARC, trong đó email không vượt qua các kiểm tra xác thực DMARC sẽ bị từ chối. Vào năm 2019, hơn 80% tất cả các miền của liên bang và hơn 50% các công ty trong danh sách Fortune 500 đã sử dụng DMARC, tăng lên từ chỉ một phần ba vào năm 2017 (Garcia-Tobar, 2019)

1. **HACKING, CYBERVANDALISM, AND HACKTIVISM**

* hacker: Một hacker là một cá nhân có ý định truy cập máy tính một cách trái phép.
* cracker: Trong cộng đồng hacking, thuật ngữ cracker thường được sử dụng để chỉ một hacker có ý định tội phạm.

Tuy nhiên trong báo chí công chúng, các thuật ngữ hacker và cracker thường được sử dụng một cách thay đổi. Hacker và cracker có thể truy cập một cách trái phép bằng cách tìm ra các điểm yếu trong các quy trình bảo mật của các trang web và hệ thống máy tính, thường tận dụng các tính năng của Internet làm cho nó trở thành một hệ thống mở dễ sử dụng. Trong quá khứ, hacker và cracker thường là những người đam mê máy tính phấn khích trước thách thức của việc xâm nhập vào các trang web của doanh nghiệp và chính phủ. Đôi khi họ chỉ cần bẻ khóa vào các tệp của một trang web thương mại điện tử. Ngày nay, hầu hết các hacker có ý định ác ý để làm gián đoạn, phá hủy hoặc tiêu diệt trang web (cybervandalism) hoặc đánh cắp thông tin cá nhân hoặc doanh nghiệp mà họ có thể sử dụng để có lợi ích tài chính (data breach). Năm 2020, giữa đại dịch Covid-19, tạo ra một làn sóng quan tâm đến việc sử dụng công cụ họp trực tuyến Zoom (xem Hệ thống Ghi âm Chương 3 về Zoom để biết thêm thông tin về Zoom), một hình thức mới của cybervandalism xuất hiện: "Zoombombing." Hacker, tận dụng các điểm yếu về bảo mật của Zoom, đã thể xâm nhập vào cuộc họp trực tuyến trên Zoom và truyền tải nội dung khiêu dâm, lời lẽ phân biệt chủng tộc và nội dung gây nhiễu loạn khác đến các người tham dự cuộc họp. Bộ Tư pháp Hoa Kỳ đã cảnh báo rằng nó sẽ truy cứu bản án về việc Zoombombing và Zoom cam kết sẽ thực hiện mọi biện pháp cần thiết để đối phó với mối đe dọa.

* hacktivism: Hacktivism thêm vào hacking một nét đặc trưng chính trị. Các nhóm hacktivists thường tấn công chính phủ, tổ chức và thậm chí cá nhân với mục đích chính trị, sử dụng các chiến thuật của cybervandalism, cuộc tấn công dịch vụ phủ định phân tán, lấy cắp dữ liệu và doxing (thu thập và tiết lộ thông tin cá nhân của nhân vật công cộng, thường từ email, bài đăng trên mạng xã hội và các tài liệu khác). Họ thường tin rằng thông tin phải là miễn phí, vì vậy việc chia sẻ thông tin trước đây bí mật là một phần của sứ mệnh của họ. Một trong những tổ chức hacktivist nổi tiếng nhất là Wikileaks, được thành lập bởi Julian Assange và những người khác, đã phát hành tài liệu và email của Bộ Ngoại giao Hoa Kỳ, Bộ Quốc phòng Hoa Kỳ và Ủy ban Quốc gia Dân chủ vào năm 2016. LulzSec và Anonymous là hai nhóm hacktivist nổi bật khác. Một nhóm khác, được gọi là Shadow Brokers, đã chịu trách nhiệm về việc phát hành một số công cụ hacking từ NSA và thông tin về các lỗ hổng phần mềm quan trọng, bao gồm lỗ hổng EternalBlue được sử dụng trong cuộc tấn công ransomware WannaCry.

Các nhóm hacker được gọi là *tiger teams* đôi khi được các bộ phận an ninh của công ty sử dụng để kiểm tra các biện pháp bảo mật của riêng họ. Bằng cách thuê các hacker để xâm nhập vào hệ thống từ bên ngoài, công ty có thể xác định các điểm yếu trong giới hạn bảo mật của hệ thống máy tính. Loại hacker này thực hiện công việc của họ dưới hợp đồng, với sự đồng thuận từ các công ty mục tiêu rằng họ sẽ không bị truy cứu hình sự vì nỗ lực để xâm nhập. Các công ty phần cứng và phần mềm như Apple, Microsoft, Intel, HP và nhiều công ty khác thường sẵn sàng trả tiền thưởng cho các hacker phát hiện ra lỗi trong phần mềm và phần cứng của họ (Holland, 2020; Warren, 2018).

Còn có các hacker tin rằng họ đang theo đuổi một mục tiêu lớn hơn bằng cách xâm nhập và tiết lộ nhược điểm của hệ thống. Các hacker này phát hiện ra các điểm yếu trong bảo mật hệ thống, sau đó công bố các điểm yếu đó mà không gây ra sự gián đoạn cho trang web hoặc cố gắng tạo lợi ích từ việc khám phá của họ. Phần thưởng duy nhất của họ là sự danh tiếng của việc khám phá điểm yếu. Tuy nhiên, hành động của họ có sự nghi ngờ, đặc biệt khi các hacker như vậy tiết lộ những lỗ hổng bảo mật làm cho việc cho phép những tên tội phạm khác dễ dàng truy cập vào hệ thống.

1. **DATA BREACHES**

**Data breaches** -một việc xâm nhập dữ liệu xảy ra mỗi khi tổ chức mất kiểm soát đối với thông tin doanh nghiệp, bao gồm thông tin cá nhân của khách hàng và nhân viên, đến bên thứ ba. Trung tâm Tài nguyên Trộm Danh tính ghi nhận 1.473 việc xâm nhập dữ liệu vào năm 2019, tăng 17% so với năm 2018. Các việc xâm nhập dữ liệu liên quan đến lĩnh vực doanh nghiệp có tác động lớn nhất, chiếm khoảng 44% tổng số việc xâm nhập dữ liệu, tiếp theo là ngành y tế/chăm sóc sức khỏe, chiếm khoảng 36%. Hacker là nguyên nhân hàng đầu gây ra việc xâm nhập dữ liệu, chiếm 39% tổng số việc xâm nhập dữ liệu, tiếp theo là truy cập trái phép (36,5%) và lỗi của nhân viên (khoảng 5%). Các việc xâm nhập dữ liệu đã tiết lộ gần 165 triệu hồ sơ nhạy cảm, chẳng hạn như số bảo hiểm xã hội và dữ liệu tài khoản tài chính, cũng như hơn 700 triệu hồ sơ, chẳng hạn như tên người dùng và mật khẩu, được phân loại là không nhạy cảm. Tuy nhiên, những hồ sơ không nhạy cảm này sau đó có thể được sử dụng để thử truy cập vào tài khoản của người dùng, đặc biệt vì nghiên cứu cho thấy hơn 80% người dùng sử dụng cùng mật khẩu cho nhiều tài khoản (Trung tâm Tài nguyên Trộm Danh tính, 2020). Việc xâm nhập dữ liệu cũng là một công cụ hỗ trợ cho các cuộc tấn công sử dụng thông tin đăng nhập. Credential stuffing (còn gọi là "đống thông tin chứng minh") là một cuộc tấn công bằng vũ trụ mà hacker thực hiện thông qua botnets và các công cụ tự động bằng cách sử dụng các kết hợp tên người dùng và mật khẩu đã biết (được gọi là danh sách combo) thu thập từ các cuộc xâm nhập dữ liệu. Các cuộc tấn công bằng đống thông tin chứng minh đang trở nên ngày càng phổ biến, đặc biệt trong ngành dịch vụ tài chính theo Akamai, đã quan sát hơn 85 tỷ cuộc tấn công đối với khách hàng sử dụng dịch vụ của họ trong khoảng thời gian từ 2017 đến 2019, với cuộc tấn công lớn nhất gồm 55 triệu lần thử đăng nhập độc hại (Akamai Technologies, Inc., 2020).

Một số cuộc xâm nhập dữ liệu nổi tiếng nhất đã mới đây trở nên nổi tiếng bao gồm cuộc xâm nhập dữ liệu của Yahoo, được cho là cuộc xâm nhập lớn nhất trong lịch sử của một công ty duy nhất, tiết lộ danh tính của tất cả người dùng dịch vụ email của Yahoo (tổng cộng 3 tỷ người), cuộc xâm nhập dữ liệu của Marriott International, tiết lộ thông tin cá nhân của gần 400 triệu người và cuộc xâm nhập dữ liệu của Equifax, trong đó hacker đã truy cập và tải xuống các tệp dữ liệu cá nhân của gần 150 triệu người tiêu dùng tại Hoa Kỳ (khoảng 45% dân số Hoa Kỳ). Đọc Hệ thống Ghi âm Xã hội, Vụ xâm nhập dữ liệu của Marriott, để biết thêm thông tin về việc xâm nhập dữ liệu. Năm 2019, xu hướng tiếp tục, khi công ty dịch vụ tài chính Capitol One thông báo rằng thông tin liên quan đến hơn 100 triệu khách hàng của họ tại Hoa Kỳ và Canada đã bị tiết lộ (Frias, 2019).

1. **CREDIT CARD FRAUD/THEFT**

Việc mất thông tin thẻ tín dụng là một trong những sự cố khiếp sợ nhất trên Internet. Sự lo sợ rằng thông tin thẻ tín dụng sẽ bị đánh cắp ngăn người dùng thực hiện các giao dịch mua sắm trực tuyến trong nhiều trường hợp. Các thương gia trực tuyến sử dụng nhiều kỹ thuật để chống lại gian lận thẻ tín dụng, bao gồm việc sử dụng các công cụ phát hiện gian lận tự động, xem xét đơn hàng thủ công, từ chối đơn hàng đáng ngờ và yêu cầu các mức độ bảo mật bổ sung như địa chỉ email, mã bưu điện và mã bảo mật CVV.

Luật liên bang Hoa Kỳ giới hạn trách nhiệm của cá nhân trong trường hợp mất thẻ tín dụng là 50 đô la. Đối với các số tiền lớn hơn 50 đô la, thông thường công ty thẻ tín dụng sẽ trả số tiền đó, tuy nhiên, trong một số trường hợp, người bán có thể phải chịu trách nhiệm nếu họ không xác minh tài khoản hoặc không kiểm tra các danh sách đã công bố về các thẻ không hợp lệ. Ngân hàng thu hồi chi phí từ gian lận thẻ tín dụng bằng cách tính lãi suất cao hơn đối với số dư chưa thanh toán. Vào năm 2015, hệ thống thẻ tín dụng tại Hoa Kỳ bắt đầu chuyển sang thẻ tín dụng EMV, còn được gọi là thẻ thông minh hoặc thẻ chip. Đã phổ biến ở châu Âu, thẻ tín dụng EMV có một vi mạch máy tính thay vì dải từ tính có thể dễ dàng bị sao chép bởi các hacker và bán dưới dạng dữ liệu thải (xem Bảng 5.2). Mặc dù công nghệ EMV không thể ngăn chặn sự vi phạm dữ liệu xảy ra, nó đã làm cho việc lợi dụng từ việc đánh cắp hàng loạt số thẻ tín dụng trở nên khó khăn hơn (Riley, 2018).

Trong quá khứ, nguyên nhân phổ biến nhất gây ra gian lận thẻ tín dụng là thẻ bị mất hoặc bị đánh cắp và được người khác sử dụng, tiếp theo là việc nhân viên đánh cắp thông tin của khách hàng và lợi dụng danh tính bị đánh cắp (tội phạm xin thẻ tín dụng bằng danh tính giả). Ngày nay, nguyên nhân phổ biến nhất gây ra việc mất thẻ và thông tin thẻ là tấn công và đánh cắp hệ thống máy chủ của doanh nghiệp nơi lưu trữ thông tin về hàng triệu giao dịch mua thẻ tín dụng.

Các đơn đặt hàng quốc tế có nguy cơ gian lận cao hơn, với mức tổn thất gian lận gấp đôi so với các đơn đặt hàng trong nước. Nếu một khách hàng quốc tế đặt hàng và sau đó tranh chấp đơn đặt hàng, thương gia trực tuyến thường không có cách nào để xác minh rằng gói hàng thực sự đã được giao và chủ thẻ thẻ tín dụng là người đã đặt hàng. Do đó, hầu hết thương gia trực tuyến sẽ không xử lý đơn đặt hàng quốc tế.

Một vấn đề bảo mật trung tâm trong thương mại điện tử là sự khó khăn trong việc xác định danh tính của khách hàng. Hiện tại không có công nghệ nào có thể xác định một người một cách chắc chắn tuyệt đối. Ví dụ, một thẻ EMV bị mất hoặc bị đánh cắp có thể được sử dụng cho đến khi thẻ bị hủy, giống như thẻ dải từ tính. Cho đến khi danh tính của khách hàng có thể được đảm bảo, các công ty trực tuyến có nguy cơ mất cao hơn so với các công ty truyền thống hoạt động ngoại tuyến. Chính phủ liên bang đã cố gắng giải quyết vấn đề này thông qua Đạo luật Chữ ký Điện tử toàn cầu và Quốc gia (được gọi là "E-Sign" law), cho phép chữ ký số có cùng thẩm quyền như chữ ký viết tay trong lĩnh vực thương mại. Đạo luật này cũng nhằm làm cho chữ ký số trở nên phổ biến hơn và dễ sử dụng hơn. Các đạo luật tương tự ở cấp bang đã được thực thi bằng cách sử dụng khuôn khổ do Đạo luật Giao dịch Điện tử Đồng nhất (UETA) cung cấp. Mặc dù việc sử dụng chữ ký số vẫn chưa phổ biến trong lĩnh vực thương mại điện tử B2C, nhiều doanh nghiệp đã triển khai giải pháp chữ ký số, đặc biệt là cho việc ký kết hợp đồng B2B, dịch vụ tài chính, bảo hiểm, chăm sóc sức khỏe và chính quyền cũng như dịch vụ chuyên nghiệp. Hiện tại, DocuSign, Adobe Sign, Citrix RightSignature và OneSpan Sign là một số giải pháp chữ ký số phổ biến nhất. Chúng sử dụng nhiều kỹ thuật, chẳng hạn như xác định người dùng từ xa thông qua các cơ sở dữ liệu bên thứ ba hoặc xác minh thông tin cá nhân như hình ảnh giấy phép lái xe; các phương thức xác thực người dùng đa yếu tố (tên người dùng và mật khẩu, xác minh địa chỉ email, câu hỏi và câu trả lời bí mật, xác định sinh trắc học); và mã hóa khóa công khai/riêng tư để tạo ra một chữ ký số và dấu vết kiểm tra được nhúng có thể được sử dụng để xác minh tính toàn vẹn của chữ ký số. Các giải pháp chữ ký số trên di động cũng bắt đầu được triển khai.

1. **IDENTITY FRAUD**

Lừa đảo danh tính liên quan đến việc sử dụng trái phép dữ liệu cá nhân của người khác, chẳng hạn như số an sinh xã hội, giấy phép lái xe và/hoặc số thẻ tín dụng, cũng như tên người dùng và mật khẩu, để đạt lợi ích tài chính trái phép. Tội phạm có thể sử dụng dữ liệu như vậy để lấy vay, mua hàng hóa hoặc sử dụng các dịch vụ khác, chẳng hạn như dịch vụ điện thoại di động hoặc các dịch vụ công cộng khác. Kẻ xâm nhập mạng thường sử dụng nhiều kỹ thuật đã được mô tả trước đó, chẳng hạn như phần mềm gián điệp, lừa đảo, việc xâm nhập dữ liệu và lấy cắp thông tin thẻ tín dụng, với mục tiêu là lừa đảo danh tính. Việc xâm nhập dữ liệu, đặc biệt là thường dẫn đến việc lừa đảo danh tính.

Tội phạm về lừa đảo danh tính là một vấn đề quan trọng trên toàn thế giới. Năm 2019, theo Javelin Strategy & Research, khoảng 13 triệu người tiêu dùng tại Hoa Kỳ bị lừa đảo danh tính. Tổng số tiền mất mát do lừa đảo danh tính là khoảng 16,9 tỷ đô la, tăng lên 13% so với năm trước (Javelin Strategy & Research, 2020).

1. **SPOOFING, PHARMING, AND SPAM (JUNK) WEBSITES**

Spoofing liên quan đến việc cố gắng che giấu danh tính thật bằng cách sử dụng địa chỉ email hoặc địa chỉ IP của người khác. Chẳng hạn, một email bị spoofing sẽ có địa chỉ email người gửi giả mạo được thiết kế để đánh lừa người nhận về người gửi của email. IP spoofing liên quan đến việc tạo ra các gói TCP/IP sử dụng địa chỉ nguồn IP của người khác, cho thấy rằng các gói đang từ một máy chủ đáng tin cậy. Hầu hết các bộ định tuyến và tường lửa hiện tại có thể cung cấp bảo vệ chống IP spoofing. Spoofing một trang web đôi khi liên quan đến pharming, tự động chuyển hướng một liên kết web đến một địa chỉ khác với địa chỉ đích ban đầu, với trang web giả mạo là địa điểm đích ban đầu. Các liên kết được thiết kế để đưa người dùng đến một trang web có thể được đặt lại để gửi người dùng đến một trang web hoàn toàn không liên quan - một trang web có lợi cho hacker.

Mặc dù spoofing và pharming không gây trực tiếp thiệt hại cho các tệp hoặc máy chủ mạng, chúng đe dọa tính chính trị của một trang web. Ví dụ, nếu hacker chuyển hướng khách hàng đến một trang web giả mạo gần giống trang web thực sự, họ có thể thu thập và xử lý đơn hàng, hiệu quả đánh cắp doanh nghiệp khỏi trang web thực sự. Hoặc nếu mục tiêu là gây gián đoạn thay vì đánh cắp, hacker có thể thay đổi đơn hàng - làm tăng chúng hoặc thay đổi sản phẩm được đặt hàng - và sau đó gửi chúng đến trang web thực sự để xử lý và giao hàng. Khách hàng trở nên không hài lòng với việc giao hàng không đúng quy trình, và công ty có thể có sự biến động lớn về hàng tồn kho có thể ảnh hưởng đến hoạt động của nó.

Ngoài việc đe dọa tính chính trị, spoofing cũng đe dọa tính xác thực bằng cách làm cho việc phân biệt người gửi thật và người gửi giả mạo trở nên khó khăn. Hacker thông minh có thể làm cho nó gần như không thể phân biệt giữa danh tính thật và giả mạo hoặc địa chỉ web thật và giả mạo.

Các trang web spam (rác) (số lần được gọi là trang trang web) có một chút khác biệt. Đây là các trang web hứa hẹn cung cấp một số sản phẩm hoặc dịch vụ, nhưng thực tế chỉ là một tập hợp các quảng cáo cho các trang web khác, trong đó một số chứa mã độc hại. Chẳng hạn, bạn có thể tìm kiếm "[tên thành phố] thời tiết", sau đó nhấp vào một liên kết hứa hẹn thời tiết cục bộ của bạn, nhưng sau đó bạn phát hiện rằng tất cả trang web này chỉ hiển thị quảng cáo cho các sản phẩm liên quan đến thời tiết hoặc các trang web khác. Các trang web rác hoặc spam thường xuất hiện trong kết quả tìm kiếm và không liên quan đến email. Những trang web này đôi khi che giấu danh tính của họ bằng cách sử dụng tên miền tương tự với tên các công ty hợp pháp và chuyển hướng lưu lượng truy cập đến các tên miền được biết đến của người chuyển hướng rác spam.

1. **SNIFFING AND MAN-IN-THE-MIDDLE ATTACKS**

Một sniffer là một loại chương trình nghe lén theo dõi thông tin di chuyển qua mạng. Khi được sử dụng một cách hợp pháp, sniffers có thể giúp xác định các điểm rủi ro tiềm năng trong mạng, nhưng khi sử dụng cho mục đích tội phạm, chúng có thể gây hại và rất khó phát hiện. Sniffers cho phép hacker đánh cắp thông tin độc quyền từ bất kỳ nơi nào trên mạng, bao gồm mật khẩu, tin nhắn email, tệp công ty và báo cáo tuyệt mật. Chẳng hạn, các chương trình sniffer đã được sử dụng để đánh cắp hơn 160 triệu số thẻ tín dụng trong một kế hoạch hack toàn cầu nhắm vào các mạng công ty của các chuỗi cửa hàng bán lẻ như 7-Eleven và chuỗi cửa hàng Pháp Carrefour SA (Voreacos, 2013).

