

Trung Thu Miracle

SOCIAL ENGINEERING: TÂM LÝ HỌC VÀ CÁCH THỨC TẦN CÔNG



LỜI GIỚI THIỆU

“*Malware for the human brain*” – bạn đã bao giờ nghe đến khái niệm này chưa?

Chúng ta luôn cảnh giác với virus máy tính, nhưng ít ai nhận ra rằng bộ não con người cũng có thể bị tấn công theo cách tương tự. Ngày nay, kẻ xấu không cần phải hack máy tính – chúng hack trực tiếp vào tâm trí nạn nhân.

Tôi viết tài liệu này với một lý do đơn giản: **viết cho những đứa trẻ đã không được bảo vệ được, và bảo vệ những đứa trẻ đang, sẽ cần được bảo vệ**. Trong thế giới số, nguy hiểm không chỉ đến từ những dòng mã độc, mà còn từ những chiến thuật thao túng tinh vi, những cuộc tấn công vào nhận thức và cảm xúc của con người.

Tài liệu này tập trung vào **Social engineering: Tâm lý học và cách thức tấn công**. Những trang viết này không chỉ đơn thuần là tập hợp những ý chính, mà còn là những cánh cửa nhỏ dẫn lối bạn đến những suy ngẫm sâu xa hơn. Mỗi dòng chữ ở đây không phải để khép lại một câu chuyện, mà để gợi mở những câu hỏi – những câu hỏi có thể thay đổi cách bạn nhìn thế giới, nhìn chính mình, và cả cách bạn lựa chọn bước tiếp.

Hãy cùng tôi, không ngừng đặt ra những câu hỏi. Không phải vì chúng ta cần tất cả câu trả lời ngay lập tức, mà vì chính hành trình tìm kiếm ấy sẽ đưa chúng ta đến những điều ý nghĩa hơn. Hãy để sự tò mò dẫn dắt ta đi xa hơn, để những câu hỏi mở ra những cánh cửa chưa từng thấy, và để mỗi ngày trôi qua, chúng ta lại tiến gần hơn một chút đến một thế giới tốt đẹp hơn..

Nếu bạn thấy tài liệu này hữu ích, hãy giúp tôi lan tỏa nó đến nhiều người hơn. Một hành động nhỏ của bạn có thể giúp ai đó tránh khỏi những cạm bẫy vô hình trên không gian mạng.

💌 Hỗ trợ tác giả

Tôi dành nhiều thời gian và tâm huyết để nghiên cứu, tổng hợp, viết và chia sẻ tài liệu này miễn phí. Nếu muốn đóng góp để tôi có thể tiếp tục tạo ra những nội dung hữu ích hơn, bạn có thể ủng hộ qua:

✉ Thông tin tài khoản

- ◆ Techcombank (Gia Định – Hồ Chí Minh)
- ◆ 19023597185015
- ◆ Trần Trung Thu

(Chỉ cần một chút hỗ trợ từ bạn cũng là nguồn động viên rất lớn để tôi tiếp tục hành trình này!)

Nội dung vẫn tiếp tục được cập nhật, nếu bạn có những góp ý, kính vui lòng chuyển gửi đến tôi nhé!

🚀 Thông tin liên hệ:

- ◆ Trung Thu Miracle
- ◆ SDT: 0901135206
- ◆ trunghu.cyberpsy@gmail.com

Thành phố Hồ Chí Minh, ngày 25 tháng 03 năm 2025!

Chân thành cảm ơn bạn đã đọc!

Hãy nhớ: Kẻ tấn công không chỉ hack máy tính, mà có thể hack tâm trí của bạn!