Wiretaps qua email là một biến thể của mối đe doạ từ sniffing. Wiretap qua email là một phương pháp ghi âm hoặc theo dõi lưu lượng email thông thường ở mức máy chủ thư. Wiretap qua email được sử dụng bởi nhà tuyển dụng để theo dõi các tin nhắn của nhân viên và bởi các cơ quan chính phủ để giám sát cá nhân hoặc các nhóm. Wiretap qua email có thể được cài đặt trên máy chủ và máy tính khách hàng. Ở Hoa Kỳ, Đạo luật USA PATRIOT cho phép FBI buộc các nhà cung cấp dịch vụ Internet (ISP) cài đặt một hộp đen trên máy chủ thư của họ để tịch thu email của một người hoặc nhóm người để sau này phân tích. Trong trường hợp của công dân Hoa Kỳ giao tiếp với công dân khác, một điều tra viên FBI hoặc luật sư chính phủ chỉ cần chứng nhận cho một thẩm phán trên Tòa án Giám sát Tình báo Nước ngoài Hoa Kỳ (FISC) gồm 11 thẩm phán là thông tin cần tìm kiếm có liên quan đến một cuộc điều tra hình sự đang diễn ra để được phép cài đặt chương trình. Thẩm phán không có quyền tự quyết định. Họ phải chấp thuận việc cài đặt wiretap dựa trên những tuyên bố không chứng minh của các đặc vụ chính phủ. Trong trường hợp hoạt động khủng bố đáng nghi, lực lượng thực thi pháp luật không cần thông báo cho tòa án trước khi cài đặt cáp hoặc e-mail. Sửa đổi năm 2007 của Đạo luật Điều tra Tình báo Nước ngoài năm 1978, được gọi là FISA, cung cấp quyền mới cho Cơ quan An ninh Quốc gia (NSA) để theo dõi email quốc tế và cuộc gọi điện thoại nơi một người ở Hoa Kỳ, và mục đích của việc ngăn chặn như là để thu thập tình báo nước ngoài (Đạo luật Điều tra Tình báo Nước ngoài năm 1978; Đạo luật Bảo vệ America năm 2007). Đạo luật Sửa đổi Về FISA năm 2017 kéo dài các quy định của FISA đến cuối năm 2023. Chương trình XKeyscore của NSA, được tiết lộ bởi Edward Snowden, là một dạng "wiretap" cho phép các nhà phân tích NSA tìm kiếm qua các cơ sở dữ liệu lớn chứa không chỉ email, mà còn trò chuyện trực tuyến và lịch sử duyệt web của hàng triệu cá nhân (Wills, 2013).

Đạo luật Hoa Kỳ về Hỗ trợ Giao tiếp cho Cảnh sát (CALEA) yêu cầu tất cả các nhà cung cấp truyền thông (bao gồm cả ISP) cung cấp quyền truy cập gần như tức thì cho các cơ quan thực thi pháp luật vào lưu lượng tin nhắn của họ. Nhiều dịch vụ Internet (như Facebook và LinkedIn) có tích hợp sẵn dịch vụ ISP kỹ thuật là không nằm trong phạm vi của CALEA. Chúng ta chỉ có thể giả định rằng những nhà điều hành email không phải là ISP này đồng tình với các cơ quan thực thi pháp luật. Khác với quá khứ, khi wiretap cần nhiều giờ để cắm trực tiếp vào đường điện thoại, trong hệ thống điện thoại kỹ thuật số hiện nay, việc cắm dây được sắp xếp trong vài phút bởi các nhà cung cấp lớn và tài khoản của họ.

Cuộc tấn công Man-in-the-middle (MitM) cũng liên quan đến việc nghe trộm nhưng hoạt động nhiều hơn so với cuộc tấn công sniffing, mà thường liên quan đến việc theo dõi bị động. Trong một cuộc tấn công MitM, kẻ tấn công có khả năng chặn các cuộc trò chuyện giữa hai bên tin rằng họ đang giao tiếp trực tiếp với nhau, trong khi thực tế, kẻ tấn công đang điều khiển các cuộc trò chuyện. Điều này cho phép kẻ tấn công thay đổi nội dung của cuộc trò chuyện.

1. **DENIAL OF SERVICE (DoS) AND DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS**

Trong cuộc tấn công từ chối dịch vụ (DoS), các hacker tấn công một trang web bằng cách gửi các yêu cầu trang web hoặc thông điệp không có giá trị nào đó đến máy chủ web của trang web, làm cho máy chủ bị quá tải và bị quá tải. Ngày càng, các cuộc tấn công DoS liên quan đến việc sử dụng các mạng bot và những cuộc tấn công "phân tán" được xây dựng từ hàng nghìn máy tính người dùng đã bị tấn công. Các cuộc tấn công DoS thường khiến trang web đóng cửa, làm cho người dùng không thể truy cập trang web. Đối với các trang web thương mại điện tử đông đúc, các cuộc tấn công này gây thiệt hại đáng kể; trong khi trang web bị đóng cửa, khách hàng không thể mua sắm. Và càng lâu trang web bị đóng cửa, thì càng nhiều thiệt hại gây đến danh tiếng của trang web. Mặc dù các cuộc tấn công như vậy không phá hủy thông tin hoặc truy cập vào các khu vực bị hạn chế của máy chủ, nhưng chúng có thể phá hủy doanh nghiệp trực tuyến của một công ty. Thường, các cuộc tấn công DoS thường đi kèm với việc tấn công cầu cứng chủ trang web để buộc chủ trang web trả tiền hàng trăm nghìn đô la hoặc hàng triệu đô la cho hacker để ngừng cuộc tấn công DoS.

Cuộc tấn công từ chối dịch vụ phân tán (DDoS) sử dụng hàng trăm hoặc thậm chí hàng ngàn máy tính để tấn công vào mạng mục tiêu từ nhiều điểm khởi đầu. Cuộc tấn công DoS và DDoS là mối đe doạ đối với hoạt động của hệ thống vì chúng có thể làm tắt nó mãi mãi. Các trang web lớn đã trải qua những cuộc tấn công như vậy, khiến các công ty nhận thức về tính dễ tổn thương của họ và cần luôn giới thiệu các biện pháp mới để ngăn chặn những cuộc tấn công trong tương lai. Theo Neustar, số lượng cuộc tấn công DDoS cả quy mô lớn và nhỏ tiếp tục tăng vào năm 2019 (Neustar, 2019). Các cuộc tấn công cũng đang tăng về sức mạnh. Chẳng hạn, cuộc tấn công DDoS lớn nhất trong lịch sử Internet đã được tiến hành vào tháng 2 năm 2020 đối với một khách hàng không được tiết lộ tên của Amazon Web Services, sử dụng dịch vụ Shield của AWS để làm giảm cuộc tấn công 2,3 Tbps (terabit mỗi giây) (Humphries, 2020).

Sự phát triển của Internet of Things (IoT), với hàng tỷ thiết bị kết nối Internet từ tủ lạnh đến camera an ninh có thể được sử dụng để gửi các yêu cầu dịch vụ đối với máy chủ, cũng tạo ra mối đe doạ mới (Cisco, 2018). Vào năm 2016, botnet Mirai đã tiến hành một cuộc tấn công DDoS quy mô lớn sử dụng các thiết bị Internet như vậy đối với một công ty giải quyết tên miền Internet, Dyn. Twitter, Amazon, Netflix, Airbnb, The New York Times và nhiều trang web khác trên toàn quốc bị ảnh hưởng. Hacker đã đoán được mật khẩu quản trị của các thiết bị thông dụng (thường được đặt thành mặc định như admin hoặc 12345), sau đó chèn hướng dẫn để tiến hành cuộc tấn công vào máy chủ Dyn (Sanger và Perlroth, 2016). Các cuộc tấn công DDoS thường giới hạn cho một công ty duy nhất, nhưng trong cuộc tấn công Dyn, công ty bị tấn công tình cờ lại là một trong các trung tâm chuyển đổi lớn của Internet tại Hoa Kỳ. Botnet IoT đã trở thành nền tảng ưa thích để tiến hành các cuộc tấn công DDoS.

Trong một biện pháp khác để đo lường tính phổ biến của các cuộc tấn công DDoS, trong một cuộc khảo sát của Netscout về các nhà cung cấp dịch vụ Internet và quản lý mạng trên toàn thế giới, người tham gia khảo sát cho biết số lượng cuộc tấn công DDoS đối với các dịch vụ SaaS đã tăng từ 13% lên 41% và số lượng cuộc tấn công đối với các trung tâm dữ liệu của bên thứ ba và dịch vụ đám mây đã tăng từ 11% lên 34% trong thời gian khảo sát. Netscout cũng

cho biết kích thước của các cuộc tấn công DDoS báo cáo đã tăng đáng kể, với các cuộc tấn công đạt trên 1 terabit về mặt băng thông và sử dụng nhiều biến thể của cuộc tấn công (Netscout, 2019). Một xu hướng khác là tạo khói che DDoS, trong đó kẻ tấn công sử dụng DDoS làm lạ distraction trong khi họ cũng chèn mã độc hoặc virus hoặc đánh cắp dữ liệu. Trong cuộc khảo sát gần đây, Neustar báo cáo rằng 90% trong số các công ty đã trải qua cuộc tấn công DDoS cũng đã báo cáo một dạng của sự vi phạm hoặc hoạt động liên quan đến sự vi phạm (Neustar, 2019). Và không có gì ngạc nhiên, khi kết nối dữ liệu di động đã trở nên nhanh hơn và ổn định hơn, các hacker đang bắt đầu tận dụng các thiết bị di động cho các cuộc tấn công DDoS dựa trên di động. Một cuộc tấn công bắt nguồn từ Trung Quốc đã sử dụng quảng cáo độc hại được tải trong các ứng dụng di động và trình duyệt di động như cơ chế tấn công (Majkowski, 2015).

1. **INSIDER ATTACKS**

Chúng ta thường nghĩ về các mối đe doạ về bảo mật đối với doanh nghiệp bắt nguồn từ bên ngoài tổ chức. Trên thực tế, mối đe doạ tài chính lớn nhất đối với các cơ sở doanh nghiệp không đến từ các vụ cướp mà đến từ việc trộm cắp bởi người bên trong tổ chức. Nhân viên ngân hàng trộm tiền nhiều hơn cả kẻ cướp ngân hàng. Điều tương tự cũng đúng đối với các trang web thương mại điện tử. Một số sự cố lớn gây ra sự gián đoạn trong dịch vụ, phá hủy trang web và làm chuyển hướng dữ liệu tài chính của khách hàng và thông tin cá nhân đã đến từ người bên trong - người trước đây từng là nhân viên được tin tưởng. Báo cáo của Cybersecurity Insiders về mối đe doạ từ người bên trong năm 2020 cho thấy rằng 70% tổ chức được khảo sát đã trải qua cuộc tấn công từ người bên trong trong vòng 12 tháng qua. Khảo sát của Ponemon Institute/IBM Security năm 2020 với hơn 200 tổ chức trên toàn cầu cho thấy tần suất các vụ cố ý từ bên trong tăng gấp ba lần giữa 2016 và 2019 và giá trị trung bình toàn cầu của mối đe doạ từ người bên trong là 11,45 triệu đô la. Nhân viên có quyền truy cập thông tin đặc biệt và khi quy trình bảo mật nội bộ yếu, họ thường có thể di chuyển trong toàn bộ hệ thống của tổ chức mà không để lại dấu vết. Nghiên cứu từ Đại học Carnegie Mellon ghi lại những thiệt hại đáng kể mà người bên trong gây ra cho cả tổ chức tư nhân lẫn tổ chức công. Đôi khi, người bên trong có thể không có ý đồ tội phạm, nhưng vô tình tiết lộ dữ liệu có thể sau đó bị khai thác bởi người khác. Các công ty phải lo ngại mức độ tương tự về việc rò rỉ dữ liệu vô tình/vô tình do sự bất cẩn của người dùng như họ lo ngại về người bên trong có ý đồ độc hại (Ponemon Institute/IBM Security, 2020; Cybersecurity Insiders, 2019; Viện Kỹ thuật Phần mềm, 2019).

1. **POORLY DESIGNED SOFTWARE**

* SQL injection attack
* zero-day vulnerability
* Heartbleed bug

Nhiều mối đe doạ về bảo mật đổ bộ vào phần mềm thiết kế kém chất lượng, đôi khi trong hệ điều hành và đôi khi trong phần mềm ứng dụng, bao gồm trình duyệt web. Sự tăng cường về phức tạp và kích thước của các chương trình phần mềm, cùng với yêu cầu về việc đưa sản phẩm ra thị trường đúng thời gian, đã đóng góp vào việc tăng lên số lượng các lỗ hoặc lỗ hổng phần mềm mà hacker có thể khai thác. Ví dụ, các cuộc tấn công SQL injection sử dụng lỗ hổng trong phần mềm ứng dụng web được thiết kế kém cỏi, không xác thực hoặc lọc dữ liệu mà người dùng nhập vào một trang web để chèn mã chương trình độc hại vào hệ thống và mạng của một công ty. Một kẻ tấn công có thể sử dụng lỗi xác nhận đầu vào này để gửi truy vấn SQL giả mạo đến cơ sở dữ liệu bên dưới để truy cập cơ sở dữ liệu, cài đặt mã độc hại hoặc truy cập các hệ thống khác trên mạng. Các ứng dụng web lớn có hàng trăm nơi cho việc nhập dữ liệu người dùng, mỗi nơi này đều tạo cơ hội cho cuộc tấn công SQL injection. Tin rằng một số lớn các ứng dụng web trực tuyến có lỗ hổng SQL injection và các công cụ sẵn có cho hacker để kiểm tra ứng dụng web để tìm các lỗ hổng này. Theo Akamai, cuộc tấn công SQL injection đã chiếm hơn 70% trong số tất cả các cuộc tấn công ứng dụng web giữa tháng 12 năm 2017 và tháng 11 năm 2019 (Akamai Technologies, Inc., 2020).

Mỗi năm, các công ty bảo mật xác định hàng ngàn lỗ hổng phần mềm trong các trình duyệt web, phần mềm PC, Macintosh và Linux, cũng như hệ điều hành và ứng dụng cho thiết bị di động. Ví dụ, vào năm 2019, hai lỗ hổng phần mềm nổi bật đã được tiết lộ trong cùng một tuần: lỗ hổng đầu tiên trong một số phiên bản cũ hơn của hệ điều hành Windows của Microsoft tương tự như một lỗ hổng đã bị lợi dụng bởi worm WannaCry và lỗ hổng thứ hai trong ứng dụng nhắn tin WhatsApp của Facebook cho phép hacker cài đặt phần mềm gián điệp trên điện thoại di động (McMillan, 2019). Một lỗ hổng zero-day là một lỗ hổng mà trước đó chưa được báo cáo và không có bản vá nào tồn tại. Theo Ponemon Institute, 80% cuộc tấn công thành công vào các điểm kết thúc của tổ chức trong năm 2019 được cho là là các cuộc tấn công zero-day và số lượng cuộc tấn công zero-day tăng thường xuyên hơn (Ponemon Institute, 2020). Thiết kế của máy tính cá nhân bao gồm nhiều cổng truyền thông mở có thể được sử dụng, và thậm chí đã được thiết kế để sử dụng, bởi máy tính bên ngoài để gửi và nhận tin nhắn. Các cổng thường bị tấn công bao gồm cổng TCP 445 (Microsoft-DS), cổng 80 (WWW/HTTP) và cổng 443 (TSL/SSL/HTTPS). Do tính phức tạp và mục tiêu thiết kế của chúng, tất cả hệ điều hành và phần mềm ứng dụng, bao gồm Linux và Macintosh, đều có lỗ hổng. Ví dụ, trong vụ việc bị xâm phạm dữ liệu của Equifax đã được đề cập trước đó trong chương, hacker đã lợi dụng lỗ hổng trong Apache Struts, một framework mã nguồn mở được sử dụng để xây dựng các ứng dụng web Java. Vào năm 2018, Google đã thông báo rằng họ đang đóng cửa mạng xã hội của họ, Google +, sau khi tiết lộ rằng một lỗ hổng phần mềm đã cho phép các nhà phát triển bên ngoài truy cập vào thông tin cá nhân của người dùng (Corbett, 2018).

Vào năm 2014, đã phát hiện một lỗ hổng trong hệ thống mã hóa OpenSSL, được sử dụng bởi hàng triệu trang web, được gọi là lỗi Heartbleed (xem Mục 5.3 để biết thêm thông tin về SSL). Lỗ hổng cho phép hacker giải mã phiên SSL và khám phá tên người dùng, mật khẩu và dữ liệu người dùng khác bằng cách sử dụng OpenSSL kết hợp với giao thức truyền thông gọi là giao thức heartbeat RFC6520 giúp người dùng từ xa duy trì liên lạc sau khi kết nối với máy chủ trang web. Trong quá trình này, một phần nhỏ của nội dung bộ nhớ máy chủ có thể rò rỉ ra ngoài (do đó được gọi là heartbleed), có khả năng đủ lớn để chứa mật khẩu hoặc khóa mã hóa có thể cho phép hacker khai thác máy chủ một cách thêm. Lỗi Heartbleed cũng ảnh hưởng đến hơn 1.300 ứng dụng Android. Cuối năm 2014, đã tiết lộ một lỗ hổng khác được gọi là ShellShock hoặc BashBug ảnh hưởng đến hầu hết các phiên bản của Linux và Unix, cũng như Mac OS X. ShellShock cho phép kẻ tấn công sử dụng CGI (xem Chương 4) để thêm các lệnh độc hại. Vào năm 2015, các nhà nghiên cứu thông báo rằng họ đã phát hiện một lỗ hổng SSL/TLS mới được gọi là FREAK (Factoring RSA Export Keys) cho phép các cuộc tấn công man-in-the-middle, cho phép sự chặn ngang và giải mã giao tiếp đã mã hóa giữa khách hàng và máy chủ, sau đó cho phép kẻ tấn công đánh cắp mật khẩu và thông tin cá nhân khác. Hơn 60% trang web đã mã hóa được cho là có thể bị tấn công thông qua lỗ hổng bảo mật này, bao gồm cả trang web của Nhà Trắng, Cục điều tra Liên bang và Cơ quan An ninh Quốc gia (Hackett, 2015; Vaughan-Nichols, 2015).

1. **SOCIAL NETWORK SECURITY ISSUES**

Các mạng xã hội như Facebook, Twitter, LinkedIn, Pinterest và Tumblr cung cấp môi trường phong phú và đáng giá cho các hacker. Trên các mạng xã hội, bạn có thể tìm thấy virus, chiếm đoạt trang web, gian lận về danh tính, ứng dụng chứa phần mềm độc hại, chuyển hướng click, lừa đảo, và thư rác. Ví dụ, vào tháng 7 năm 2020, một cuộc tấn công xã hội được tổ chức có thể lừa dối nhiều nhân viên của Twitter, giúp kẻ tấn công tiếp quản các tài khoản Twitter của hàng chục nhà lãnh đạo chính trị, giải trí và công nghệ nổi tiếng tại Hoa Kỳ và đăng một kế hoạch lừa đảo về Bitcoin. Các loại lừa đảo phổ biến khác trên mạng xã hội bao gồm các hình thức lừa đảo chia sẻ thủ công, trong đó các nạn nhân không biết rằng họ đang chia sẻ video, câu chuyện và hình ảnh có chứa liên kết đến các trang web độc hại và các chương trình khuyến mãi giả mạo mời nạn nhân tham gia sự kiện hoặc nhóm giả mạo với lời hứa như thẻ quà tặng miễn phí và yêu cầu người dùng chia sẻ thông tin của họ với kẻ tấn công. Các kỹ thuật khác bao gồm các nút Phản ứng giả mạo, khi nhấp vào đó, sẽ cài đặt phần mềm độc hại và đăng cập nhật lên Trang thông tin của người dùng, khiến cuộc tấn công lây lan rộng hơn, và các ứng dụng giả mạo. Bằng cách ẩn mình giữa bạn bè của chúng tôi, các hacker có thể giả vờ là bạn bè và lừa dối người dùng trong các cuộc lừa đảo.

Các công ty mạng xã hội cho đến nay vẫn chưa quá giỏi trong việc làm "cảnh sát" bởi họ đã không thể loại bỏ một cách mạnh mẽ các tài khoản gửi khách truy cập đến các trang web có chứa phần mềm độc hại. Mạng xã hội là mở cửa: bất kỳ ai cũng có thể thiết lập một trang cá nhân, kể cả tội phạm. Hầu hết các cuộc tấn công đều là cuộc tấn công xã hội mà kích thích khách truy cập nhấp vào các liên kết mà có vẻ hợp lý. Các ứng dụng xã hội được tải xuống từ mạng xã hội hoặc từ một trang web nước ngoài không được chứng nhận bởi mạng xã hội là sạch sẽ khỏi phần mềm độc hại. Nên luôn phải cẩn trọng khi nhấp chuột.