MỤC LỤC

I. TỔNG QUAN VỀ CÁC MỐI ĐE DỌA AN NINH MẠNG VÀ TỘI PHẠM MẠNG	1
1.1. Giới thiệu	1
1.2. Các loại mối đe dọa an ninh mạng	2
1.3. Phân loại tội phạm mạng	3
1.4. Rủi ro an toàn trên mạng xã hội	3
1.5. Lừa đảo trực tuyến (cyber-enabled fraud)	3
II. TỔNG QUAN VỀ YẾU TỐ CON NGƯỜI TRONG TỘI PHẠM MẠNG	5
2.1. Tội phạm mạng	5
2.2. Mối quan hệ giữa các thực thể trong môi trường tội phạm mạng	5
2.3. Động cơ phạm tội mạng	5
2.4. Tâm lý nạn nhân và sự dễ tổn thương	5
2.5. Hạn chế của cơ quan thực thi pháp luật trong xử lý tội phạm mạng	6
2.6. Sự hạn chế trong nhận thức & ra quyết định của con người	6
2.7. Ảnh hưởng của tính cách đối với tội phạm mạng	6
2.8. Góc nhìn văn hóa trong tội phạm mạng	7
2.9. Văn hóa an ninh trong doanh nghiệp	7
2.10. Kết luận	7
III. PHÂN TÍCH SÂU VỀ CÁC THỰC THỂ TRONG TỘI PHẠM MẠNG	8
3.1. Động cơ và lợi ích của kẻ tấn công	8
3.2. Nạn nhân (victims) trong tội phạm mạng	9
3.3. Cơ quan thực thi pháp luật (law enforcement) và những thách thức	9
3.4. Kết luận: làm sao để giảm tội phạm mạng?	10
IV. SOCIAL ENGINEERING: TÂM LÝ HỌC & CÁCH THỨC TẤN CÔNG	11
4.1. Social engineering là gì?	11
4.2. Các hiệu ứng tâm lý mà kẻ tấn công sử dụng	11
4.3. Xây dựng sự tin tưởng và quan hệ với mục tiêu	13
4.4. Ba kỹ thuật thuyết phục của Aristotle để thao túng nạn nhân	14
4.5. Chu trình tấn công social engineering (theo Kevin Mitnick)	15
4.6. Kết luận & bài học rút ra	16
V. GIẢI PHÁP BẢO VỆ BẢN THÂN NHẰM PHÒNG CHỐNG SOCIAL ENGINEERING	18
VI. CÁC CÂU HỎI LIÊN QUAN ĐẾN SOCIAL ENGINEERING	19
VII. TÀI LIỆU THAM KHẢO	30

I. TỔNG QUAN VỀ CÁC MỐI ĐE DỌA AN NINH MẠNG VÀ TỘI PHẠM MẠNG

1.1. Giới thiệu

♦ An ninh mạng ngày càng trở thành mối quan tâm lớn đối với cá nhân, doanh nghiệp và chính phủ. Các mối đe dọa ngày càng phức tạp và nguy hiểm hơn.

♦ **Những yếu tố khiến tội phạm mạng trở nên nghiêm trọng và khó kiểm soát**

• **Không có ranh giới địa lý**

- Toàn cầu hóa kinh tế cho phép các cuộc tấn công có phạm vi ảnh hưởng lớn.
- Sự kết nối giữa các hệ thống cho phép mã độc, virus và các cuộc tấn công lừa đảo lan rộng với quy mô lớn.

• **Tự động hóa và tốc độ tấn công**

- Các tội phạm truyền thống như gian lận thẻ tín dụng đã được nâng lên một cấp độ mới trên không gian mạng.
- Các tội phạm mạng chỉ cần một phần nhỏ các cuộc tấn công thành công (ví dụ, dưới 1%) để có lợi nhuận.

• **Tội phạm mạng như một dịch vụ (Cybercrime-as-a-Service)**

- Tội phạm không cần có chuyên môn cao, vì đã có các nhóm phát triển công cụ tấn công và bán cho những kẻ khác.
- Mô hình ransomware-as-a-service (RaaS) giúp tội phạm dễ dàng kiếm lợi nhuận bằng cách thu một phần từ tiền chuộc.

• **Công nghệ mới hỗ trợ tội phạm**

- Tiền mã hóa và blockchain giúp che giấu danh tính người giao dịch.
- Mã hóa đầu cuối (End-to-End Encryption) bảo vệ quyền riêng tư nhưng cũng cản trở cơ quan thực thi pháp luật điều tra.