1. **MOBILE PLATFORM SECURITY ISSUES**

Sự bùng nổ trong số lượng thiết bị di động đã mở ra cơ hội rộng lớn cho các hacker. Người dùng di động đang lưu trữ thông tin cá nhân và tài chính trên thiết bị của họ và sử dụng chúng để tiến hành ngày càng nhiều giao dịch, từ mua sắm bán lẻ đến ngân hàng di động, khiến cho họ trở thành mục tiêu tuyệt vời cho các hacker. Nói chung, các thiết bị di động đối mặt với tất cả các rủi ro giống như bất kỳ thiết bị Internet nào cũng như một số rủi ro mới liên quan đến bảo mật mạng không dây. Ví dụ, các mạng Wi-Fi công cộng không được bảo mật rất dễ bị tấn công. Ví dụ, một lỗ hổng trong phiên bản cũ (WPA2) của giao thức bảo mật Wi-Fi đã cho phép các hacker thu thập mật khẩu, thư điện tử và dữ liệu khác trên các mạng Wi-Fi. Hơn 40% tất cả các thiết bị Android được phát hiện có thể bị ảnh hưởng bởi một biến thể đặc biệt tàn phá của cuộc tấn công (Ricker, 2017). Mặc dù hầu hết mọi người nhận thức được máy tính và trang web có thể bị tấn công và chứa phần mềm độc hại, nhiều người dùng điện thoại di động tin rằng điện thoại di động của họ là an toàn như một chiếc điện thoại bình thường. Giống như các thành viên mạng xã hội, người dùng điện thoại di động dễ dàng nghĩ rằng họ đang ở trong một môi trường chia sẻ đáng tin cậy.

Phần mềm độc hại trên điện thoại di động (thỉnh thoảng được gọi là các ứng dụng di động độc hại (MMAs) hoặc các ứng dụng di động giả mạo) đã được phát triển từ năm 2004 với Cabir, một loại sâu Bluetooth ảnh hưởng đến hệ điều hành Symbian (điện thoại Nokia) và làm cho điện thoại liên tục tìm kiếm các thiết bị hỗ trợ Bluetooth khác, nhanh chóng làm hết pin. Sâu iKee.B, được phát hiện lần đầu vào năm 2009, chỉ hai năm sau khi iPhone ra mắt, đã bị nhiễm trên các chiếc iPhone đã được jailbreak (sửa đổi để cho phép cài đặt các phiên bản iOS bị hack của bên thứ ba). Một chiếc iPhone ở châu Âu có thể bị hack bởi một chiếc iPhone ở Hoa Kỳ và toàn bộ dữ liệu cá nhân của nó được gửi đến một máy chủ ở Ba Lan. IKee.B đã xác định được khả năng của botnet điện thoại di động. Năm 2014, cuộc tấn công đầu tiên vào iPhone chưa được jailbreak (đã được sửa đổi để cho phép cài đặt các ứng dụng bên thứ ba) đã xảy ra, thông qua phần mềm độc hại được gọi là Wirelurker.

Năm 2018, Symantec đã chặn trung bình hơn 10.500 ứng dụng di động độc hại mỗi ngày. Cuộc tấn công ransomware di động tăng lên 33%. N

ăm 2019, Trend Micro đã xác định hơn 220.000 mẫu phần mềm độc hại cho ngân hàng di động, như phần mềm độc hại ngân hàng Anubis, được tìm thấy ẩn trong các ứng dụng trên cửa hàng Google Play với tên là Currency Converter và BatterySaver Mobi. Đa số các phần mềm độc hại di động vẫn tập trung vào nền tảng Android, mặc dù nền tảng iPhone của Apple đang bắt đầu bị tấn công nhiều hơn (Trend Micro, 2020; Symantec, 2019). Và không chỉ có các ứng dụng giả mạo mà còn có cả các ứng dụng chính thống phổ biến mà đơn giản không có bảo vệ khỏi sự tấn công của các hacker. Ví dụ, năm 2014, các nhà nghiên cứu bảo mật đã phát hiện rằng ứng dụng thanh toán di động của Starbucks, ứng dụng thanh toán di động phổ biến nhất tại Hoa Kỳ vào thời điểm đó, đã lưu trữ tên người dùng, địa chỉ thư điện tử và mật khẩu dưới dạng văn bản thuần túy, sao cho bất kỳ ai có quyền truy cập vào điện thoại có thể thấy mật khẩu và tên người dùng bằng cách kết nối điện thoại với máy tính. Theo các nhà nghiên cứu, Starbucks đã mắc sai lầm trong việc đặt yếu tố tiện lợi và dễ sử dụng lên trên bảo mật khi thiết kế ứng dụng (Schuman, 2014).

Các cuộc tấn công vishing nhắm vào những người dùng điện thoại di động dễ tin, bằng các thông điệp bằng lời để gọi số cố định và, ví dụ, quyên góp tiền cho trẻ em đang đói ở Haiti. Cuộc tấn công smishing sử dụng tin nhắn SMS. Tin nhắn văn bản đã bị nhiễm trùng có thể chứa địa chỉ thư điện tử và trang web có thể dẫn người dùng vô tội đến một trang web chứa phần mềm độc hại. Dịch vụ gian lận SMS của tội phạm đã xuất hiện, ẩn số điện thoại thực sự của kẻ tấn công trên thay vào đó là một tên chữ số giả. SMS gian lận cũng có thể được sử dụng bởi các tội phạm trực tuyến để mời người dùng di động vào một trang web độc hại bằng cách gửi một tin nhắn văn bản có vẻ đến từ một tổ chức hợp pháp trong trường hộp Từ và đề xuất người nhận nhấp vào một siêu liên kết URL độc hại để cập nhật tài khoản hoặc nhận một thẻ quà tặng. Một số ứng dụng tải xuống từ cửa hàng ứng dụng cũng đã chứa phần mềm độc hại. Madware - các ứng dụng trông vô hại chứa quảng cáo mở cửa sổ pop-up và tin nhắn văn bản trên thiết bị di động của bạn - cũng đang trở thành một vấn đề ngày càng gia tăng (Palan, 2019; McAfee, 2019).

1. **CLOUD SECURITY ISSUES**

Việc di chuyển nhiều dịch vụ Internet vào đám mây cũng đặt ra các rủi ro về bảo mật. Từ góc độ cơ sở hạ tầng, các cuộc tấn công DDoS đe dọa tính sẵn có của các dịch vụ đám mây mà ngày càng nhiều công ty đang phụ thuộc. Ví dụ, như đã đề cập trước đó, cuộc tấn công DDoS vào Dyn đã gây ra sự cố lớn cho các dịch vụ đám mây trên khắp Hoa Kỳ. Theo Alert Logic, các công ty có mạng hỗn hợp, với các ứng dụng phân tán trên các đám mây công cộng, đám mây riêng và hệ thống trên chỗ, đang đối mặt với nguy cơ cao nhất (Alert Logic, 2017). Bảo vệ dữ liệu đang được duy trì trong môi trường đám mây công cộng cũng là một vấn đề lớn (Cybersecurity Insiders/Alert Logic, 2018). Ví dụ, các nhà nghiên cứu đã xác định một số cách để truy cập dữ liệu mà không có sự cho phép trên Dropbox, dịch vụ chia sẻ tệp trên đám mây phổ biến. Năm 2014, các hình ảnh bị chiếm đoạt của tới 100 ngôi sao như Jennifer Lawrence đã được đăng trực tuyến, được cho là đã bị đánh cắp từ iCloud của Apple. Mặc dù ban đầu có vẻ như việc xâm nhập được thực hiện thông qua một lỗ hổng trong API Find My iPhone của Apple, nhưng có vẻ rằng nó thay vào đó xuất phát từ các cuộc tấn công lừa đảo kỹ thuật thấp hơn mà đã thu được mật khẩu có thể được sử dụng để kết nối với iCloud. Những sự việc này làm nổi bật các rủi ro khi các thiết bị, danh tính và dữ liệu trở nên ngày càng kết nối trong đám mây. Cuộc khảo sát Thales/Ponemon Institute năm 2019 với hơn 3.300 nhân viên bảo mật thông tin và công nghệ thông tin đã tìm thấy hơn 55% tin rằng việc sử dụng dịch vụ đám mây làm cho việc bảo vệ dữ liệu nhạy cảm trở nên khó khăn hơn. Cuộc khảo sát cũng tìm thấy hầu hết các tổ chức không đảm nhận trách nhiệm đầy đủ cho việc bảo mật dữ liệu của họ trong đám mây, thay vào đó nhìn vào các nhà cung cấp đám mây của họ để cung cấp bảo mật đó (Thales/Ponemon Institute, 2019).

1. **INTERNET OF THINGS SECURITY ISSUES**

Như bạn đã học ở Chương 3, Internet of Things (IoT) liên quan đến việc sử dụng Internet để kết nối nhiều loại cảm biến, thiết bị và máy móc, và đang thúc đẩy sự phát triển của rất nhiều vật kết nối thông minh, chẳng hạn như thiết bị điện tử gia đình (smart TV, bình nhiệt độ, hệ thống an ninh gia đình và nhiều thiết bị khác), ô tô kết nối, thiết bị y tế và thiết bị công nghiệp hỗ trợ cho ngành sản xuất, năng lượng, giao thông và các ngành công nghiệp khác. IoT đặt ra một loạt vấn đề về bảo mật có một cách tương tự với các vấn đề bảo mật hiện có, nhưng lại khó khăn hơn nhiều, do cần phải xử lý một loạt các thiết bị rộng lớn hoạt động trong môi trường toàn cầu không kiểm soát, và với phạm vi tấn công mở rộng. Trong một thế giới của những thứ kết nối, các thiết bị, dữ liệu được sản xuất và sử dụng bởi các thiết bị và các hệ thống và ứng dụng được hỗ trợ bởi các thiết bị đó, tất cả đều có thể bị tấn công. Bảng 5.5 giới thiệu một cái nhìn cận cảnh vào một số thách thức bảo mật đặc biệt do IoT gây ra, được xác định bởi Internet Society (ISOC), một liên minh của các tập đoàn, cơ quan chính phủ và tổ chức phi lợi nhuận theo dõi chính sách và thực tiễn của Internet (Internet Society, 2016, 2015).

Những báo cáo đáng báo động về các thiết bị IoT bị tấn công đã xuất hiện trên báo chí phổ biến. Ví dụ, các nhà nghiên cứu đã chứng minh khả năng xâm nhập vào một chiếc xe Jeep Cherokee thông qua hệ thống giải trí của nó, gửi các lệnh đến bảng điều khiển, tay lái, phanh và hệ thống truyền động từ một laptop từ xa, khiến bánh lái quay, tắt phanh và tắt máy (Greenberg, 2015). Fiat Chrysler Automobiles ngay lập tức ban hành thông báo triệu hồi để sửa lỗ hổng phần mềm liên quan, nhưng rất có thể rằng những sự việc như vậy sẽ tiếp tục xảy ra, khi các nhà sản xuất ô tô thêm nhiều tính năng "xe kết nối" không dây hơn cho các xe hơi. Các báo cáo khác đã xuất hiện về việc các máy theo dõi trẻ sơ sinh không dây bị tấn công, cũng như các thiết bị y tế như máy phân tích khí máu của phòng thí nghiệm bệnh viện, hệ thống lưu trữ và truyền tải hình ảnh trong ngành công nghiệp y học, máy bơm truyền dược và hệ thống tia X bệnh viện (Storm, 2015a, 2015b). Cuộc tấn công DDoS đã được đề cập trước đó vào Dyn được thực hiện bởi botnet Mirai dựa vào một phần trên hơn 500.000 thiết bị IoT như camera an ninh kết nối Internet (Sanger và Perlroth, 2016). Vào năm 2017, một botnet được biết đến với tên Reaper hoặc IoTroop đã hình thành, với các nhà phân tích bảo mật cảnh báo rằng nó đang tuyển dụng các thiết bị IoT như bộ định tuyến, máy quay và DVR với tốc độ nhanh hơn và có tiềm năng gây ra nhiều hơn sự cố hơn botnet Mirai (Kan, 2017). Sự chú tâm cũng được tập trung vào việc tấn công và lỗ hổng bảo mật liên quan đến các thiết bị kết nối Internet như camera chuông cửa Ring của Amazon và camera Nest của Google, TV thông minh, loa thông minh và thậm chí là bóng đèn thông minh và máy pha cà phê thông minh (Srinivas, 2020).

1. **TECHNOLOGY SOLUTIONS** (trang 324 - trang 338)

*Xem xét các mối đe dọa bảo mật trong phần trước, rõ ràng rằng* ***những mối đe dọa đối với thương mại điện tử là thực tế, phổ biến****, toàn cầu, có khả năng gây hậu quả nghiêm trọng cho cá nhân, doanh nghiệp và cả các quốc gia, và có thể tăng cường tính mãnh liệt theo sự phát triển của thương mại điện tử và mở rộng tiếp tục của Internet. Tuy nhiên, trên thực tế,* ***đã có sự tiến bộ đáng kể được thực hiện bởi các công ty bảo mật tư nhân, người dùng cá nhân và doanh nghiệp, quản trị mạng, các công ty công nghệ và các cơ quan chính phủ****. Trong phần này, chúng tôi xem xét một số giải pháp công nghệ sau:*

*■ Protecting Internet communications (Bảo vệ thông tin liên lạc trên Internet)*

*❖Encryption (Mã hóa)*

*■ Securing channels of communication (Bảo mật kênh truyền thông)*

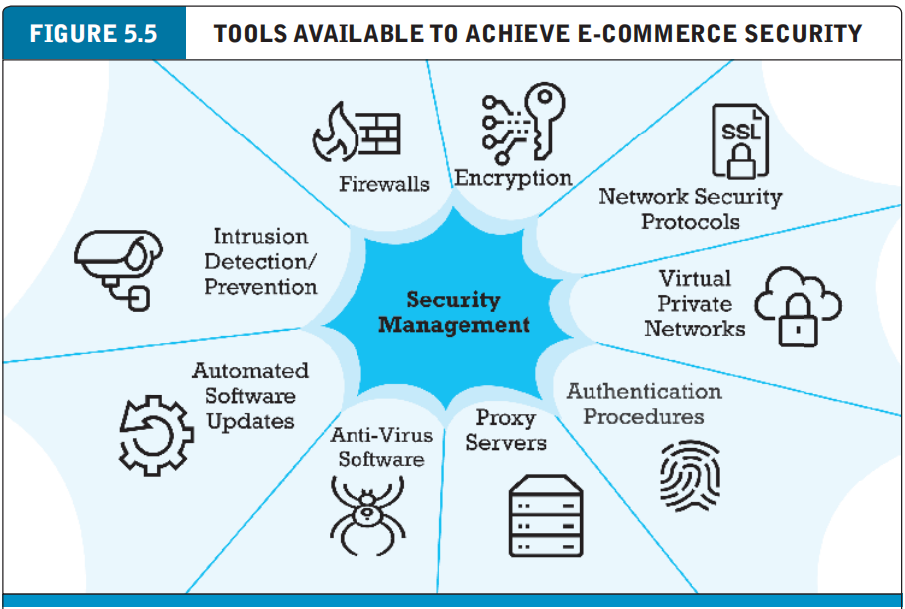
*❖SSL, VPNs*

*■ Protecting networks (Bảo vệ mạng)*

*❖Firewalls (Tường lửa)*

*■ Protecting servers and clients (Bảo vệ máy chủ và máy khách)*

*Dòng phòng thủ đầu tiên đối diện với nhiều loại mối đe dọa bảo mật thương mại điện tử là* ***một bộ công cụ có thể làm cho việc xâm nhập hoặc phá hủy trang web trở nên khó khăn đối với người ngoài****. Dưới đây mô tả các công cụ chính có sẵn để đảm bảo bảo mật thương mại điện tử.*



1. **PROTECTING INTERNET COMMUNICATIONS**

* Các giao dịch thương mại điện tử phải trôi qua Internet công cộng và thông qua hàng ngàn máy chủ và bộ định tuyến, các chuyên gia bảo mật cho rằng mối đe dọa lớn nhất xảy ra ở mức giao tiếp trên Internet.
* Khác biệt với mạng riêng tư, nơi một đường truyền truyền thông riêng biệt được thiết lập giữa hai bên.
* *Có nhiều công cụ để bảo vệ tính bảo mật của giao tiếp trên Internet, và mã hóa thông điệp là công cụ cơ bản nhất trong số đó.*

1. **ENCRYPTION**

* encryption (mã hóa) : là quá trình biến đổi văn bản thô hoặc dữ liệu thành văn bản mã hóa mà không thể đọc được bởi bất kỳ ai ngoài người gửi và người nhận.
* cipher text (văn bản mật mã) :văn bản đã được mã hóa và do đó không ai có thể đọc được ngoài người gửi và người nhận
* key (cipher) : phương pháp để chuyển văn bản gốc thành văn bản mật mã
* substitution cipher (mật mã thay thế): mỗi lần xuất hiện của một chữ cái nhất định đều được thay thế một cách có hệ thống bằng một chữ cái khác
* transposition cipher (mật mã chuyển vị): thứ tự các chữ cái trong mỗi từ được thay đổi một cách có hệ thống

*Mã hóa là quá trình chuyển đổi văn bản hoặc dữ liệu thuần túy thành văn bản mật mã mà không thể được đọc bởi bất kỳ ai khác ngoài người gửi và người nhận.* ***Mục đích của việc mã hóa là: (a) để bảo mật thông tin được lưu trữ và (b) để bảo mật việc truyền thông tin.***

*Mã hóa có thể cung cấp bốn trong số sáu khía cạnh chính của bảo mật thương mại điện tử được đề cập ở Bảng 5.3 trên trang 298:*

*•* ***Tính toàn vẹn của thông tin—cung cấp sự đảm bảo rằng thông tin không bị thay đổi.***

***• Chống chối bỏ—ngăn chặn người dùng từ chối việc họ đã gửi thông tin.***

***• Xác thực—cung cấp xác minh danh tính của người (hoặc máy tính)***

***gửi thông tin.***

***• Tính bảo mật—đảm bảo rằng thông tin không bị người khác đọc.***

Việc chuyển đổi văn bản thuần túy thành văn bản mật mã này được thực hiện bằng cách sử dụng khóa hoặc mật mã.

M*ã hóa đã được thực hiện kể từ những hình thức văn bản và giao dịch thương mại sớm nhất. Các hồ sơ thương mại của người Ai Cập và Phoenician cổ đại được mã hóa bằng cách sử dụng mật mã thay thế và hoán vị.* *Trong mật mã thay thế, mỗi lần xuất hiện của một chữ cái nhất định sẽ được thay thế một cách có hệ thống bằng một chữ cái khác.* Ví dụ: nếu chúng ta sử dụng mật mã “chữ cái cộng hai”—có nghĩa là thay thế mọi chữ cái trong một từ bằng một chữ cái mới tiến hai vị trí—thì từ “Xin chào” trong văn bản thuần túy sẽ được chuyển thành văn bản mật mã sau: “ JGNNQ.” *Trong mật mã chuyển vị, thứ tự các chữ cái trong mỗi từ được thay đổi một cách có hệ thống.* Leonardo Da Vinci đã ghi lại các ghi chú trong cửa hàng của mình theo thứ tự ngược lại, khiến chúng chỉ có thể đọc được khi soi gương. Từ “Xin chào” có thể được viết ngược là “OLLEH”. *Một mật mã phức tạp hơn sẽ (a) chia tất cả các từ thành hai từ và (b) đánh vần từ đầu tiên với mọi chữ cái khác bắt đầu bằng chữ cái đầu tiên, sau đó đánh vần từ thứ hai với tất cả các chữ cái còn lại.* Trong mật mã này, “HELLO” sẽ được viết là “HLO EL.”