• **Ẩn danh trên mạng**

- Các công cụ như mạng Tor cho phép người dùng ẩn danh một cách tương đối.
- Nghiên cứu hành vi chỉ ra rằng sự ẩn danh có thể khiến con người hành xử khác đi, làm gia tăng hành vi phạm tội.

• **Tính cơ hội của tội phạm mạng**

- Tội phạm nhanh chóng lợi dụng tình huống mới, như thuê người làm "money mule" để rửa tiền trong đại dịch COVID-19.

• **Thách thức về thẩm quyền và luật pháp**

- Tội phạm mạng có thể xảy ra giữa nhiều quốc gia, gây khó khăn cho việc dẫn độ tội phạm.
- Một số quốc gia có thể từ chối hợp tác điều tra vì khác biệt về luật pháp hoặc xung đột lợi ích.

• **Bằng chứng số và điều tra tội phạm mạng**

- Để chứng cứ số được công nhận trước tòa, cần đảm bảo quy trình thu thập, lưu trữ và phân tích hợp lệ.

• **Tính liên ngành của tội phạm mạng**

- Nó liên quan đến nhiều lĩnh vực: tội phạm học, xã hội học, quan hệ quốc tế, khoa học máy tính, tâm lý học, an ninh mạng, kinh tế học, v.v.

- **Tỷ lệ báo cáo thấp**

- Doanh nghiệp e ngại báo cáo vi phạm vì lo ngại ảnh hưởng đến danh tiếng.
- Nạn nhân cá nhân có thể không biết cách báo cáo hoặc sợ hậu quả tâm lý.

Tất cả những yếu tố trên làm cho tội phạm mạng trở thành một vấn đề phức tạp, khó kiểm soát và đòi hỏi sự hợp tác toàn cầu để đối phó. Trong các bài học tiếp theo, chúng ta sẽ đi sâu vào từng khía cạnh này.

1.2. Các loại mối đe dọa an ninh mạng

☞ Theo báo cáo của Cơ quan An ninh mạng Liên minh Châu Âu (ENISA), các mối đe dọa phổ biến bao gồm:

1.2.1. Ransomware

- ♦ Mô tả: Mã độc tống tiền, mã hóa dữ liệu và yêu cầu nạn nhân trả tiền chuộc để lấy lại quyền truy cập.
- ♦ Ví dụ: WannaCry (2017) làm tê liệt hàng nghìn tổ chức trên toàn cầu.

1.2.2. Malware (phần mềm độc hại)

- ♦ Mô tả: Phần mềm gây hại, xâm nhập hệ thống để đánh cắp thông tin, gián điệp, hoặc phá hoại.
- ♦ Các loại:
 - Virus: Lây nhiễm từ tệp tin này sang tệp tin khác.
 - Worms: Tự sao chép và lây lan trong hệ thống mạng.
 - Trojan: Ẩn dưới dạng phần mềm hợp pháp để đánh cắp dữ liệu.
 - Spyware: Gián điệp thu thập thông tin mà không có sự cho phép.

1.2.3. Cryptojacking

- ♦ Mô tả: Tội phạm mạng lén cài đặt phần mềm khai thác tiền điện tử trên máy tính hoặc thiết bị của nạn nhân.
- ♦ Dấu hiệu nhận biết: Máy tính bị chậm bất thường, quạt CPU hoạt động mạnh hơn bình thường.

1.2.4. Tấn công email (phishing, spear phishing, business email compromise - BEC)

- ♦ Phishing: Email giả mạo yêu cầu cung cấp thông tin cá nhân hoặc nhấp vào liên kết độc hại.
- ♦ Spear Phishing: Nhắm mục tiêu cụ thể, thường là cá nhân trong tổ chức.
- ♦ BEC: Giả danh giám đốc hoặc đối tác yêu cầu chuyển tiền gấp.

1.2.5. Mối đe dọa đối với dữ liệu

- ♦ Mất dữ liệu: Do tấn công, lỗi hệ thống hoặc nhân viên vô tình xóa.
- ♦ Rò rỉ dữ liệu: Dữ liệu bị đánh cắp hoặc công khai do lỗ hổng bảo mật.

1.2.6. Tấn Công Từ Chối Dịch Vụ (Ddos)

- ♦ Mô tả: Hacker gửi lượng lớn truy vấn đến máy chủ, làm tê liệt hệ thống.
- ♦ Ví dụ: Tấn công DDoS vào GitHub năm 2018 với lưu lượng 1,3Tbps.

1.2.7. Thông tin sai lệch (disinformation, misinformation)

- ♦ Disinformation: Có ý lan truyền thông tin sai lệch để thao túng công chúng.
- ♦ Misinformation: Thông tin sai lệch nhưng không có chủ ý xấu.

- ◆ Tác động: Ảnh hưởng đến bầu cử, uy tín cá nhân/ doanh nghiệp.

1.3. Phân loại tội phạm mạng

❖ **Tội phạm mạng được chia thành hai nhóm chính:**

1.3.1. Cyber-dependent crimes (tội phạm mạng phụ thuộc công nghệ)

- ◆ Mô tả: Tội phạm chỉ có thể thực hiện thông qua công nghệ.
- ◆ Ví dụ:
 - Hacking (Tấn công hệ thống)
 - Phát tán mã độc
 - DDoS

1.3.2. Cyber-enabled crimes (tội phạm mạng được hỗ trợ bởi công nghệ)

- ◆ Mô tả: Tội phạm truyền thống nhưng trở nên nguy hiểm hơn nhờ công nghệ.
- ◆ Ví dụ:
 - Gian lận tài chính trực tuyến (Online Fraud)
 - Lừa đảo tình cảm (Romance Scam)
 - Buôn bán dữ liệu cá nhân

1.4. Rủi ro an toàn trên mạng xã hội

❖ **Tội phạm lợi dụng mạng xã hội để thực hiện hành vi xấu:**

1.4.1. Nội dung gây hại (harmful content)

- ◆ Nội dung có thể không vi phạm pháp luật nhưng gây tác động tiêu cực (khuyến khích rối loạn ăn uống, kích động bạo lực, thù hận, hoặc **tự sát**).
- ◆ Tác động tiêu cực đến trẻ em và thanh thiếu niên.

1.4.2. Quấy rối trực tuyến (cyberbullying & cyberstalking)

- ◆ Cyberbullying: Lăng mạ, đe dọa trên mạng.
- ◆ Cyberstalking: Theo dõi, gửi tin nhắn quấy rối liên tục.

1.4.3. Tấn công hội đồng (trolling & virtual mobbing)

- ◆ Trolling: Đăng bình luận khiêu khích, lăng mạ.
- ◆ Virtual Mobbing: Một nhóm người tấn công trực tuyến vào một cá nhân.

1.4.4. Lạm dụng trẻ em trực tuyến (online child exploitation & grooming)

- ◆ Grooming: Dụ dỗ trẻ em thực hiện hành vi nguy hiểm (gửi ảnh, gặp mặt trực tiếp).
- ◆ Nội dung bất hợp pháp liên quan đến trẻ em.

1.5. Lừa đảo trực tuyến (cyber-enabled fraud)

1.5.1. Lừa đảo tài chính (financial fraud)

- ◆ Lấy cắp thông tin cá nhân để mở tài khoản ngân hàng, vay tín dụng.

- ◆ Giả danh ngân hàng, yêu cầu nạn nhân cung cấp thông tin.

1.5.2. Lừa đảo tình cảm (romance scam & catfishing)

- ◆ Catfishing: Giả danh người khác trên mạng để lừa tình hoặc tiền.
- ◆ Romance Scam: Dụ dỗ nạn nhân chuyển tiền bằng cách giả vờ yêu đương.

1.5.3. Lừa đảo đầu tư & lừa đảo ngân hàng

- ◆ Đầu tư giả mạo: Kêu gọi đầu tư vào dự án không có thật.
- ◆ Lừa đảo ngân hàng: Chuyển khoản giả mạo, lấy cắp thông tin tài khoản.

1.5.4. Xâm phạm sở hữu trí tuệ (intellectual property fraud)

- ◆ Làm giả hàng hóa (giày, túi, đồng hồ).
- ◆ Truyền phát phim, trận đấu thể thao trái phép.