2.1 Symmetric Key Cryptography

*Để giải mã những thông điệp này, người nhận cần phải biết khóa bí mật được sử dụng để mã hóa văn bản gốc. Điều này được gọi là mật mã khóa đối xứng hoặc mật mã khóa bí mật. Trong* ***Symmetric Key Cryptography (mật mã khóa đối xứng) cả người gửi và người nhận sử dụng cùng một khóa để mã hóa và giải mã thông điệp****. Làm thế nào để họ có cùng một khóa? Họ phải gửi nó qua các phương tiện truyền thông hoặc trao đổi khóa trực tiếp.* ***Đồng thời, cần yêu cầu bộ khóa khác nhau cho mỗi giao dịch****. Mật mã khóa đối xứng đã được sử dụng rộng rãi trong Thế chiến II và vẫn là một phần của mật mã trên Internet.*

Có vô số khả năng cho các mật mã thay thế và hoán vị đơn giản, nhưng chúng đều có nhược điểm chung. Trước hết, trong thời đại số hóa, máy tính mạnh mẽ và nhanh chóng đến mức các phương pháp mã hóa cổ điển này có thể bị giải mã một cách nhanh chóng. Thứ hai, mật mã khóa đối xứng yêu cầu cả hai bên phải chia sẻ cùng một khóa. Để chia sẻ cùng một khóa, họ phải gửi khóa qua một phương tiện truyền thông có thể bị đánh cắp và sử dụng để giải mã thông điệp. Nếu khóa bí mật bị mất hoặc đánh cắp, toàn bộ hệ thống mã hóa sẽ thất bại. Thứ ba, ***trong việc sử dụng thương mại, khi chúng ta không cùng một nhóm, bạn sẽ cần một khóa bí mật cho mỗi bên mà bạn giao dịch, tức là, một khóa cho ngân hàng, một khóa khác cho cửa hàng, và một khóa khác cho chính phủ*.** Trong một dân số lớn người dùng, điều này có thể dẫn đến cần đến n(n–1) khóa. Trong một dân số hàng tỷ người sử dụng Internet, cần hàng tỷ khóa để phục vụ tất cả khách hàng thương mại điện tử (ước tính là khoảng 2,3 tỷ người tại Hoa Kỳ). Tiềm năng, cần 2,3 tỷ khóa khác nhau. Rõ ràng tình huống này sẽ quá không thuận tiện để hoạt động trong thực tế.

Hệ thống mã hóa hiện đại là số học. Các mật mã hoặc khóa được sử dụng để biến đổi văn bản gốc thành văn bản đã mã hóa là chuỗi số học. Máy tính lưu trữ văn bản hoặc dữ liệu khác dưới dạng chuỗi nhị phân gồm 0 và 1. Ví dụ, biểu diễn nhị phân của chữ cái "A" trong mã máy tính ASCII được thực hiện bằng tám chữ số nhị phân (bit): 01000001. Một cách để chuyển đổi chuỗi số học thành văn bản đã mã hóa là nhân mỗi ký tự số học trong tin nhắn của chúng ta bằng một số nhị phân khác, ví dụ, một số khóa tám bit 0101 0101. Nếu chúng ta nhân mọi ký tự số học trong tin nhắn của chúng ta bằng số khóa tám bit này và gửi thông điệp đã mã hóa cho một người bạn cùng với khóa bí mật tám bit, người bạn có thể giải mã thông điệp dễ dàng.

***Sức mạnh của bảo vệ an ninh hiện đại được đo bằng độ dài của khóa nhị phân được sử dụng, và việc sử dụng khóa dài hơn làm cho việc tấn công bằng phương pháp "brute force" trở nên khó khăn đối với kẻ xâm nhập, và có thể đòi hỏi hàng thập kỷ của các máy tính làm việc để tìm ra khóa đúng.***

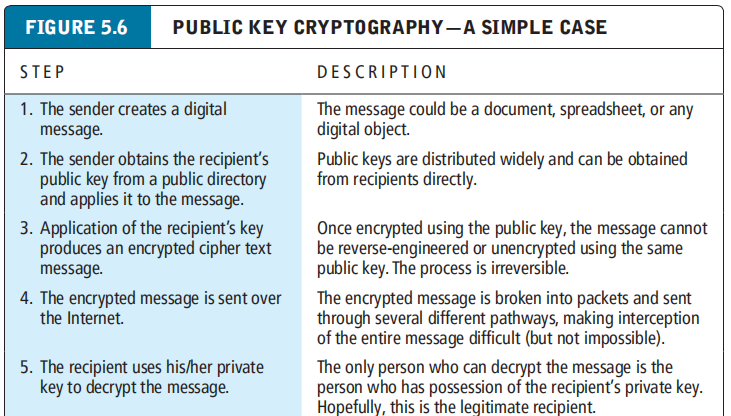
***Data Encryption Standard (DES)(Tiêu chuẩn Mã hóa Dữ liệu) đã được phát triển bởi Cơ quan An ninh Quốc gia (NSA) và IBM vào những năm 1950. DES sử dụng một khóa mã hóa 56 bit****. Để đối phó với máy tính nhanh hơn nhiều, nó đã được cải tiến bằng Thuật toán Mã hóa Triple DES (TDEA), bản chất là mã hóa thông điệp ba lần, mỗi lần với một khóa riêng biệt. Ngày nay,* ***thuật toán khóa đối xứng phổ biến nhất là Advanced Encryption Standard (AES) (Tiêu chuẩn Mã hóa Nâng cao (AES)), cung cấp kích thước khóa 128, 192 và 256 bit****. AES đã được xem là tương đối an toàn, nhưng vào năm 2011, các nhà nghiên cứu từ Microsoft và một đại học ở Bỉ đã công bố rằng họ đã tìm ra cách để phá vỡ thuật toán, và với công việc này, "khoảng cách an toàn" của AES tiếp tục giảm đi.* ***Còn nhiều hệ thống khóa đối xứng khác hiện đang ít được sử dụng rộng rãi, với các khóa lên đến 2.048 bit.***

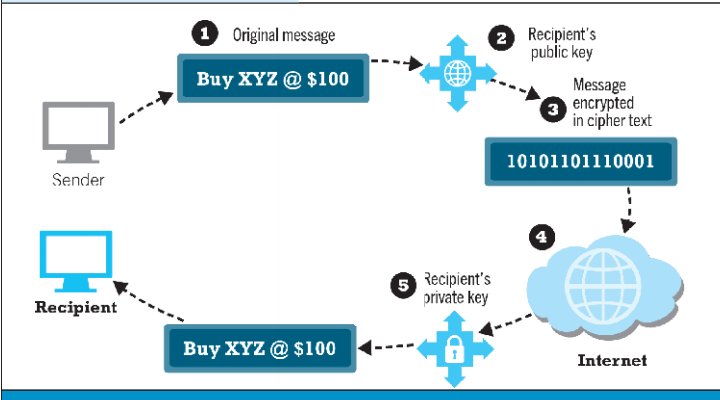
2.2 Public Key Cryptography

***Trong mật mã khóa công khai, hai khóa số học có mối quan hệ toán học với nhau được sử dụng: một khóa công khai và một khóa riêng tư. Khóa riêng tư được giữ bí mật bởi chủ sở hữu, trong khi khóa công khai được phổ biến rộng rãi. Cả hai khóa có thể được sử dụng để mã hóa và giải mã một thông điệp. Tuy nhiên, sau khi các khóa được sử dụng để mã hóa một thông điệp, thì cùng một khóa đó không thể được sử dụng để giải mã thông điệp đó. Người gửi sử dụng khóa chung của người nhận để mã hóa 1 thông điệp và người nhận sẽ sử dụng khóa riêng để giải mã nó***

2.3 Public Key Cryptography Using Digital Signatures and Hash Digests (Mật mã khóa công khai sử dụng chữ ký số và thông báo băm)

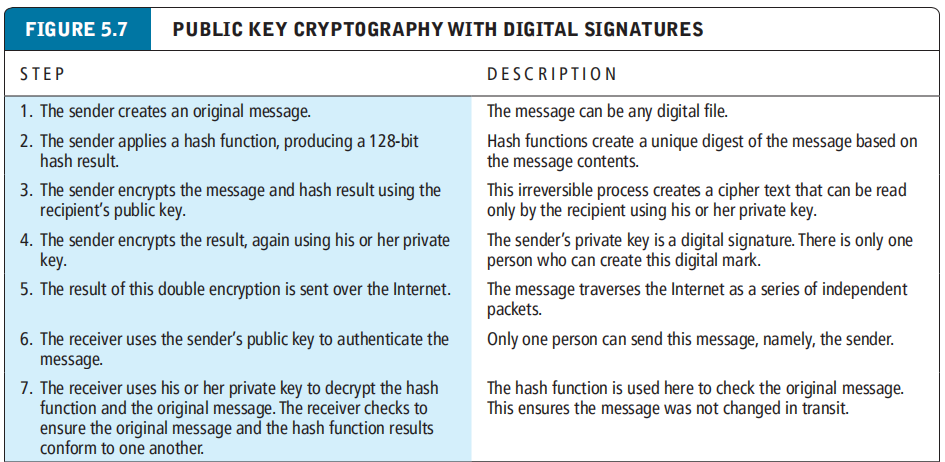
*Trong mật mã khóa công khai, mặc dù chúng ta có đảm bảo tính bảo mật của thông điệp, tức là thông điệp không bị đọc bởi bên thứ ba, nhưng vẫn có những khía cạnh bảo mật khác chưa được đảm bảo*. Đầu tiên, không có sự xác thực đối với người gửi, người gửi có thể phủ nhận việc gửi thông điệp. Thứ hai, không có đảm bảo về tính toàn vẹn của thông điệp, có nguy cơ thông điệp bị thay đổi trong quá trình truyền tải, gây ra sự thiếu tin cậy trong hệ thống.

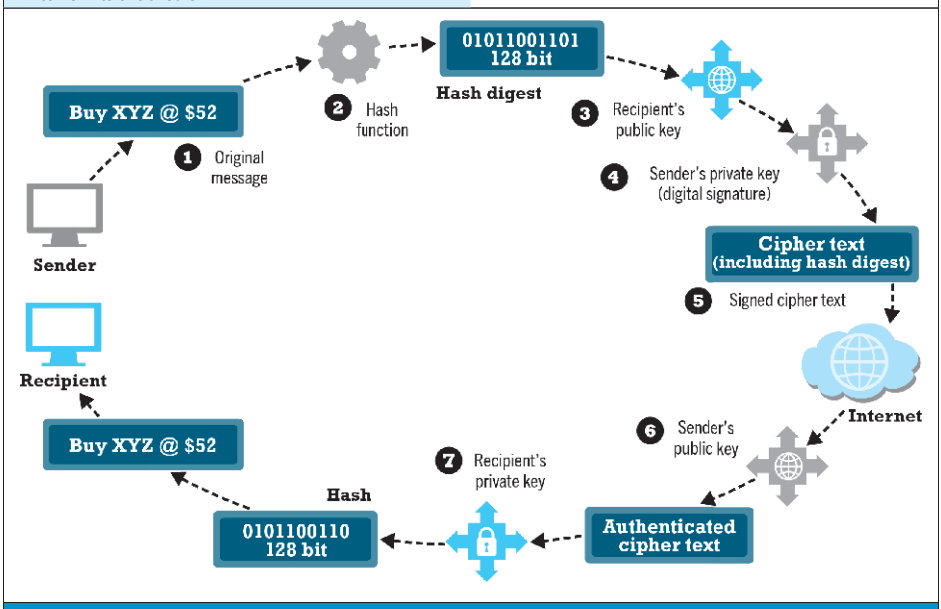




***Trong cách sử dụng đơn giản nhất của mật mã khóa công khai, người gửi mã hóa tin nhắn bằng cách sử dụng khóa công khai của người nhận, sau đó gửi nó qua Internet. Người duy nhất có thể giải mã tin nhắn này là người nhận, sử dụng khóa riêng của mình. Tuy nhiên, trường hợp đơn giản này không đảm bảo tính toàn vẹn hoặc thông điệp xác thực.***

*Để kiểm tra tính toàn vẹn của một thông điệp và đảm bảo rằng nó không bị thay đổi trong quá trình truyền tải, một hàm băm được sử dụng trước để tạo ra một bản tóm tắt của thông điệp.* ***Hash funtion*** *(****Hàm băm) là một thuật toán tạo ra một số có độ dài cố định gọi là băm hoặc bản tóm tắt của thông điệp****. Một hàm băm có thể đơn giản, đếm số chữ số 1 trong một thông điệp, hoặc có thể phức tạp hơn, tạo ra một số 128 bit hoặc 160 bit phản ánh số lượng chữ số 0 và 1, số lượng 00 và 11, và cách thức khác*. Có sẵn các hàm băm tiêu chuẩn (MD4 và MD5 tạo ra băm 128 và 160 bit) (Stein, 1998). Các hàm băm phức tạp này tạo ra các băm hoặc kết quả băm duy nhất cho mỗi thông điệp.





*Việc sử dụng mật mã khóa công khai thực tế hơn sử dụng hàm băm và chữ ký số để vừa đảm bảo tính bảo mật của tin nhắn vừa xác thực người gửi. Người duy nhất có thể gửi tin nhắn này là chủ sở hữu hoặc người gửi sử dụng khóa riêng của họ. Điều này xác thực tin nhắn. Hàm băm đảm bảo tin nhắn không bị thay đổi trong quá trình truyền. Như trước đây, người duy nhất có thể giải mã được tin nhắn là người nhận bằng cách sử dụng khóa riêng của họ.*

*Cần thêm một bước nữa. Để đảm bảo tính xác thực của tin nhắn và đảm bảo tính không chối bỏ, người gửi mã hóa toàn bộ khối văn bản mật mã một lần nữa bằng khóa riêng của người gửi. Điều này tạo ra* ***digital signature (e-signature) (chữ ký số (còn gọi là chữ ký điện tử)) hoặc văn bản mật mã “có chữ ký” có thể được gửi qua Internet.***

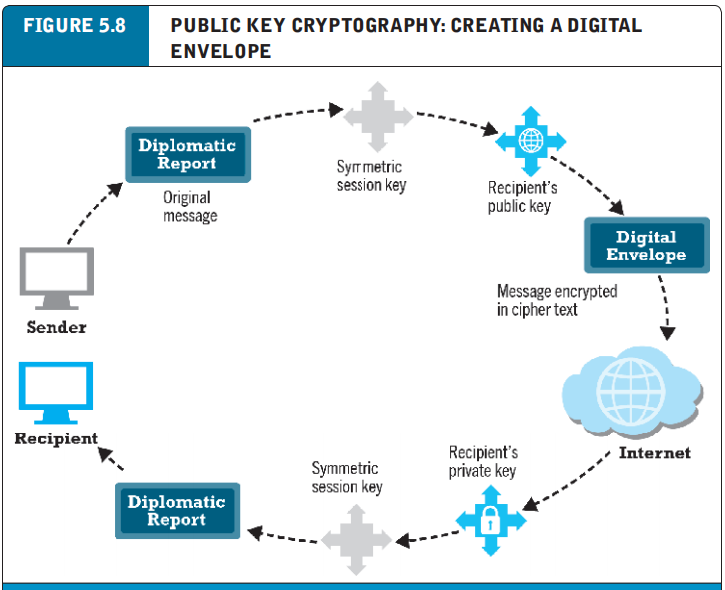
*Chữ ký số tương đương với chữ ký bằng tay và duy nhất, chỉ người sở hữu khóa riêng tư mới có thể tạo ra nó. Khi được sử dụng với một hàm băm, chữ ký số trở nên độc đáo hơn cả chữ ký bằng tay. Nó không chỉ độc quyền cho cá nhân cụ thể, mà còn độc quyền cho từng tài liệu và thay đổi cho mỗi tài liệu.*

Người nhận thông điệp đã ký đầu tiên sử dụng khóa công khai của người gửi để xác thực thông điệp. Sau khi xác thực, người nhận sử dụng khóa riêng tư của họ để lấy kết quả băm và thông điệp gốc. Sau đó, người nhận so sánh kết quả của việc áp dụng cùng một hàm băm vào thông điệp gốc với kết quả đã gửi bởi người gửi. Nếu kết quả giống nhau, người nhận biết rằng thông điệp không bị thay đổi trong quá trình truyền tải, đảm bảo tính toàn vẹn của thông điệp.

2.4 Digital Envelopes

*Mật mã khóa công khai yêu cầu tính toán chậm. Nếu sử dụng khóa 128 hoặc 256 bit để* ***mã hóa các tài liệu lớn*** *như chương này hoặc cả cuốn sách, tốc độ truyền tải sẽ giảm đáng kể và thời gian xử lý sẽ tăng lên. Mật mã khóa đối xứng tính toán nhanh hơn, nhưng như đã trình bày trước đó, nó có một điểm yếu, đó là khóa đối xứng phải được gửi đến người nhận qua đường truyền không an toàn.* ***Một giải pháp là sử dụng mật mã đối xứng hiệu quả hơn để mã hóa và gửi khóa đối xứng cho người nhận bằng mật mã khóa* *công khai. Kỹ thuật này được gọi là sử dụng một "phong bì số học" (digital envelope).***

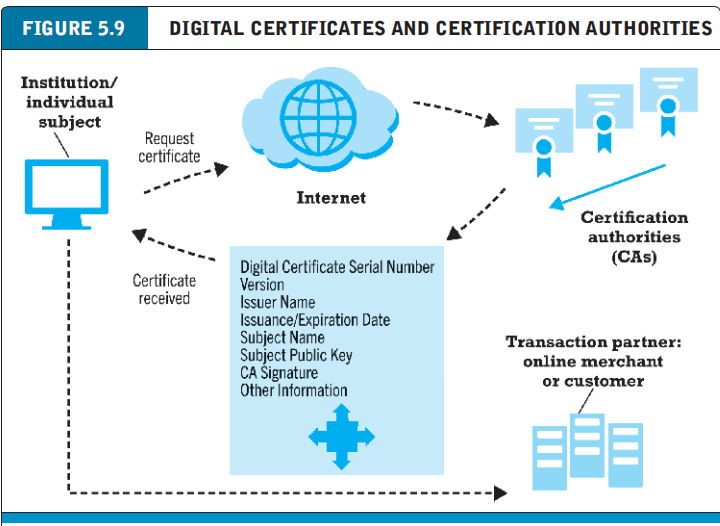
*Trong hình 5.8, một tài liệu ngoại giao được mã hóa bằng một khóa đối xứng. Khóa đối xứng - mà người nhận sẽ cần để giải mã tài liệu - cũng được mã hóa, bằng cách sử dụng khóa công khai của người nhận. Vì vậy, chúng ta có một "khóa trong khóa" (một phong bì số học). Tài liệu đã mã hóa và phong bì số học được gửi qua Internet. Người nhận đầu tiên sử dụng khóa riêng tư của họ để giải mã khóa đối xứng, sau đó người nhận sử dụng khóa đối xứng để giải mã tài liệu. Phương pháp này tiết kiệm thời gian vì cả mã hóa và giải mã đều nhanh hơn với khóa đối xứng.*



Một phong bì kỹ thuật số có thể được tạo ra để truyền một khóa đối xứng cho phép người nhận giải mã tin nhắn và đảm bảo rằng tin nhắn không bị chặn trong quá trình truyền.

2.5 Digital Certificates and Public Key Infrastructure (PKI)

*Chứng chỉ số học và cơ sở hạ tầng khóa công khai hỗ trợ cố gắng giải quyết vấn đề về danh tính số học.* ***Một chứng chỉ số học digital certificate là một tài liệu số học được cấp bởi một tổ chức bên ngoài tin cậy được gọi là một cơ quan chứng nhận certification authority (CA) chứa tên của chủ thể hoặc công ty, khóa công khai của chủ thể, số serial của chứng chỉ số học, ngày hết hạn, ngày cấp, chữ ký số học của cơ quan chứng nhận*** *(tên của CA được mã hóa bằng khóa riêng tư của CA)*, và thông tin nhận biết khác (xem Hình 5.9).



PKI bao gồm các cơ quan chứng nhận cấp, xác minh và bảo đảm chứng chỉ kỹ thuật số được sử dụng trong thương mại điện tử để đảm bảo danh tính của các đối tác giao dịch.

Trên khắp thế giới, hàng nghìn tổ chức cấp giấy chứng nhận (CAs). GlobalSign là cơ quan chứng nhận đầu tiên được tạo ra tại châu Âu. Các quốc gia thành viên của EU và các quốc gia châu Âu khác duy trì danh sách các CAs được phê duyệt. Một cấu trúc phân cấp của các CAs đã xuất hiện, trong đó các CAs ít nổi tiếng hơn được chứng nhận bởi các CAs lớn và nổi tiếng hơn, tạo ra một cộng đồng của các tổ chức xác minh lẫn nhau. ***Cơ sở hạ tầng khóa công khai public key infrastructure (PKI) đề cập đến các CAs và các thủ tục chứng chỉ số học được chấp nhận bởi tất cả các bên****. Khi bạn đăng nhập vào một trang web "an toàn", URL sẽ bắt đầu bằng "https" và biểu tượng ổ khóa sẽ xuất hiện trên trình duyệt của bạn. Điều này có nghĩa là trang web này có một chứng chỉ số học được cấp bởi một CA tin cậy. Điều này ngụ ý rằng trang web không phải là một trang web giả mạo.*

Cơ sở hạ tầng khóa công khai (PKI) và CAs cũng có thể được sử dụng để bảo mật mã nguồn và nội dung cho các ứng dụng được tải trực tiếp xuống thiết bị di động từ Internet. Bằng cách sử dụng một kỹ thuật được gọi là ký mã, các nhà phát triển ứng dụng di động sử dụng khóa riêng của họ để mã hóa một chữ ký số học. Khi người dùng cuối giải mã chữ ký với khóa công khai tương ứng, điều này xác nhận danh tính của nhà phát triển và tính toàn vẹn của mã nguồn.