Trung Thu Miracle

II. TỔNG QUAN VỀ YÊU TỐ CON NGƯỜI TRONG TỘI PHẠM MẠNG

2.1. Tội phạm mạng

◆ Tại sao tội phạm xảy ra?

- Tại sao tội phạm mạng xảy ra?
- Động cơ, mục tiêu và quá trình ra quyết định của tội phạm mạng là gì?
- Các yếu tố tạo điều kiện cho tội phạm mạng diễn ra?
- Ai là nạn nhân tiềm năng và tại sao họ dễ bị tấn công?
- Những rào cản con người trong việc chống lại tội phạm mạng là gì?

◆ Góc độ nạn nhân:

- Hành vi của cá nhân trước nguy cơ tội phạm
- Ai có nguy cơ trở thành nạn nhân?
- Phản ứng của nạn nhân trước hành vi xâm phạm
- Những hạn chế con người gặp phải trong việc chống lại tội phạm mạng

◆ Góc độ pháp luật:

- Cơ chế hình thành luật pháp
- Quy luật xã hội và sự thay đổi của luật theo thời gian
- Tội phạm mạng có thể bị ảnh hưởng bởi nhận thức và quan điểm xã hội

2.2. Mối quan hệ giữa các thực thể trong môi trường tội phạm mạng

◆ Ba thực thể chính:

- Kẻ tấn công (Attacker): Động cơ, mục tiêu, phương thức hoạt động
- Nạn nhân (Victim): Đặc điểm dễ bị tổn thương, phản ứng, hành vi
- Cơ quan thực thi pháp luật (Law Enforcement): Những thách thức trong việc đối phó với tội phạm mạng

2.3. Động cơ phạm tội mạng

◆ Kẻ tấn công tham gia vào tội phạm mạng vì lý do gì?

- Tiền bạc (tấn công ransomware, lừa đảo tài chính)
- Chính trị (tấn công mạng do động cơ ý thức hệ)
- Tò mò, thử nghiệm năng lực bản thân (hacker tân binh)
- Lý do cá nhân (trả thù, cạnh tranh)

◆ Sự liên kết với tâm lý học:

- Tội phạm mạng không chỉ có động cơ kinh tế mà còn liên quan đến tâm lý con người và xã hội

2.4. Tâm lý nạn nhân và sự dễ tổn thương

◆ Những đặc điểm làm tăng nguy cơ bị tấn công:

- Thiếu hiểu biết về an toàn thông tin
- Niềm tin dễ bị thao túng (ví dụ: lừa đảo tình cảm)
- Tính cách dễ tổn thương (cô đơn, tìm kiếm sự công nhận)

- Không có thói quen bảo vệ tài khoản và dữ liệu cá nhân

◆ **Phản ứng của nạn nhân:**

- Hoảng loạn, mất kiểm soát
- Chấp nhận mất mát vì sợ hãi hoặc xấu hổ
- Không báo cáo hoặc không biết cách phản ứng

2.5. Hạn chế của cơ quan thực thi pháp luật trong xử lý tội phạm mạng

◆ **Những thách thức:**

- Tội phạm mạng có thể hoạt động xuyên biên giới
- Thiếu nguồn lực và chuyên môn về kỹ thuật số
- Rào cản pháp lý trong việc truy vết và xử lý tội phạm

2.6. Sự hạn chế trong nhận thức & ra quyết định của con người

◆ **Lý thuyết về tính duy lý hạn chế (Bounded rationality):**

- Con người không luôn đưa ra quyết định lý trí
- Hạn chế về nhận thức, thông tin và thời gian
- Ứng dụng trong việc hiểu hành vi của tội phạm, nạn nhân và cơ quan thực thi pháp luật

◆ **Các yếu tố tâm lý ảnh hưởng đến quyết định:**

- Thiên vị nhận thức (Cognitive biases): Định kiến, nhận thức sai lệch
- Heuristics (Quy tắc ngón tay cái): Quyết định dựa trên mô thức quen thuộc, không suy nghĩ thấu đáo
- Xu hướng duy trì hiện trạng (Status quo bias): Không muốn thay đổi do sự quen thuộc
- Ảnh hưởng của cách diễn đạt (Framing effect): Quyết định bị ảnh hưởng bởi cách vấn đề được trình bày

◆ **Các yếu tố rủi ro và nhận thức rủi ro:**

- Con người phản ứng khác nhau với các tình huống không chắc chắn
- Có xu hướng đánh giá thấp rủi ro liên quan đến công nghệ
- Hành vi cá nhân ảnh hưởng đến mức độ dễ bị tấn công

2.7. Ảnh hưởng của tính cách đối với tội phạm mạng

◆ **Mô hình Big Five (OCEAN) và tội phạm mạng:**

- Openness (Cởi mở): Người cởi mở cao có thể thích thử nghiệm công nghệ mới, nhưng điều này cũng khiến họ dễ gặp rủi ro bảo mật.
- Conscientiousness (Tận tâm): Người tận tâm thấp dễ có hành vi bất cẩn, như dùng mật khẩu yếu, không cập nhật phần mềm.
- Extraversion (Hướng ngoại): Người hướng ngoại dễ bị lừa qua mạng xã hội do họ có xu hướng tin tưởng người khác nhiều hơn.
- Agreeableness (Dễ chịu): Những người dễ chịu cao dễ bị thao túng cảm xúc, đặc biệt là trong các vụ lừa đảo tình cảm (romance scam).
- Neuroticism (Bất ổn cảm xúc): Những người này có thể phản ứng mạnh mẽ hơn với các cuộc tấn công mạng, dễ hoảng loạn hoặc đưa ra quyết định sai lầm.

◆ **Dark Triad (Bộ ba đen tối) và tội phạm mạng:**

- Machiavellianism (Chủ nghĩa mưu mô): Những kẻ lừa đảo mạng thường tinh ranh, giỏi thao túng và không quan tâm đến đạo đức.
- Narcissism (Tự ái): Những hacker hoặc tội phạm mạng có thể phạm tội vì muốn khẳng định bản thân hoặc thể hiện quyền lực.
- Psychopathy (Rối loạn nhân cách chống đối xã hội): Những người này không có cảm giác tội lỗi khi gây hại cho người khác, dễ thực hiện các hành vi phạm tội nguy hiểm.

2.8. Góc nhìn văn hóa trong tội phạm mạng

◆ **Sáu chiều văn hóa ảnh hưởng đến tội phạm mạng:**

- Khoảng cách quyền lực (Power Distance): Chỉ mức độ mà các cá nhân trong một xã hội chấp nhận sự phân bổ quyền lực không đồng đều. Ví dụ các nước Châu Á có thể có cấu trúc phân cấp chặt chẽ, với những kẻ đứng đầu chỉ huy và điều phối hoạt động lừa đảo hơn Châu Âu.
- Chủ nghĩa cá nhân vs. tập thể (Individualism vs. Collectivism): Phản ánh mức độ mà cá nhân ưu tiên lợi ích cá nhân hay lợi ích của nhóm.
- Tránh sự bất định (Uncertainty Avoidance): Chỉ mức độ mà một xã hội cảm thấy không thoải mái với sự không chắc chắn và rủi ro. Ở các nước có chỉ số tránh rủi ro thấp, người dùng có thể dễ dàng chấp nhận công nghệ mới nhưng cũng dễ rơi vào các mô hình lừa đảo mạo hiểm như đầu tư tiền mã hóa lừa đảo.
- Nam tính vs. nữ tính (Masculinity vs. Femininity): Chỉ mức độ mà một xã hội đề cao các giá trị nam tính (cạnh tranh, thành công, quyền lực) so với giá trị nữ tính (hợp tác, quan tâm, bình đẳng). Ví dụ: Ở các nền văn hóa nam tính cao, tội phạm mạng có thể khai thác tham vọng cá nhân, ham muôn thành công (như lừa đảo đầu tư tài chính).
- Định hướng dài hạn vs. ngắn hạn (Long-term vs. Short-term orientation): Đo lường cách một nền văn hóa nhìn nhận thời gian, ưu tiên các giá trị truyền thống hay đổi mới để phát triển trong tương lai. Ví dụ, xã hội có định hướng ngắn hạn có thể có phản ứng nhanh với các mối đe dọa nhưng cũng dễ bị lừa bởi các trò gian lận mang lại lợi nhuận nhanh.
- Sự hưởng thụ vs. kiềm chế (Indulgence vs. Restraint): Phản ánh mức độ mà một xã hội cho phép thỏa mãn các nhu cầu cá nhân như vui chơi, hưởng thụ, tiêu dùng. Ví dụ: Ở các nước có mức độ hưởng thụ cao, tội phạm mạng có thể lợi dụng tâm lý ham vui, thích thử nghiệm (ví dụ: lừa đảo qua trò chơi trực tuyến, trang web cá cược giả mạo).