***Pretty Good Privacy (PGP), một công cụ phần mềm mã hóa email dựa trên khóa công khai,*** *đã được phát minh vào năm 1991 bởi Phil Zimmerman.* ***OpenPGP là một giao thức không thuộc sở hữu dựa trên PGP****, đã trở thành tiêu chuẩn cho hầu hết các email được mã hóa trên toàn cầu trong thập kỷ qua. Bằng cách sử dụng phần mềm PGP trên máy tính của bạn, bạn có thể nén và mã hóa các thông điệp cũng như xác thực cả bạn và người nhận*. Signal, một ứng dụng nhắn tin mã nguồn mở và miễn phí, mã hóa các tin nhắn văn bản và đa phương tiện. Cũng có nhiều tiện ích mở rộng hoặc plugin dành cho Firefox, Chrome, Internet Explorer và Safari cho phép bạn mã hóa email của bạn. Hiện nay, cả máy tính và thiết bị di động đều có phần mềm mã hóa tích hợp, chẳng hạn như BitLocker của Windows, có thể được bật và cũng có nhiều ứng dụng mã hóa bên thứ ba, như VeraCrypt.

*Hình 5.9: Khi máy chủ gửi một yêu cầu chứng chỉ đến CA, thì CA gửi chứng chỉ ký số về máy chủ. Máy chủ sau đó sử dụng chứng chỉ này để xác minh danh tính của mình trong quá trình giao tiếp mật mã và xác thực với các máy chủ hoặc máy tính khác trong một hệ thống mạng.*

* Limitations of KPI

*PKI là một giải pháp công nghệ mạnh mẽ cho các vấn đề bảo mật, nhưng nó có nhiều hạn chế, đặc biệt liên quan đến CAs, và không hiệu quả trong việc bảo vệ thông tin khách hàng trong các hệ thống công ty hoặc trang web thương mại điện tử.*

*Trong một ví dụ, Trung tâm Thông tin Quốc gia của Ấn Độ, một CA trung gian được tin tưởng bởi Cơ quan Chứng nhận Cơ bản Ấn Độ, chứng chỉ của họ được bao gồm trong Microsoft Root Store và do đó được tin tưởng bởi hầu hết các chương trình chạy trên Windows, bao gồm Internet Explorer và Chrome, đã bị tấn công và một số chứng chỉ số học không được ủy quyền đã được cấp cho các tên miền do Google và Yahoo điều hành. Cuối cùng, chính sách về việc thu hồi hoặc gia hạn chứng chỉ như thế nào? Tuổi thọ dự kiến của chứng chỉ số học hoặc khóa riêng tư là một hàm số của tần suất sử dụng và tính dễ bị tổn thương của hệ thống sử dụng chứng chỉ. Tuy nhiên, hầu hết các CAs không có chính sách hoặc chỉ có một chính sách hàng năm để cấp lại chứng chỉ. Nếu Microsoft, Apple hoặc Cisco thu hồi một số CAs, hàng triệu người dùng sẽ không thể truy cập trang web. Hệ thống CA rất khó và tốn kém để kiểm soát.*

*Tóm lại, PKI có nhiều hạn chế, đặc biệt liên quan đến việc bảo vệ danh tính trực tuyến và tính bảo mật của các hệ thống CA.*

1. **SECURING CHANNELS OF COMMUNICATION (Bảo mật kênh truyền thông)**

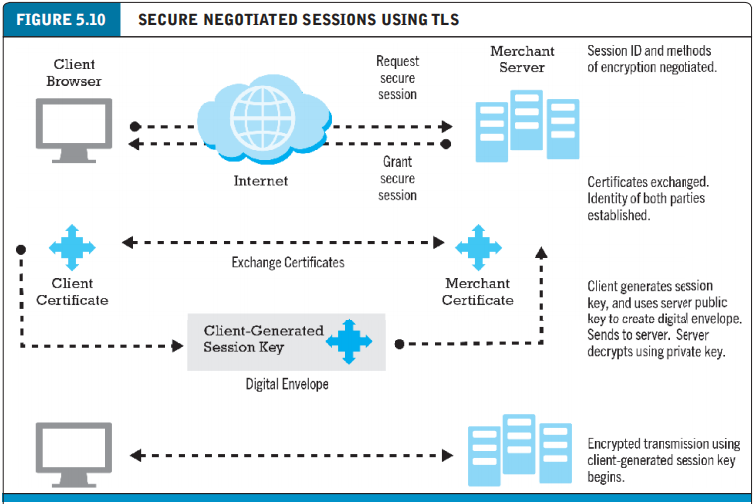
*Các khái niệm về mật mã khóa công khai được sử dụng thường xuyên để bảo mật các kênh của giao tiếp.*

*3.1 Secure Sockets Layer (SSL), Transport Layer Security (TLS) and HTTPS*

***Giao thức Secure Sockets Layer (SSL) ban đầu cho phép giao tiếp an toàn trên Internet****. Tuy nhiên, ngày nay,* ***nó đã được thay thế bằng giao thức Transport Layer Security (TLS), là một phiên bản cập nhật và an toàn hơn của SSL****. Khi bạn nhận một thông báo từ máy chủ trên Web mà bạn sẽ giao tiếp thông qua một kênh an toàn, điều này có nghĩa là bạn sẽ sử dụng TLS để thiết lập một phiên đàm phán an toàn. (Lưu ý rằng URL thay đổi từ HTTP thành HTTPS.)* ***Một phiên đàm phán an toàn secure negotiated session là một phiên làm việc giữa máy khách và máy chủ trong đó URL của tài liệu được yêu cầu, cùng với nội dung, nội dung của biểu mẫu và các cookie trao đổi, đều được mã hóa*** (xem Hình 5.10). Ví dụ, số thẻ tín dụng mà bạn nhập vào một biểu mẫu sẽ được mã hóa. Qua một loạt các bước bắt tay và truyền thông, trình duyệt và máy chủ xác định danh tính của nhau bằng cách trao đổi chứng chỉ số học, quyết định về một dạng mã hóa chung mạnh nhất được chia sẻ và sau đó tiến hành truyền thông bằng cách sử dụng một khóa phiên được đồng ý. **Khóa phiên session key là một khóa mã hóa đối xứng duy nhất được chọn chỉ dành cho phiên an toàn duy nhất này**. Một khi đã sử dụng, nó sẽ biến mất mãi mãi. Hình 5.10 thể hiện cách thức hoạt động của nó.

TLS cung cấp mã hóa dữ liệu, xác thực máy chủ, xác thực tùy chọn của khách hàng và tính toàn vẹn của thông điệp cho các kết nối TCP/IP. TLS giải quyết vấn đề về tính xác thực bằng cách cho phép người dùng xác minh danh tính của người dùng khác hoặc danh tính của máy chủ. Nó cũng bảo vệ tính toàn vẹn của các thông điệp trao đổi. *Mặc dù TLS* ***cung cấp các giao dịch an toàn giữa người bán và người tiêu dùng, nó chỉ đảm bảo xác thực phía máy chủ. Xác thực của khách hàng là tùy chọn****. Ngoài ra,* ***TLS không thể cung cấp tính không thể chối bỏ trong giao dịch***- người tiêu dùng có thể đặt hàng sản phẩm hoặc tải xuống thông tin và sau đó tuyên bố rằng giao dịch không bao giờ xảy ra.

Phiên bản TLS mới nhất là phiên bản 1.3, được phát hành vào năm 2018. Vào tháng 3 năm 2020, hầu hết các trình duyệt lớn sẽ loại bỏ sự hỗ trợ cho các phiên bản TLS 1.0 và TLS 1.1 cũ hơn.



*Chứng chỉ đóng vai trò quan trọng trong việc sử dụng TLS để thiết lập kênh liên lạc an toàn.*

***TLS được sử dụng kết hợp với HTTPS, một phiên bản an toàn của giao thức HTTP sử dụng TLS để mã hóa và xác thực****.* Nó được triển khai bởi một máy chủ thực hiện tính năng HTTP Strict Transport Security (HSTS), đóng vai trò đưa ra yêu cầu cho trình duyệt chỉ truy cập máy chủ bằng cách sử dụng HTTPS. ***Hiện nay, khoảng 60% các trang web đã sử dụng HTTPS như giao thức mặc định của họ (W3techs.com, 2020).***

3.2 Virtual Private Networks (VPNs)

***Mạng riêng ảo Virtual Private Networks (VPNs) cho phép người dùng từ xa truy cập an toàn vào mạng khu vực cục bộ của một tập đoàn thông qua Internet, sử dụng một loạt các giao thức VPN****. VPN* ***sử dụng cả xác thực và mã hóa để bảo vệ thông tin*** *khỏi những người không được ủy quyền (****đảm bảo tính bảo mật và tính toàn vẹn****)*. *Xác thực ngăn chặn việc giả mạo và biểu hiện sai về danh tính. Một người dùng từ xa có thể kết nối với mạng cục bộ riêng từ xa bằng cách sử dụng một nhà cung cấp dịch vụ Internet (ISP) địa phương*. Các giao thức VPN sẽ thiết lập liên kết từ máy khách đến mạng doanh nghiệp như là người dùng đã quay số trực tiếp vào mạng doanh nghiệp. **Quá trình kết nối một giao thức thông qua một giao thức khác (IP) được gọi là đào đường (tunneling)**, vì VPN tạo ra một kết nối riêng tư bằng cách thêm một lớp bọc vô hình xung quanh một thông điệp để che giấu nội dung của nó. Khi thông điệp di chuyển qua Internet giữa ISP và mạng doanh nghiệp, nó được bảo vệ khỏi sự quan sát bằng một lớp bọc được mã hóa.

VPN là một kết nối an toàn tạm thời, xuất hiện trước người dùng như một đường truyền an toàn dành riêng và chủ yếu được sử dụng để **thiết lập giao tiếp an toàn** giữa các đối tác kinh doanh và nhân viên **làm việc từ xa, giúp giảm chi phí đáng kể**.

***Việc sử dụng VPN tăng mạnh vào đầu năm 2020 do sự tăng đột ngột về số lượng người làm việc từ xa do đại dịch Covid-19 (Steele, 2020).***

3.3 Wireless (Wi-Fi) Networks

Truy cập Internet thông qua mạng không dây (Wi-Fi) có những vấn đề bảo mật riêng. Ban đầu, mạng Wi-Fi sử dụng một tiêu chuẩn bảo mật gọi là Wired Equivalent Privacy (WEP) để mã hóa thông tin. Tuy nhiên, WEP rất yếu và dễ dàng bị hacker xâm nhập. Một tiêu chuẩn thay thế, Wi-Fi Protected Access (WPA), đã được phát triển để cung cấp một mức bảo vệ cao hơn, nhưng cũng sớm trở nên dễ bị xâm nhập. **WPA2, được giới thiệu vào năm 2004, sử dụng thuật toán AES cho mã hóa và CCMP, một giao thức mã xác thực tiên tiến hơn**. Năm 2018, Wi-Fi Alliance, tổ chức thương mại giám sát giao thức WPA, đã công bố thế hệ tiếp theo của giao thức, **WPA3 - một phiên bản tiến hóa của giao thức WPA , mà thực hiện một giao thức trao đổi khóa mạnh mẽ hơn và một cách an toàn hơn để kết nối các thiết bị IoT. Nó cũng bao gồm mã hóa mở rộng cho các mạng công cộng**. Tuy nhiên, thậm chí tiêu chuẩn WPA3 cập nhật cũng vẫn có những điểm yếu có thể cho phép kẻ tấn công khôi phục lại mật khẩu (Kan, 2019; Barrett, 2018).

1. **PROTECTING NETWORKS**

4.1 Firewalls

*Tường lửa và máy chủ proxy nhằm mục đích xây dựng một bức tường xung quanh mạng của bạn cũng như các máy chủ và máy khách đính kèm. Tường lửa và máy chủ proxy có chung một số chức năng nhưng chúng khá khác nhau.*

***Một tường lửa (firewall) đề cập đến cả phần cứng lẫn phần mềm được sử dụng để lọc các gói tin truyền thông và ngăn một số gói tin từ việc vào hoặc ra khỏi mạng dựa trên một chính sách bảo mật****. Tường lửa kiểm soát lưu lượng truy cập và ra khỏi máy chủ và máy khách, từ chối các kết nối từ nguồn không đáng tin cậy và cho phép các kết nối khác từ nguồn tin cậy tiến hành. Mọi thông điệp sẽ được xử lý bởi tường lửa trước khi được gửi hoặc nhận từ mạng, và tường lửa quyết định xem thông điệp có tuân theo các hướng dẫn bảo mật được thiết lập hay không.* Nếu có, thông điệp được phép được phân phối, và nếu không, thông điệp sẽ bị chặn. Tường lửa có thể lọc lưu lượng dựa trên các đặc điểm gói tin như địa chỉ IP nguồn, cổng hoặc địa chỉ IP đích, loại dịch vụ (như WWW hoặc HTTP), tên miền nguồn và nhiều chiều khác. *Một cài đặt mặc định phổ biến trên các tường lửa phần cứng (router DSL và cáp mạng) đơn giản là bỏ qua các giao tiếp với cổng TCP 445, cổng thường bị tấn công nhiều nhất.* Việc sử dụng ngày càng nhiều tường lửa bởi người dùng Internet gia đình và doanh nghiệp đã làm giảm đáng kể hiệu quả của các cuộc tấn công và buộc hacker phải tập trung hơn vào việc phân phối sâu hơn qua email để phát tán các loại virus.

***Có hai phương pháp chính mà tường lửa sử dụng để xác thực lưu lượng: bộ lọc gói tin và cổng ứng dụng****. Bộ lọc gói tin kiểm tra các gói dữ liệu để xác định xem chúng có đến một cổng bị cấm hoặc xuất phát từ địa chỉ IP bị cấm (như được chỉ định bởi quản trị bảo mật). Bộ lọc cụ thể kiểm tra thông tin nguồn và đích, cũng như cổng và loại gói tin khi xác định xem thông tin có thể được truyền đi hay không.*

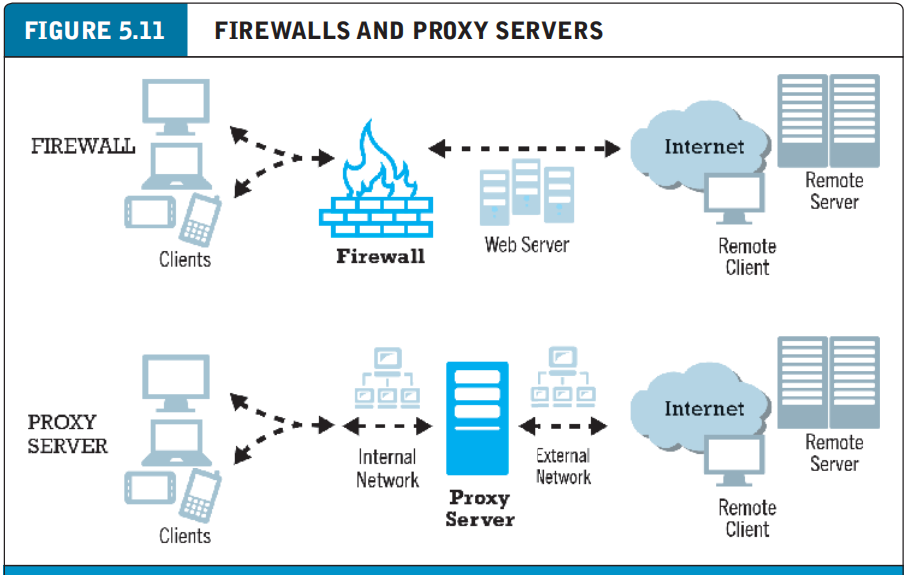
Cổng ứng dụng là một loại tường lửa mà lọc thông tin dựa trên ứng dụng được yêu cầu, chứ không phải là nguồn hoặc đích của thông tin.

Tường lửa thế hệ tiếp theo sử dụng một cách tiếp cận tập trung vào ứng dụng trong việc kiểm soát tường lửa.

4.2 Proxy Servers

***Máy chủ proxy (proxies) là các máy chủ phần mềm (thường là một máy tính được dành riêng) xử lý tất cả các giao tiếp bắt nguồn từ hoặc được gửi đến Internet bởi các máy khách trong mạng cục bộ, đóng vai trò như một người phát ngôn hoặc bảo vệ cho tổ chức.*** *Máy chủ proxy hoạt động chủ yếu để giới hạn quyền truy cập của các máy khách nội bộ vào các máy chủ Internet bên ngoài, mặc dù một số máy chủ proxy cũng hoạt động như tường lửa. Máy chủ proxy đôi khi được gọi là hệ thống hai mạng vì chúng có hai giao diện mạng. Đối với máy tính nội bộ, máy chủ proxy được biết đến như là cổng ra ngoài, trong khi đối với máy tính bên ngoài, nó được biết đến như là máy chủ thư hoặc địa chỉ số.*

*Khi một người dùng trên mạng nội bộ yêu cầu một trang web, yêu cầu được định tuyến trước tiên đến máy chủ proxy. Máy chủ proxy xác thực người dùng và tính chất của yêu cầu, sau đó gửi yêu cầu ra Internet. Một trang web được gửi bởi máy chủ Internet bên ngoài đầu tiên đi qua máy chủ proxy. Nếu được chấp nhận, trang web sẽ đi tiếp đến máy chủ web trong mạng nội bộ và sau đó đến máy tính máy khách.* Bằng cách ngăn người dùng giao tiếp trực tiếp với Internet, các công ty có thể hạn chế quyền truy cập vào một số loại trang web, chẳng hạn như trang web khiêu dâm, trang đấu giá hoặc giao dịch cổ phiếu. Máy chủ proxy cũng cải thiện hiệu suất web bằng cách lưu trữ các trang web được yêu cầu thường xuyên một cách cục bộ, giảm thời gian tải lên và ẩn địa chỉ mạng nội bộ, làm cho việc theo dõi của các hacker trở nên khó khăn hơn. Hình 5.11 mô tả cách tường lửa và máy chủ proxy bảo vệ mạng cục bộ khỏi người xâm nhập từ Internet và ngăn người dùng nội bộ tiếp cận các máy chủ web bị cấm.



*Chức năng chính của tường lửa là từ chối quyền truy cập của máy khách từ xa vào máy tính cục bộ. Mục đích chính của máy chủ proxy là cung cấp quyền truy cập có kiểm soát từ máy tính cục bộ đến máy tính từ xa.*

4.3 Intrusion Detection and Prevention Systems

Ngoài tường lửa và máy chủ proxy, một hệ thống phát hiện và/hoặc ngăn chặn xâm nhập có thể được cài đặt. **Hệ thống phát hiện xâm nhập intrusion detection system (IDS) xem xét lưu lượng mạng, theo dõi xem liệu nó khớp với một số mẫu hoặc quy tắc được cấu hình trước chỉ ra một cuộc tấn công**. Nếu nó phát hiện hoạt động đáng ngờ, IDS sẽ kích hoạt một cảnh báo để thông báo cho các quản trị viên và ghi lại sự kiện trong cơ sở dữ liệu. IDS hữu ích để phát hiện hoạt động độc hại mà tường lửa có thể bỏ lỡ. **Hệ thống ngăn chặn xâm nhập intrusion prevention system (IPS) có tất cả các chức năng của một IDS, với khả năng bổ sung để thực hiện các biện pháp để ngăn chặn và chặn hoạt động đáng ng**ờ. Ví dụ, IPS có thể chấm dứt một phiên và thiết lập lại kết nối, chặn lưu lượng từ một địa chỉ IP đáng ngờ, hoặc cấu hình lại tường lửa hoặc kiểm soát bảo mật bộ định tuyến.

1. **PROTECTING SERVERS AND CLIENTS**

*Các tính năng của hệ điều hành và phần mềm chống vi-rút có thể giúp bảo vệ hơn nữa máy chủ và máy khách khỏi một số kiểu tấn công nhất định.*

*5.1 Operating System and Application Software Security Enhancements ̣̣(Cải tiến bảo mật phần mềm ứng dụng và hệ điều hành)*

*Để bảo vệ máy chủ và máy khách là tận dụng các bản vá bảo mật tự động. Hệ điều hành của Microsoft, Apple và Linux/Unix luôn được cập nhật liên tục để vá các lỗ hổng được phát hiện bởi các hacker. Các bản vá này hoạt động tự động; nghĩa là khi sử dụng các hệ điều hành này trên Internet, bạn sẽ nhận được thông báo và thông tin rằng các cải tiến cho hệ điều hành có sẵn.*

*Trong năm 2014, Microsoft đã chấm dứt việc hỗ trợ bảo mật và cập nhật cho hệ điều hành Windows XP. Tuy nhiên, nhiều tổ chức tiếp tục sử dụng các hệ thống dựa trên XP, vào năm 2017, sau một đợt bùng phát lớn về ransomware WannaCry sử dụng các lỗ hổng của Windows XP, Microsoft đã đưa ra một biện pháp chưa từng có bằng cách phát hành thêm các bản vá bảo mật cho Windows XP để ngăn chặn các đợt bùng phát tiếp theo.*  
 Những lỗ hổng ứng dụng cũng được sửa chữa bằng cách tương tự. Trong những năm gần đây, những gì được gọi là **cuộc tấn công chuỗi cung ứng phần mềm software supply chain attack, trong đó các hacker tấn công môi trường phát triển để nhiễm phần mềm sau đó được tải xuống bởi người dùng cuối**, đã tăng cường tần suất. Ví dụ, vào năm 2019, các hacker đã xâm nhập vào máy chủ được sử dụng bởi Asus để cung cấp các bản cập nhật hệ điều hành và bảo mật và có thể cài đặt phần mềm độc hại ShadowHammer trên khoảng 1 triệu máy tính Asus.

5.2 Anti-Virus Software

***Cách đơn giản và chi phí thấp nhất để ngăn chặn các mối đe dọa đối với tính toàn vẹn của hệ thống là cài đặt phần mềm diệt virus****. Các chương trình từ Malwarebytes, McAfee, Symantec (Norton AntiVirus) và nhiều công ty khác cung cấp các công cụ giá rẻ để* ***xác định và tiêu diệt các loại mã độc hại phổ biến khi chúng xâm nhập vào máy tính, cũng như tiêu diệt những mã độc hại đã tồn tại trên ổ cứng****. Các chương trình diệt virus có thể được thiết lập để kiểm tra các tệp đính kèm trong email trước khi bạn nhấp vào chúng, và các tệp đính kèm sẽ bị loại bỏ nếu chúng chứa mã độc hại hoặc sâu mà đã được biết đến. Tuy nhiên, việc chỉ cài đặt phần mềm một lần không đủ. Vì mỗi ngày có các loại virus mới được phát triển và phát hành, việc cập nhật hàng ngày là cần thiết để ngăn chặn các mối đe dọa mới được tải lên. Một số phần mềm diệt virus cấp cao còn được cập nhật hàng giờ.*

Có sẵn các gói phần mềm diệt virus và các chương trình đứng riêng lẻ để loại bỏ các mối xâm nhập như các chương trình bot, adware và các mối đe dọa bảo mật khác. Các chương trình này hoạt động tương tự như phần mềm diệt virus bằng cách tìm kiếm các công cụ hacker đã được công nhận hoặc hành động chữ ký của các xâm nhập đã biết đến.

1. **MANAGEMENT POLICIES, BUSINESS PROCEDURES, AND PUBLIC LAWS** (trang 339 - trang 347) CHÍNH SÁCH QUẢN LÝ, THỦ TỤC KINH DOANH VÀ LUẬT CÔNG
2. **A SECURITY PLAN: MANAGEMENT POLICIES**

**KẾ HOẠCH AN NINH: CHÍNH SÁCH QUẢN LÝ**

* Đánh giá rủi ro: Xác định các rủi ro và điểm dễ bị tấn công.

Đầu tiên chúng ta phải xác định các thông tin tài sản cần bảo vệ bằng cách là kiểm tra thông tin và lượt truy cập của trang web thương mại điện tử và công ty. Thông tin nào có nguy cơ bị đánh cấp? Đó có phải là thông tin khách hàng, thiết kế độc quyền, hoạt động kinh doanh, quy trình bí mật hoặc thông tin nội bộ khác, chẳng hạn như bảng giá, lương thưởng cho giám đốc điều hành hoặc bảng lương? Đối với mỗi loại tài sản thông tin, hãy cố gắng ước tính giá trị đồng đô la đối với công ty nếu thông tin này bị xâm phạm, sau đó nhân số tiền đó với xác suất xảy ra tổn thất. Một khi bạn đã làm như vậy, hãy xếp hạng các kết quả. Bây giờ bạn có một danh sách các tài sản thông tin được ưu tiên theo giá trị của chúng đối với công ty

|  |
| --- |
| * Các thông tin tài sản cần bảo vệ. * Giá trị của các thông tin tài sản này đối với công ty. * Xác suất xảy ra rủi ro. * Mức độ rủi ro chấp nhận được. |

* Phát triển chính sách bảo mật

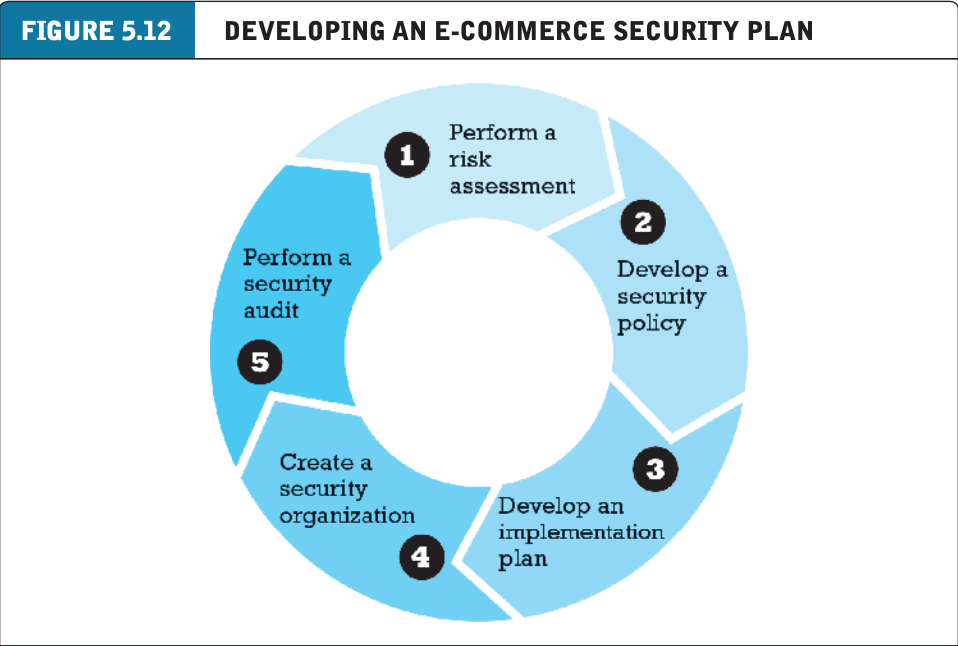
|  |
| --- |
| * Dựa trên danh sách rủi ro đã được lượng hóa, bạn có thể bắt đầu phát triển chính sách bảo mật. * Chính sách bảo mật là một tập hợp các tuyên bố ưu tiên các rủi ro về thông tin, xác định các mục tiêu rủi ro có thể chấp nhận được và xác định các cơ chế để đạt được các mục tiêu này. * Để phát triển chính sách bảo mật, bạn cần xem xét các yếu tố sau:   + Nội dung thông tin có sự ưu tiên cao nhất trong đánh giá rủi ro.   + Ai tạo ra và kiểm soát thông tin này trong công ty.   + Các chính sách bảo mật hiện có nào được áp dụng để bảo vệ thông tin.   + Những cải tiến nào có thể được thực hiện để cải thiện tính bảo mật của những tài sản có giá trị nhất.   + Mức độ rủi ro nào bạn sẵn sàng chấp nhận đối với từng tài sản.   + Chi phí để đạt được mức độ rủi ro có thể chấp nhận được. |

* Triển khai kế hoạch bảo mật

Tiếp theo, hãy xem xét kế hoạch triển khai—các bước bạn sẽ thực hiện để đạt được mục tiêu của kế hoạch bảo mật. Cụ thể, bạn phải xác định cách bạn sẽ chuyển các mức độ rủi ro có thể chấp nhận được thành một bộ công cụ, công nghệ, chính sách và thủ tục. Bạn sẽ triển khai những công nghệ mới nào để đạt được mục tiêu và cần có những quy trình mới nào cho nhân viên?

* Thành lập một tổ chức bảo mật

|  |
| --- |
| * Tổ chức bảo mật là cần thiết để thực hiện kế hoạch bảo mật thương mại điện tử. Tổ chức bảo mật chịu trách nhiệm về việc đào tạo và đào tạo người dùng, giúp ban quản lý nhận thức được các mối đe dọa và sự cố bảo mật, đồng thời duy trì các công cụ đã chọn để triển khai bảo mật. Tổ chức bảo mật thường quản lý các biện pháp kiểm soát truy cập (access control), quy trình xác thực(authentication procedures) và chính sách ủy quyền (authorization policies) * Các biện pháp kiểm soát truy cập, quy trình xác thực và chính sách ủy quyền là các thành phần quan trọng của kế hoạch bảo mật thương mại điện tử. Các biện pháp kiểm soát truy cập xác định những người bên ngoài và bên trong có thể truy cập hợp pháp vào mạng của bạn. Quy trình xác thực xác minh danh tính của người dùng trước khi họ được phép truy cập vào tài sản thông tin. Chính sách ủy quyền xác định các mức độ truy cập khác nhau vào tài sản thông tin cho các mức độ người dùng khác nhau. * Kiểm tra bảo mật là một bước quan trọng trong việc phát triển kế hoạch bảo mật thương mại điện tử. Kiểm tra bảo mật bao gồm việc xem xét thường xuyên các nhật ký truy cập để xác định các kiểu hoạt động bất thường. |



1. **THE ROLE OF LAWS AND PUBLIC POLICY**

2.1 Private and Private-Public Cooperation Efforts

Những nỗ lực hợp tác tư nhân và công-tư

|  |
| --- |
| * Các trang web thương mại điện tử không đơn độc trong cuộc chiến chống lại các cuộc tấn công mạng. Có một số tổ chức, cả công và tư, đang nỗ lực bảo vệ các trang web này.Ở cấp liên bang Hoa Kỳ, Văn phòng An ninh mạng và Truyền thông (CS&C) thuộc Bộ An ninh Nội địa Hoa Kỳ (DHS) chịu trách nhiệm giám sát tính bảo mật, khả năng phục hồi và độ tin cậy của cơ sở hạ tầng mạng và truyền thông của Hoa Kỳ. Trung tâm Tích hợp An ninh mạng và Truyền thông Quốc gia (NCCIC) hoạt động như một trung tâm theo dõi, ứng phó sự cố và quản lý mạng 24/7. Ngoài ra, DHS cũng vận hành Nhóm Sẵn sàng Đối phó Khẩn cấp Máy tính Hoa Kỳ (US-CERT), nơi phối hợp các cảnh báo và ứng phó sự cố mạng trên cả chính phủ và khu vực tư nhân. * Các tổ chức này cung cấp một loạt các dịch vụ, bao gồm:   + Theo dõi hoạt động tội phạm trực tuyến   + Phối hợp cảnh báo và ứng phó sự cố mạng   + Cung cấp đào tạo và hỗ trợ kỹ thuật |

2.2 Government Policies and Controls on Encryption

Chính sách và kiểm soát của chính phủ về mã hóa

Tại Hoa Kỳ, cả Quốc hội và nhánh hành pháp đều đã tìm cách điều chỉnh việc sử dụng mã hóa và hạn chế khả năng tiếp cận và xuất khẩu các hệ thống mã hóa như một biện pháp ngăn chặn tội phạm và khủng bố. Ở cấp quốc tế, bốn tổ chức đã tác động đến việc buôn bán phần mềm mã hóa quốc tế: Tổ chức Hợp tác và Phát triển Kinh tế (OECD), G-7 (gồm nguyên thủ quốc gia của 7 nước công nghiệp phát triển hàng đầu thế giới, không bao gồm Nga, nước đã bị đình chỉ tham gia vào năm 2014), Hội đồng châu Âu và Sáng kiến Wassenaar (bao gồm 42 quốc gia sản xuất thiết bị công nghiệp nhạy cảm hoặc vũ khí). Các chính phủ khác nhau đã đề xuất các chương trình kiểm soát phần mềm mã hóa hoặc ít nhất là ngăn chặn tội phạm có được các công cụ mã hóa mạnh (xem Bảng 5.7). Chính phủ Hoa Kỳ và Vương quốc Anh cũng đang dành một lượng lớn nguồn lực cho các chương trình liên quan đến mật mã sẽ cho phép họ phá vỡ các liên lạc được mã hóa được thu thập trên Internet. Các tài liệu do cựu nhà thầu NSA Edward Snowden tiết lộ cho thấy cả NSA và đối tác Vương quốc Anh của nó, GCHQ, có thể phá vỡ các chương trình mã hóa được sử dụng bởi TLS, VPN và trên điện thoại thông minh (Vaughan-Nichols, 2013). Trong những năm gần đây, cuộc chiến giữa chính phủ Hoa Kỳ và các công ty công nghệ về mã hóa đã chuyển sang nền tảng di động, với việc Apple chống lại các nỗ lực của chính phủ Hoa Kỳ nhằm phá vỡ các hệ thống mã hóa iCloud và Apple iPhone của Apple và lo ngại về các ứng dụng nhắn tin mã hóa, chẳng hạn như WhatsApp, Signal và Telegram, cung cấp mã hóa đầu cuối cho văn bản, ảnh và video, khiến cho việc chính quyền chặn các liên lạc sử dụng các dịch vụ đó trở nên khó khăn, nếu không muốn nói là không thể (Isaac, 2016).

|  |
| --- |
| * Mã hóa là một công cụ quan trọng để bảo vệ thông tin cá nhân và riêng tư. * Một số chính phủ lo ngại rằng mã hóa có thể được sử dụng bởi tội phạm và khủng bố để che giấu hoạt động của họ. * Các chính phủ đã tìm cách điều chỉnh việc sử dụng mã hóa, bao gồm cả việc hạn chế khả năng tiếp cận và xuất khẩu các hệ thống mã hóa. * Cuộc chiến giữa chính phủ và các công ty công nghệ về mã hóa vẫn đang tiếp diễn. |

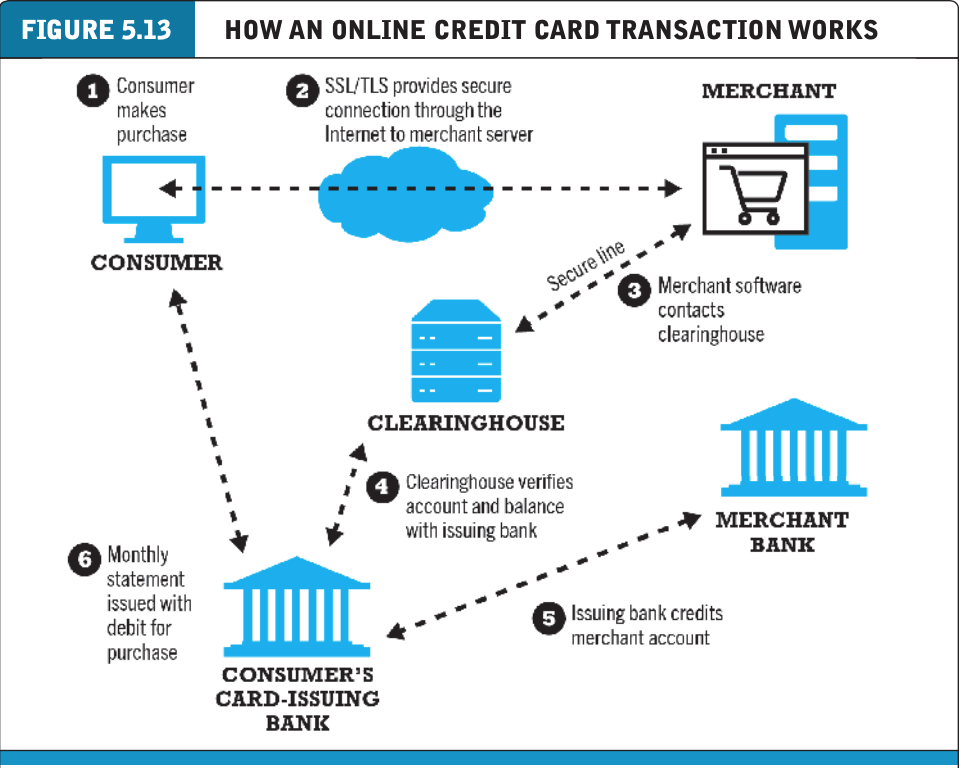
1. **E-COMMERCE PAYMENT SYSTEMS** (trang 347 - trang 358) HỆ THỐNG THANH TOÁN THƯƠNG MẠI ĐIỆN TỬ
2. **ONLINE CREDIT CARD TRANSACTIONS**

**GIAO DỊCH THẺ TÍN DỤNG TRỰC TUYẾN**

Hình 5.13 minh họa chu kỳ mua sắm thẻ tín dụng trực tuyến. Có năm bên tham gia vào giao dịch mua thẻ tín dụng trực tuyến: người tiêu dùng, thương nhân, trung tâm thanh toán, ngân hàng thương mại (đôi khi được gọi là “ngân hàng thu mua”) và ngân hàng phát hành thẻ của người tiêu dùng. Để chấp nhận thanh toán bằng thẻ tín dụng, các thương nhân trực tuyến phải có tài khoản thương mại được thiết lập với ngân hàng hoặc tổ chức tài chính. Tài khoản thương mại đơn giản là một tài khoản ngân hàng cho phép các công ty xử lý thanh toán bằng thẻ tín dụng và nhận tiền từ các giao dịch đó.

Như được hiển thị trong Hình 5.13, giao dịch thẻ tín dụng trực tuyến bắt đầu bằng việc mua hàng (1). Khi người tiêu dùng muốn thực hiện giao dịch mua, họ sẽ thêm sản phẩm vào giỏ hàng của thương nhân. Khi người tiêu dùng muốn thanh toán cho các sản phẩm trong giỏ hàng, một đường hầm bảo mật qua Internet sẽ được tạo bằng TLS. Sử dụng mã hóa, TLS bảo vệ phiên giao dịch trong thời gian thông tin thẻ tín dụng được gửi đến thương nhân và bảo vệ thông tin khỏi kẻ trộm trên Internet (2). TSL không xác thực thương nhân hoặc người tiêu dùng. Các bên giao dịch phải tin tưởng lẫn nhau.

Sau khi thông tin thẻ tín dụng của người tiêu dùng được nhận bởi thương nhân, phần mềm của thương nhân sẽ liên hệ với trung tâm thanh toán (3). Như đã đề cập trước đây, trung tâm thanh toán là một trung gian tài chính xác thực thẻ tín dụng và xác minh số dư tài khoản. Trung tâm thanh toán liên hệ với ngân hàng phát hành để xác minh thông tin tài khoản (4). Sau khi được xác minh, ngân hàng phát hành sẽ ghi có vào tài khoản của thương nhân tại ngân hàng thương mại (thường xảy ra vào ban đêm trong quá trình xử lý hàng loạt) (5). Khoản nợ vào tài khoản người tiêu dùng được gửi đến người tiêu dùng trong một bảng sao kê hàng tháng (6).

****

|  |
| --- |
| * Giao dịch thẻ tín dụng trực tuyến là hình thức thanh toán phổ biến, nhưng có một số rủi ro. * Các rủi ro bao gồm:   + Thương nhân không bao giờ nhìn thấy thẻ thực tế được sử dụng, nên có thể bị gian lận.   + Người tiêu dùng có thể tranh chấp giao dịch sau này. * Để bảo vệ quyền lợi của mình, người tiêu dùng nên:   + Hiểu cách thức hoạt động của giao dịch thẻ tín dụng trực tuyến.   + Chọn các trang web thương mại điện tử uy tín.   + Sử dụng mật khẩu mạnh và thay đổi mật khẩu thường xuyên.   + Cẩn thận khi cung cấp thông tin thẻ tín dụng. |

1.1 Credit Card E-commerce Enablers

Người hỗ trợ thương mại điện tử thẻ tín dụng

Các công ty có tài khoản thương mại vẫn cần mua hoặc xây dựng một phương tiện để xử lý giao dịch trực tuyến; bảo mật tài khoản thương mại chỉ là bước một trong quy trình hai phần. Ngày nay, các nhà cung cấp dịch vụ thanh toán Internet (đôi khi được gọi là cổng thanh toán) có thể cung cấp cả tài khoản thương mại và các công cụ phần mềm cần thiết để xử lý các giao dịch mua thẻ tín dụng trực tuyến.