2.9. Văn hóa an ninh trong doanh nghiệp

◆ **Yếu tố con người trong bảo mật tổ chức:**

- Nhận thức và thái độ của nhân viên đối với bảo mật
- Truyền thông rủi ro trong nội bộ công ty
- Tuân thủ quy tắc và chính sách bảo mật
- Trách nhiệm cá nhân đối với an toàn thông tin

◆ **Tầm quan trọng của đào tạo nhận thức bảo mật:**

- Giáo dục giúp giảm nguy cơ tấn công mạng
- Nhân viên có hiểu biết sẽ bảo vệ dữ liệu tổ chức tốt hơn
- Văn hóa an ninh mạnh giúp ngăn chặn ransomware và các cuộc tấn công có chủ đích

2.10. Kết luận

- Tội phạm mạng không chỉ là vấn đề công nghệ mà còn là vấn đề con người.
- Hiểu rõ tâm lý của kẻ tấn công, nạn nhân và cơ quan thực thi pháp luật giúp tăng cường khả năng đối phó.

III. PHÂN TÍCH SÂU VỀ CÁC THỰC THỂ TRONG TỘI PHẠM MẠNG

Tội phạm mạng không chỉ là ván đề kỹ thuật mà còn liên quan chặt chẽ đến các yếu tố con người. Trong bối cảnh này, có ba nhóm chính tham gia vào tội phạm mạng:

1. Kẻ tấn công (Attackers)
2. Nạn nhân (Victims)
3. Cơ quan thực thi pháp luật (Law Enforcement)

Mặc dù có thể xem xét thêm các yếu tố xã hội rộng lớn hơn, nhưng cách tiếp cận này giúp chúng ta tập trung vào ba thực thể cốt lõi.

3.1. Động cơ và lợi ích của kẻ tấn công

Một trong những câu hỏi quan trọng trong tội phạm học là: Tại sao tội phạm, đặc biệt là tội phạm mạng, xảy ra?

- ◆ Phân biệt động cơ và lợi ích:
 - Lợi ích (Incentives): Yếu tố bên ngoài thúc đẩy hành vi phạm tội, chẳng hạn như tiền bạc, quyền lực hoặc sự công nhận.
 - Động cơ (Motivations): Yếu tố nội tại xuất phát từ tâm lý cá nhân, như niềm tin, trí tò mò, hoặc mong muốn thách thức bản thân.

PHÂN LOẠI KẺ TẤN CÔNG DỰA TRÊN ĐỘNG CƠ

Loại kẻ tấn công	Động cơ & lợi ích chính	Ví dụ hành vi
Tội phạm có tổ chức (Organized cybercriminals, như nhóm ransomware)	Chủ yếu là tiền bạc, kiếm lợi nhuận từ tống tiền hoặc đánh cắp dữ liệu.	Ransomware, gian lận tài chính, bán thông tin cá nhân.
Hacktivists (Tin tức hoạt động vì lý tưởng)	Động cơ chính trị, xã hội, muốn phản đối hoặc thay đổi một vấn đề cụ thể.	Đánh sập website chính phủ, rò rỉ dữ liệu bí mật.
Cyberpunks, Script Kiddies, Novices	Tò mò, thử thách trí tuệ, khẳng định bản thân. Có thể muốn gây ấn tượng với cộng đồng mạng.	Hack trang web, khai thác lỗ hổng bảo mật, làm rò rỉ dữ liệu.
Nhóm hacker do chính phủ tài trợ (Nation-state actors)	Kết hợp lợi ích bên ngoài (lương, tài trợ) và động cơ lý tưởng (ý thức hệ).	Tấn công gián điệp, phá hoại hệ thống nước ngoài.
Cá nhân thực hiện tấn công vì trả thù (Revenge, Message Sending)	Muốn trả thù cá nhân, tổ chức hoặc gửi thông điệp cảnh báo.	DDoS, phá hoại website, xâm nhập hệ thống đối thủ.