Ví dụ, Authorize.net là một nhà cung cấp dịch vụ thanh toán trực tuyến. Công ty giúp thương nhân bảo mật tài khoản với một trong những đối tác cung cấp tài khoản thương mại của mình và sau đó cung cấp phần mềm xử lý thanh toán để cài đặt trên máy chủ của thương nhân. Phần mềm thu thập thông tin giao dịch từ trang web của thương nhân và sau đó chuyển nó qua “cổng thanh toán” Authorize.net đến ngân hàng thích hợp, đảm bảo rằng khách hàng được phép thực hiện giao dịch mua của họ. Sau đó, số tiền cho giao dịch được chuyển vào tài khoản thương mại của thương nhân. Các nhà cung cấp dịch vụ thanh toán trực tuyến khác bao gồm Cybersource, Stripe và Square.

|  |
| --- |
| * Các công ty có tài khoản thương mại cần mua hoặc xây dựng một phương tiện để xử lý giao dịch trực tuyến. * Các nhà cung cấp dịch vụ thanh toán Internet có thể cung cấp cả tài khoản thương mại và các công cụ phần mềm cần thiết để xử lý các giao dịch mua thẻ tín dụng trực tuyến. * Đây là một giải pháp thuận tiện cho các doanh nghiệp muốn chấp nhận thanh toán thẻ tín dụng trực tuyến mà không cần phải tự xây dựng và quản lý hệ thống thanh toán của riêng mình. |

1.2 PCI-DSS Compliance

Tuân thủ PCI-DSS

PCI-DSS (Payment Card Industry-Data Security Standard) là một tiêu chuẩn bảo mật dữ liệu toàn cầu được ban hành bởi năm công ty thẻ tín dụng lớn (Visa, MasterCard, American Express, Discover và JCB). PCI-DSS không phải là luật pháp hoặc quy định của chính phủ, mà là một tiêu chuẩn bắt buộc của ngành. Mọi thương nhân trực tuyến đều phải tuân thủ cấp độ PCI-DSS phù hợp để chấp nhận thanh toán bằng thẻ tín dụng. Những người không tuân thủ và tham gia vào vi phạm thẻ tín dụng cuối cùng có thể bị phạt tiền và các chi phí khác. PCI-DSS có nhiều cấp độ khác nhau, liên quan đến số lượng thẻ tín dụng và/hoặc thẻ ghi nợ được thương nhân xử lý mỗi năm (PCI Security Standards Council, 2019).

|  |
| --- |
| * PCI-DSS là một tiêu chuẩn bảo mật dữ liệu toàn cầu do các công ty thẻ tín dụng lớn ban hành. * Mọi thương nhân trực tuyến đều phải tuân thủ PCI-DSS để chấp nhận thanh toán bằng thẻ tín dụng. * Nếu không tuân thủ, thương nhân có thể bị phạt tiền và các chi phí khác. |

1.3 Limitations of Online Credit Card Payment Systems

Hạn chế của hệ thống thanh toán thẻ tín dụng trực tuyến

Có một số hạn chế đối với hệ thống thanh toán thẻ tín dụng hiện tại. Những hạn chế quan trọng nhất liên quan đến an ninh, rủi ro thương mại, chi phí hành chính và giao dịch cũng như công bằng xã hội. Hệ thống hiện tại có mức độ bảo mật kém. Cả người bán và người tiêu dùng đều không thể được xác thực đầy đủ. Người bán có thể là một tổ chức tội phạm được thiết kế để thu thập số thẻ tín dụng và người tiêu dùng có thể là kẻ trộm sử dụng thẻ bị đánh cắp hoặc gian lận. Rủi ro mà người bán phải đối mặt là rất cao: người tiêu dùng có thể từ chối các khoản phí ngay cả khi hàng hóa đã được vận chuyển hoặc sản phẩm đã được tải xuống. Như bạn đã biết ở đầu chương này, các công ty tín dụng đã giới thiệu thẻ EMV (thẻ có chip máy tính) để giảm thiểu gian lận thẻ tín dụng. Con chip lưu trữ dữ liệu tài khoản và tạo mã giao dịch duy nhất cho mỗi lần sử dụng. Điều này đã giảm khoảng 50% gian lận thẻ tín dụng khi mua hàng tại cửa hàng (được gọi là gian lận thẻ quà tặng (CP)) kể từ khi được giới thiệu. Nhưng bọn tội phạm đã tăng cường tập trung vào gian lận không có thẻ (CNP), dự kiến sẽ đạt tổng trị giá 130 tỷ USD từ năm 2018 đến năm 2023 (Juniper Research, 2019). Chi phí hành chính đối với người bán trong việc thiết lập hệ thống thẻ tín dụng trực tuyến và được phép chấp nhận thẻ tín dụng là rất cao. Chi phí giao dịch đối với người bán cũng rất đáng kể—khoảng 3% giao dịch mua cộng với phí giao dịch 20–35 xu cho mỗi giao dịch, cộng với các phí thiết lập khác. Thẻ tín dụng không dân chủ cho lắm, mặc dù chúng có vẻ phổ biến. Hàng triệu thanh niên không có thẻ tín dụng, cùng với hàng triệu người khác không có khả năng mua thẻ hoặc những người bị coi là có rủi ro thấp vì thu nhập thấp.

|  |
| --- |
| * Hệ thống thanh toán thẻ tín dụng hiện tại có một số hạn chế, bao gồm:   + An ninh: Hệ thống hiện tại có mức độ bảo mật kém, cả người bán và người tiêu dùng đều không thể được xác thực đầy đủ. Điều này khiến cho thẻ tín dụng dễ bị gian lận.   + Rủi ro thương mại: Người bán phải đối mặt với rủi ro cao khi chấp nhận thẻ tín dụng. Người tiêu dùng có thể từ chối các khoản phí ngay cả khi hàng hóa đã được vận chuyển hoặc sản phẩm đã được tải xuống.   + Chi phí hành chính và giao dịch: Chi phí hành chính và giao dịch đối với người bán rất cao. Điều này khiến cho việc chấp nhận thẻ tín dụng trở nên tốn kém đối với các doanh nghiệp nhỏ.   + Công bằng xã hội: Thẻ tín dụng không dân chủ cho lắm. Hàng triệu người không có khả năng mua thẻ hoặc bị coi là có rủi ro thấp vì thu nhập thấp. * Một số giải pháp tiềm năng để khắc phục các hạn chế này bao gồm:   + Tăng cường an ninh: Sử dụng các công nghệ mới như thẻ EMV và xác thực hai yếu tố để giảm gian lận.   + Giảm rủi ro thương mại: Chuyển rủi ro gian lận từ người bán sang người phát hành thẻ.   + Giảm chi phí hành chính và giao dịch: Tăng cạnh tranh giữa các công ty thẻ tín dụng và người xử lý thanh toán.   + Tăng tính khả dụng: Tạo ra các chương trình thẻ tín dụng dành cho các nhóm đối tượng bị loại trừ. |

1. **ALTERNATIVE ONLINE PAYMENT SYSTEMS**

Những hạn chế của hệ thống thẻ tín dụng trực tuyến đã mở đường cho sự phát triển của một số hệ thống thanh toán trực tuyến thay thế. Trưởng trong số đó là PayPal. PayPal (được eBay mua lại vào năm 2002 và sau đó được tách ra thành một công ty độc lập vào năm 2015) cho phép cá nhân và doanh nghiệp có tài khoản email thực hiện và nhận thanh toán lên đến một giới hạn nhất định. Paypal là một ví dụ về hệ thống thanh toán có giá trị lưu trữ trực tuyến, cho phép người tiêu dùng thực hiện thanh toán trực tuyến cho các thương gia và cá nhân khác bằng tài khoản ngân hàng hoặc thẻ tín dụng/ghi nợ của họ. Nó có sẵn ở hơn 200 quốc gia và 25 loại tiền tệ trên toàn thế giới. PayPal xây dựng dựa trên cơ sở hạ tầng tài chính hiện có của các quốc gia mà nó hoạt động. Bạn lập tài khoản PayPal bằng cách chỉ định tài khoản tín dụng, ghi nợ hoặc séc mà bạn muốn bị tính phí hoặc thanh toán khi thực hiện các giao dịch trực tuyến. Khi bạn thanh toán bằng PayPal, bạn sẽ gửi email thanh toán đến tài khoản PayPal của người bán. PayPal sẽ chuyển số tiền từ tài khoản tín dụng hoặc tài khoản vãng lai của bạn vào tài khoản ngân hàng của người bán. Điều tuyệt vời của PayPal là không cần chia sẻ thông tin tín dụng cá nhân giữa những người dùng và dịch vụ có thể được sử dụng bởi các cá nhân để thanh toán cho nhau ngay cả với số tiền nhỏ. Tuy nhiên, một vấn đề với PayPal là chi phí tương đối cao của nó. Ví dụ, khi sử dụng thẻ tín dụng làm nguồn tiền, để gửi hoặc yêu cầu tiền, chi phí dao động từ 2,9% đến 5,99% số tiền (tùy thuộc vào loại giao dịch) cộng với một khoản phí cố định nhỏ (thường là $0,30) cho mỗi giao dịch. Paypal tiếp tục thống trị thị trường thanh toán thay thế với hơn 280 triệu người dùng tiêu dùng hoạt động và 24 triệu tài khoản thương gia hoạt động. Gần 80% trong số 500 nhà bán lẻ trực tuyến hàng đầu sử dụng nút thanh toán của PayPal (PayPal Holdings, Inc., 2020; Kim, 2019).

Mặc dù PayPal là giải pháp thay thế thẻ tín dụng trực tuyến được biết đến và sử dụng nhiều nhất, nhưng cũng có một số giải pháp thay thế khác. Amazon Pay dành cho những người tiêu dùng lo ngại về việc giao phó thông tin thẻ tín dụng của họ cho các nhà bán lẻ trực tuyến không quen thuộc. Người tiêu dùng có thể mua hàng hóa và dịch vụ tại các trang web không thuộc Amazon bằng phương thức thanh toán được lưu trữ trong tài khoản Amazon của họ, mà không cần phải nhập lại thông tin thanh toán của họ tại trang web của người bán. Amazon cung cấp dịch vụ xử lý thanh toán. Facebook Pay, được giới thiệu vào tháng 11 năm 2019, là một dịch vụ cho phép người dùng chuyển tiền trực tiếp từ ngân hàng và thẻ tín dụng của họ để mua hàng từ các thương gia và gửi và nhận tiền. Ban đầu, nó có sẵn trên Facebook và Messenger và sau đó sẽ được triển khai trên Instagram và WhatsApp. Người dùng nhập phương thức thanh toán ưa thích của họ và sau đó Facebook sẽ lưu thông tin đó cho các giao dịch trong tương lai (Liu, 2019).

Visa Checkout (trước đây là V.me) và MasterPass của MasterCard thay thế tên người dùng và mật khẩu cho số thẻ thanh toán thực tế trong quá trình thanh toán trực tuyến. Cả MasterPass và Visa Checkout đều được hỗ trợ bởi một số bộ xử lý thanh toán lớn và các nhà bán lẻ trực tuyến. Tuy nhiên, chúng vẫn chưa đạt được mức sử dụng của Paypal.

PayPal Credit (trước đây là Bill Me Later) cũng hấp dẫn những người tiêu dùng không muốn nhập thông tin thẻ tín dụng của họ trực tuyến. PayPal Credit là một tài khoản tín dụng mở. Người dùng chọn tùy chọn PayPal Credit khi thanh toán. Afterpay là nhà cung cấp kế hoạch thanh toán trả góp kỹ thuật số cho phép người dùng thanh toán cho các giao dịch mỗi hai tuần trong bốn đợt, với người bán chi trả mọi khoản phí liên quan đến chương trình. Afterpay hiện đang được cung cấp bởi hơn 9.000 nhà bán lẻ của Hoa Kỳ và được hơn 3,6 triệu người tiêu dùng sử dụng tích cực (Kats, 2020). Các sản phẩm tương tự (đôi khi cũng được gọi là khoản vay tại điểm bán hàng (POS)) được cung cấp bởi Sezzle, Afirm và Klarna.

|  |
| --- |
| * Những hạn chế của hệ thống thẻ tín dụng trực tuyến   + Mức độ bảo mật kém: Cả người bán và người tiêu dùng đều không thể được xác thực đầy đủ. Điều này khiến cho thẻ tín dụng dễ bị gian lận.   + Rủi ro thương mại cao: Người bán phải đối mặt với rủi ro cao khi chấp nhận thẻ tín dụng. Người tiêu dùng có thể từ chối các khoản phí ngay cả khi hàng hóa đã được vận chuyển hoặc sản phẩm đã được tải xuống.   + Chi phí hành chính và giao dịch cao: Chi phí hành chính và giao dịch đối với người bán rất cao. Điều này khiến cho việc chấp nhận thẻ tín dụng trở nên tốn kém đối với các doanh nghiệp nhỏ. * Sự phát triển của các hệ thống thanh toán trực tuyến thay thế   + PayPal là hệ thống thanh toán thay thế phổ biến nhất. Nó cung cấp một số lợi ích cho cả người tiêu dùng và người bán, bao gồm bảo mật cao hơn, chi phí thấp hơn và tính tiện lợi.   + Một số hệ thống thanh toán thay thế khác bao gồm Amazon Pay, Facebook Pay, Visa Checkout, PayPal Credit và Afterpay. Các hệ thống này cung cấp các tính năng và lợi ích khác nhau để đáp ứng nhu cầu của các đối tượng mục tiêu khác nhau. |

1. **MOBILE PAYMENT SYSTEMS: YOUR SMARTPHONE WALLET**

Hệ thống thanh toán di động là thành phần phát triển nhanh nhất của các phương thức thanh toán thay thế.

Việc sử dụng thiết bị di động làm phương thức thanh toán đã được thiết lập tốt ở Châu Á và nhiều quốc gia ở Châu Âu, chẳng hạn như Đan Mạch, Na Uy, Ý và Hà Lan, và hiện đang phát triển ở Hoa Kỳ, nơi cơ sở hạ tầng hỗ trợ thanh toán di động hiện đã có sẵn. Thanh toán di động bao gồm bất kỳ loại thanh toán nào sử dụng thiết bị di động, bao gồm thanh toán hóa đơn, mua hàng trực tuyến, mua hàng tại cửa hàng và thanh toán P2P.

Ví di động (đôi khi cũng được gọi là ví kỹ thuật số) là các ứng dụng điện thoại thông minh lưu trữ thẻ ghi nợ, phiếu thưởng, hóa đơn và chứng từ có thể được tìm thấy trong ví truyền thống (First Annapolis Consulting, 2017).

Có ba loại chính của ứng dụng ví di động: ví tiệm cận phổ quát, ví tiệm cận thương hiệu và ứng dụng P2P. Ví di động tiệm cận phổ quát, chẳng hạn như Apple Pay, Google Pay và Samsung Pay, có thể được sử dụng tại nhiều nhà bán lẻ khác nhau cho các giao dịch bán hàng tại điểm nếu nhà bán lẻ hỗ trợ dịch vụ đó (ví dụ: có ứng dụng dành cho thương nhân của Apple và có thể chấp nhận các loại thanh toán đó) là loại ví được biết đến nhiều nhất và phổ biến nhất. Ví di động tiệm cận thương hiệu là các ứng dụng di động chỉ có thể được sử dụng tại một nhà bán lẻ duy nhất. Ví dụ, Walmart, Tesco và Starbucks đều có các ứng dụng ví di động rất thành công. Ứng dụng thanh toán di động P2P, chẳng hạn như Venmo và Square Cash, được sử dụng để thanh toán giữa những cá nhân có cùng ứng dụng.

Apple Pay, Google Pay và Samsung Pay là một trong những ứng dụng ví di động phổ biến nhất được sử dụng trên toàn thế giới, mặc dù ở Trung Quốc, Alipay và WeChat Pay chiếm ưu thế (Xem Hình 5.14). Nhìn chung, vào năm 2020, khoảng 1,1 tỷ người trên toàn thế giới đã sử dụng các ứng dụng thanh toán di động tiệm cận.

Tại Hoa Kỳ, các ứng dụng tiệm cận di động (cả phổ quát và thương hiệu) đã được sử dụng để xử lý khoảng 130 tỷ đô la thanh toán trong năm 2020, tăng gần 20% so với năm 2019. Giá trị giao dịch của ứng dụng thanh toán di động P2P tại Hoa Kỳ thậm chí còn cao hơn, đạt gần 400 tỷ đô la trong năm 2020 (eMarketer, Inc., 2020b, 2020c).

Thanh toán di động tiếp tục là hình thức thanh toán phát triển nhanh nhất, nhưng chỉ chiếm một phần nhỏ trong tổng thị trường thanh toán của Hoa Kỳ trị giá 97 nghìn tỷ đô la, bao gồm thẻ tín dụng, thẻ ghi nợ, thanh toán tự động (gọi là thanh toán ACH) và thanh toán bằng séc (Cục Dự trữ Liên bang, 2019). Người tiêu dùng vẫn thoải mái khi sử dụng thẻ tín dụng và thẻ ghi nợ, mặc dù các ứng dụng thanh toán trong cửa hàng có thương hiệu tại các nhà bán lẻ quốc gia của Hoa Kỳ như Starbucks, Walmart và Target đã rất thành công và đang phát triển nhanh hơn về mặt người dùng và đặc biệt là mức sử dụng thực tế trong các cửa hàng so với Apple Pay, Google Pay và Samsung Pay.

Trong thanh toán P2P, các nhà dẫn đầu của Hoa Kỳ là Venmo thuộc sở hữu của PayPal, Zelle được cung cấp bởi hơn 250 ngân hàng của Hoa Kỳ và Square Cash thuộc sở hữu của Square, công ty tiên phong trong Square Reader, một thiết bị cho phép bất kỳ ai có điện thoại thông minh hoặc máy tính bảng đều có thể chấp nhận thanh toán bằng thẻ (Daly, 2019; eMarketer, Inc., 2020d). Để biết thêm về thanh toán di động, hãy xem nghiên cứu điển hình, Alipay và WeChat Pay dẫn đầu trong thanh toán di động, ở cuối chương.

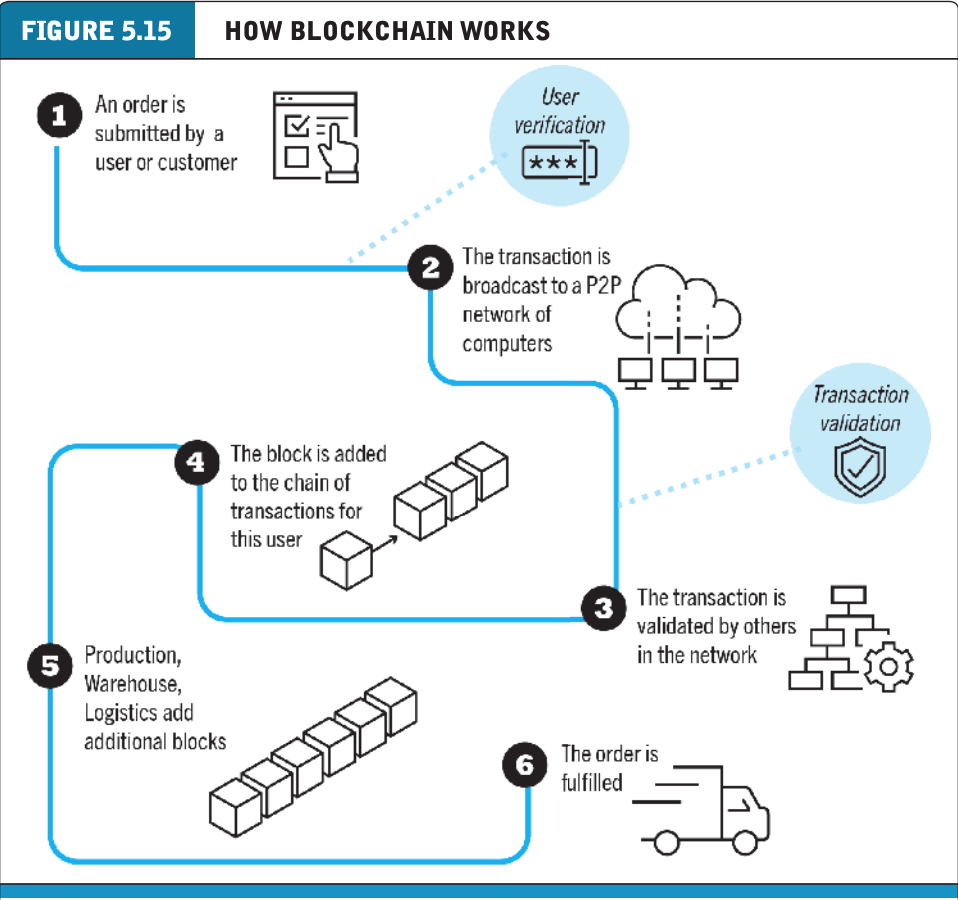
Giao tiếp trường gần (NFC) là một tập hợp các công nghệ không dây tầm ngắn được sử dụng để chia sẻ thông tin giữa các thiết bị trong khoảng cách khoảng 2 inch (50 mm) của nhau. Thiết bị NFC có thể là thiết bị hoạt động hoặc thiết bị thụ động. Một kết nối yêu cầu một thiết bị hoạt động (thiết bị khởi tạo, chẳng hạn như điện thoại thông minh) và một thiết bị mục tiêu, chẳng hạn như đầu đọc NFC của nhà bán hàng, có thể phản hồi yêu cầu từ thiết bị khởi tạo. Các thiết bị mục tiêu NFC có thể là các dạng rất đơn giản như thẻ, nhãn dán, móc khóa hoặc đầu đọc. Giao tiếp ngang hàng NFC có thể thực hiện được khi cả hai thiết bị đều hoạt động. Người tiêu dùng có thể quẹt điện thoại có trang bị NFC của họ gần đầu đọc của nhà bán hàng để thanh toán cho các giao dịch mua.

Cả Apple Pay và Google Pay đều yêu cầu NFC, trong khi Samsung Pay sử dụng cả NFC và công nghệ truyền tải bảo mật từ tính tương tự như công nghệ được sử dụng trên dải từ trên thẻ tín dụng. Công nghệ mã QR (Quick Response) sử dụng ứng dụng di động để tạo mã vạch hai chiều (mã QR) trong đó thông tin được mã hóa. Sau đó, người bán sẽ quét mã QR và số tiền thanh toán sẽ được trừ khỏi ví di động của khách hàng, được liên kết với thẻ tín dụng hoặc thẻ ghi nợ. Walmart Pay, Starbucks Pay, Target Pay, Dunkin và nhiều nhà bán lẻ khác đều sử dụng công nghệ dựa trên mã QR.

|  |
| --- |
| * Thanh toán di động là một thị trường đang phát triển nhanh chóng. Trong năm 2020, khoảng 1,1 tỷ người trên toàn thế giới đã sử dụng các ứng dụng thanh toán di động tiệm cận, và giá trị giao dịch của ứng dụng thanh toán di động P2P tại Hoa Kỳ đã đạt gần 400 tỷ đô la. * Có hai loại chính của ứng dụng thanh toán di động: ví tiệm cận phổ quát và ví tiệm cận thương hiệu. Ví tiệm cận phổ quát, chẳng hạn như Apple Pay và Google Pay, có thể được sử dụng tại nhiều nhà bán lẻ khác nhau, trong khi ví tiệm cận thương hiệu chỉ có thể được sử dụng tại một nhà bán lẻ duy nhất. * Giao tiếp trường gần (NFC) là công nghệ hỗ trợ chính cho ví tiệm cận phổ quát. NFC là một công nghệ không dây tầm ngắn cho phép thiết bị di động giao tiếp với các thiết bị khác, chẳng hạn như đầu đọc thanh toán của nhà bán lẻ. |

1. **BLOCKCHAIN AND CRYPTOCURRENCIES**

Blockchain là một công nghệ cho phép các tổ chức tạo và xác minh các giao dịch trên mạng gần như ngay lập tức mà không cần cơ quan trung tâm. Blockchain về cơ bản là một cơ sở dữ liệu phân tán được chia sẻ trên mạng ngang hàng (P2P). Các giao dịch được ghi lại trên blockchain theo chuỗi thời gian, có nghĩa là mỗi giao dịch đều được liên kết với giao dịch trước đó. Điều này làm cho blockchain rất khó bị giả mạo hoặc thay đổi.



Blockchain có nhiều lợi ích cho các doanh nghiệp và cá nhân, bao gồm:

* Tính minh bạch và an toàn: Tất cả các giao dịch trên blockchain đều được công khai và được bảo vệ bằng mật mã, điều này giúp giảm thiểu rủi ro gian lận và bảo mật dữ liệu.
* Hiệu quả và tiết kiệm chi phí: Blockchain có thể giúp các doanh nghiệp giảm chi phí và cải thiện hiệu quả hoạt động bằng cách tự động hóa nhiều quy trình thủ công.
* Tính tiện lợi: Blockchain có thể được sử dụng để thực hiện các giao dịch xuyên biên giới một cách nhanh chóng và dễ dàng.

Blockchain có nhiều ứng dụng tiềm năng trong nhiều lĩnh vực khác nhau, bao gồm:

* Tài chính: Blockchain có thể được sử dụng để tạo và quản lý các loại tiền điện tử, chẳng hạn như Bitcoin và Ethereum. Blockchain cũng có thể được sử dụng để cải thiện hiệu quả và minh bạch của các hệ thống thanh toán và tài chính truyền thống.
* Quản lý chuỗi cung ứng: Blockchain có thể được sử dụng để theo dõi và quản lý chuỗi cung ứng hiệu quả hơn, giúp giảm thiểu rủi ro và cải thiện chất lượng sản phẩm.
* Y tế: Blockchain có thể được sử dụng để lưu trữ và chia sẻ dữ liệu y tế một cách an toàn và hiệu quả. Điều này có thể giúp cải thiện chất lượng chăm sóc sức khỏe và giảm chi phí.
* Bất động sản: Blockchain có thể được sử dụng để số hóa và đơn giản hóa các quy trình giao dịch bất động sản, giúp tiết kiệm thời gian và chi phí cho cả người mua và người

Bitcoin là một loại tiền điện tử được phân cấp và ẩn danh. Nó được khai thác bằng máy tính giải quyết các vấn đề toán học phức tạp. Bitcoin bị giới hạn nguồn cung ở mức 21 triệu xu. Các giao dịch bitcoin được ghi lại trên blockchain, đây là sổ cái công khai của tất cả các giao dịch.

Bitcoin đã được ca ngợi vì tính bảo mật, ẩn danh và phí giao dịch thấp. Tuy nhiên, nó cũng bị chỉ trích vì tính biến động, tiêu thụ năng lượng và liên quan đến các hoạt động bất hợp pháp.

Bitcoin đang được chấp nhận trong thế giới tài chính, với các ngân hàng và sàn giao dịch lớn cung cấp giao dịch Bitcoin. Tuy nhiên, một số chính phủ và cơ quan quản lý đã cấm hoặc hạn chế Bitcoin.

Tương lai của Bitcoin là không chắc chắn, nhưng nó có tiềm năng cách mạng hóa cách chúng ta thanh toán hàng hóa và dịch vụ.bán.

1. **ELECTRONIC BILLING PRESENTMENT AND PAYMENT**

**TRÌNH BÀY VÀ THANH TOÁN ĐIỆN TỬ**

(trang 358 - trang 361)

1. **MARKET SIZE AND GROWTH**

**QUY MÔ THỊ TRƯỜNG VÀ TĂNG TRƯỞNG**

Vào năm 2002, 61% hóa đơn ở Hoa Kỳ được thanh toán bằng séc và chỉ 12% được thanh toán trực tuyến. Ngược lại, theo khảo sát gần đây nhất của Fiserv về hành vi tiêu dùng, 65% người tiêu dùng sử dụng thanh toán hóa đơn trực tuyến, hơn 50% đã thiết lập thanh toán trực tuyến tự động và gần 60% nhận hóa đơn điện tử thay vì hóa đơn giấy. Người tiêu dùng, đặc biệt là những người thuộc thế hệ lớn tuổi, đang ngày càng cảm thấy thoải mái hơn về tính bảo mật của việc nhận và thanh toán hóa đơn trực tuyến. Thanh toán hóa đơn trên thiết bị di động đang gia tăng, với hầu hết người tiêu dùng cho biết sự thuận tiện và tiết kiệm thời gian khi sử dụng thanh toán hóa đơn trên thiết bị di động (Fiserv, 2019).

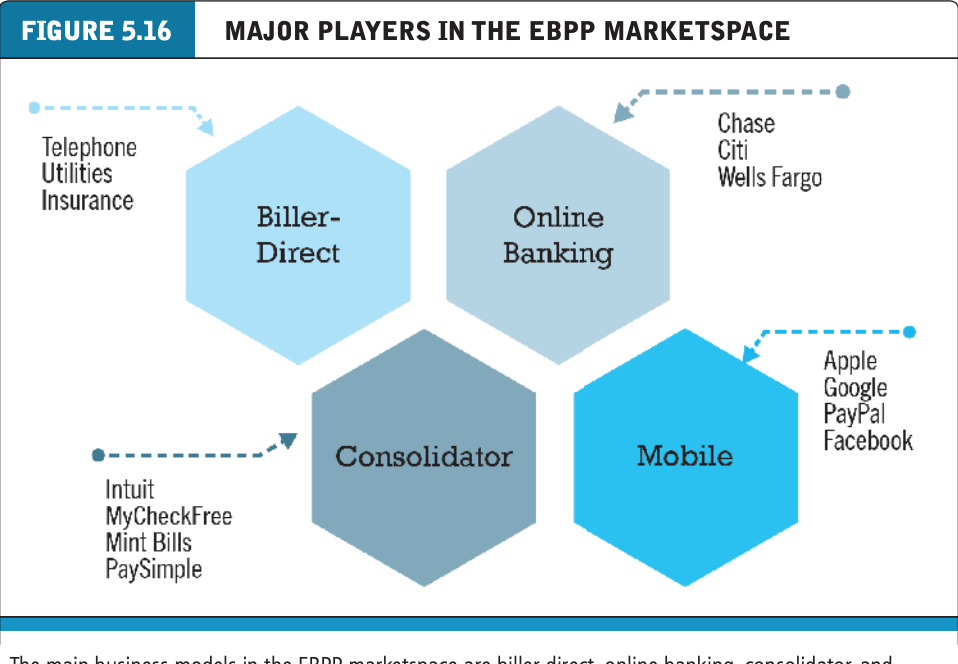
Một lý do chính cho sự gia tăng của việc sử dụng EBPP là các công ty đã nhận ra họ có thể tiết kiệm bao nhiêu tiền thông qua việc lập hóa đơn trực tuyến. Không chỉ có khoản tiết kiệm tiền bưu phí và xử lý, mà các khoản thanh toán cũng có thể được nhận nhanh hơn (nhanh hơn từ 3 đến 12 ngày so với hóa đơn giấy được gửi qua đường bưu điện thông thường), do đó cải thiện dòng tiền. Các tùy chọn thanh toán hóa đơn trực tuyến cũng có thể giảm số lượng cuộc gọi điện đến đường dây dịch vụ khách hàng của công ty. Để nhận ra những khoản tiết kiệm này, nhiều công ty đã trở nên quyết liệt hơn trong việc khuyến khích khách hàng chuyển sang EBPP bằng cách áp dụng phí cho đặc quyền tiếp tục nhận hóa đơn giấy.

Tuy nhiên, tài chính không phải là tất cả. Các công ty cũng phát hiện ra rằng hóa đơn là cả cơ hội bán hàng và cơ hội giữ chân khách hàng, và phương tiện kỹ thuật số cung cấp nhiều lựa chọn hơn khi nói đến tiếp thị và quảng cáo. Hoàn tiền, ưu đãi tiết kiệm, bán chéo và bán tăng đều có thể thực hiện được trong lĩnh vực kỹ thuật số và ít tốn kém hơn nhiều so với việc gửi thư phong bì nhồi nhét các ưu đãi.

|  |
| --- |
| * Thanh toán hóa đơn trực tuyến (EBPP) đã trở nên phổ biến hơn trong những năm gần đây. Theo khảo sát của Fiserv, 65% người tiêu dùng ở Hoa Kỳ hiện sử dụng EBPP, tăng từ 12% vào năm 2002. * Có nhiều lý do cho sự gia tăng này, bao gồm sự tiện lợi, tiết kiệm chi phí và cơ hội tiếp thị và bán hàng. * Các công ty đã nhận ra họ có thể tiết kiệm tiền bằng cách chuyển sang EBPP. Không chỉ bưu phí và chi phí xử lý mà còn cả thời gian và nhân lực. * EBPP cũng có thể giúp các công ty cải thiện dòng tiền và giảm số lượng cuộc gọi đến dịch vụ khách hàng. * Ngoài những lợi ích tài chính, EBPP còn cung cấp cho các công ty cơ hội tiếp thị và bán hàng. Các công ty có thể sử dụng hóa đơn điện tử để gửi các ưu đãi và khuyến mãi, cũng như để bán chéo và bán tăng các sản phẩm và dịch vụ bổ sung. |

1. **EBPP BUSINESS MODELS**

Có bốn mô hình kinh doanh EBPP: ngân hàng trực tuyến, biller-direct, di động và tổng hợp.



* Mô hình ngân hàng trực tuyến là mô hình được sử dụng rộng rãi nhất hiện nay. Người tiêu dùng thiết lập dịch vụ thanh toán trực tuyến với ngân hàng của họ và sử dụng nó để thanh toán hóa đơn khi đến hạn hoặc tự động thanh toán cho các khoản như tiền thuê nhà. Các khoản thanh toán được thực hiện trực tiếp vào tài khoản ngân hàng của người bán. Mô hình này có ưu điểm là tiện lợi cho người tiêu dùng vì các khoản thanh toán được tự động trừ đi, thường có thông báo từ ngân hàng hoặc thương gia rằng tài khoản của họ đã bị ghi nợ.
* Trong mô hình biller-direct, người tiêu dùng được gửi hóa đơn qua thông báo e-mail và truy cập trang web của thương gia để thực hiện thanh toán bằng thông tin đăng nhập ngân hàng của họ. Mô hình này có ưu điểm cho phép thương gia tương tác với khách hàng bằng cách gửi phiếu giảm giá hoặc phần thưởng. Tuy nhiên, mô hình biller-direct là một quy trình hai bước và ít thuận tiện hơn cho người tiêu dùng.
* Mô hình di động cho phép người tiêu dùng thực hiện thanh toán bằng các ứng dụng di động, một lần nữa dựa vào thông tin đăng nhập ngân hàng của họ làm nguồn tiền. Người tiêu dùng được thông báo về hóa đơn qua tin nhắn văn bản và xác nhận thanh toán. Một phần mở rộng của mô hình này là mô hình xã hội-di động, nơi các mạng xã hội như Facebook tích hợp thanh toán vào dịch vụ nhắn tin của họ. Mô hình di động có một số ưu điểm, không chỉ là sự tiện lợi cho người tiêu dùng khi thanh toán hóa đơn khi sử dụng điện thoại của họ, mà còn là tốc độ mà hóa đơn có thể được thanh toán trong một bước. Đây là hình thức EBPP phát triển nhanh nhất. Ví dụ: Facebook Messenger cho phép người dùng gửi và nhận tiền P2P tới và từ bạn bè và gia đình bằng thẻ ghi nợ hoặc tài khoản PayPal. Facebook không tính phí cho những giao dịch này (Facebook, 2020).
* Trong mô hình tổng hợp, một bên thứ ba, chẳng hạn như một tổ chức tài chính hoặc một cổng thông tin tập trung như Intuit's Paytrust, Fiserv's MyCheckFree, Mint Bills và những người khác, tổng hợp tất cả hóa đơn cho người tiêu dùng và cho phép thanh toán hóa đơn một cửa. Mô hình này có ưu điểm cho phép người tiêu dùng xem tất cả hóa đơn của họ tại một trang web hoặc ứng dụng. Tuy nhiên, vì hóa đơn đến hạn vào những thời điểm khác nhau nên người tiêu dùng cần thường xuyên kiểm tra cổng thông tin của họ. Mô hình tổng hợp phải đối mặt với một số thách thức. Đối với các biller, sử dụng mô hình tổng hợp đồng nghĩa với việc thời gian trễ giữa việc lập hóa đơn và thanh toán tăng lên, đồng thời cũng đưa ra một trung gian giữa công ty và khách hàng của họ.

Hỗ trợ các mô hình kinh doanh chính này là các nhà cung cấp cơ sở hạ tầng như Fiserv, Envestnet Yodlee, FIS Global, ACI Worldwide, MasterCard RPPS (Remote Payment and Presentment Service) và những người khác cung cấp phần mềm để tạo hệ thống EBPP hoặc xử lý lập hóa đơn và thu tiền cho biller. Hình 5.16 phân loại các đối thủ cạnh tranh chính trên thị trường EBPP.

Tại Liên minh Châu Âu, Chỉ thị Dịch vụ Thanh toán Đã sửa đổi (PSD 2), có hiệu lực từ năm 2018, cho phép khách hàng ngân hàng dễ dàng sử dụng các nhà cung cấp bên thứ ba để thanh toán hóa đơn và quản lý tài chính của họ bằng cách yêu cầu các ngân hàng cấp quyền truy cập cho các nhà cung cấp đó vào tài khoản khách hàng ngân hàng thông qua các giao diện lập trình ứng dụng mở (API).

|  |
| --- |
| Có bốn mô hình kinh doanh EBPP chính: ngân hàng trực tuyến, biller-direct, di động và tổng hợp. Mỗi mô hình có những ưu nhược điểm riêng. Mô hình di động là mô hình phát triển nhanh nhất hiện nay.  Hỗ trợ các mô hình kinh doanh chính này là các nhà cung cấp cơ sở hạ tầng cung cấp phần mềm để tạo hệ thống EBPP hoặc xử lý lập hóa đơn và thu tiền cho biller.  Tại Liên minh Châu Âu, Chỉ thị Dịch vụ Thanh toán Đã sửa đổi (PSD 2) cho phép khách hàng ngân hàng dễ dàng sử dụng các nhà cung cấp bên thứ ba để thanh toán hóa đơn và quản lý tài chính của họ. |

1. **CASE STUDY**

**Alipay**

* Alibaba là một công ty thương mại điện tử lớn nhất ở Trung Quốc. Họ cung cấp các dịch vụ thương mại điện tử B2B, B2C và C2C thông qua các trang web như Alibaba, Taobao và Tmall.
* Alibaba thành lập Alipay vào năm 2004 để giải quyết vấn đề thiếu niềm tin giữa người mua và người bán trên các nền tảng của họ. Hệ thống ký quỹ của Alipay giúp tạo lòng tin của người tiêu dùng Trung Quốc.
* Từ năm 2010 đến năm 2020, số lượng người dùng Internet di động ở Trung Quốc đã tăng từ khoảng 265 triệu lên hơn 835 triệu và tỷ lệ dân số mua sắm trực tuyến đã tăng từ khoảng 17% dân số Trung Quốc lên gần 65%.. Điều này đã đóng góp vào sự tăng vọt của Alipay trên thị trường thanh toán di động Trung Quốc.
* Alipay đã mở rộng hoạt động sang nhiều khu vực khác ngoài Trung Quốc, như Pakistan, Hàn Quốc, Malaysia, Thái Lan và Singapore.
* Alipay đã mở rộng khỏi hoạt động thanh toán trực tuyến và di động và hiện cung cấp nhiều sản phẩm tài chính khác,
* quỹ thị trường tiền tệ Yu'e Bao của Alipay hiện là quỹ thị trường tiền tệ lớn nhất trên thế giới; Người dùng Alipay có thể đầu tư vào quỹ một cách nhanh chóng và dễ dàng bằng chính ứng dụng họ sử dụng để thanh toán tại nhà hàng hoặc cửa hàng tạp hóa.
* Alipay cũng sử dụng các đánh giá thuật toán để cung cấp khoản vay cả cho cá nhân lẫn doanh nghiệp; công cụ xử lý rủi ro được hỗ trợ bởi trí tuệ nhân tạo của nó đã làm giảm đáng kể tỷ lệ thua lỗ do gian lận của Alipay
* Alipay đang tham gia vào các dự án liên quan đến công nghệ blockchain, trí tuệ nhân tạo, bảo mật, Internet of Things và nhiều lĩnh vực khác.

⇒ Alipay là một ví dụ điển hình cho sự phát triển và đa dạng hóa dịch vụ tài chính và thanh toán di động, bắt đầu từ một hệ thống thanh toán và mở rộng sang các dịch vụ tài chính và nghiên cứu công nghệ.