- ◆ Nhận định quan trọng:
 - Việc xác định động cơ và lợi ích của kẻ tấn công giúp chúng ta xây dựng chiến lược phòng chống và giảm thiểu tội phạm mạng hiệu quả hơn.
 - Ví dụ, các nhóm ransomware bị thúc đẩy bởi lợi nhuận => cần chặn nguồn thanh toán để giảm động lực của họ.
- ◆ So sánh giữa tội phạm truyền thống và tội phạm mạng
 - **Điểm tương đồng:**
 - Tội phạm mạng cũng có gắng giảm thiểu rủi ro bị bắt giữ, giống như tội phạm truyền thống.

- Nạn nhân của tội phạm mạng có nhu cầu tương tự như nạn nhân của tội phạm truyền thống: hỗ trợ cảm xúc, tài chính, thông tin.
- **Khác biệt:**
 - Nhiều trường hợp, nạn nhân không được cơ quan thực thi pháp luật xem là nạn nhân thực sự, dẫn đến việc điều tra không được tiến hành.

3.2. Nạn nhân (victims) trong tội phạm mạng

Câu hỏi đặt ra: Ai có nguy cơ trở thành nạn nhân và họ cần hỗ trợ gì?

- ◆ **Một số đặc điểm làm tăng nguy cơ bị lừa đảo, tấn công mạng:**
 1. Người lớn tuổi – Dễ bị lừa đảo tài chính do ít kinh nghiệm với công nghệ.
 2. Người có tính cách bốc đồng, thích rủi ro (Impulsive & Sensation-seeking) – Dễ bị dụ dỗ bởi các khoản đầu tư lãi suất cao hoặc các chiêu trò lừa đảo.
 3. Người có thói quen trực tuyến rủi ro cao – Như sử dụng mật khẩu yếu, truy cập các trang web không an toàn, tải phần mềm lậu.
- ◆ **Nhu cầu của nạn nhân tội phạm mạng (giống với nạn nhân tội phạm truyền thống) sau khi sự kiện xảy ra:**
 - Cảm xúc (Emotional Support): Giảm thiểu sự hoang mang, sợ hãi sau khi bị tấn công.
 - Tài chính (Financial Support): Hỗ trợ thiệt hại kinh tế do lừa đảo, đánh cắp dữ liệu.
 - Thông tin (Informational Support): Hướng dẫn cách tự bảo vệ, phục hồi dữ liệu, báo cáo sự cố.
- ◆ **Nhận định quan trọng:**
 - Giáo dục nhận thức an toàn mạng là chìa khóa để giảm số lượng nạn nhân.
 - Tạo các kênh hỗ trợ rõ ràng để nạn nhân biết nơi báo cáo và tìm kiếm trợ giúp.

3.3. Cơ quan thực thi pháp luật (law enforcement) và những thách thức

- ◆ **Mối liên hệ giữa nạn nhân và cơ quan thực thi pháp luật:**
 - Nhiều nạn nhân không báo cáo tội phạm mạng, dẫn đến sự thiếu thông tin của cơ quan thực thi pháp luật.
 - Một số lý do chính:
 - Không biết báo cáo ở đâu hoặc có quá nhiều kênh thông tin gây nhầm lẫn.
 - Lo ngại rằng cảnh sát không coi trọng các tội phạm mạng.
- ◆ **Những thách thức của cơ quan thực thi pháp luật:**
 - Áp lực gia tăng: Khi số lượng tội phạm mạng tăng nhanh, cảnh sát gặp khó khăn trong việc xử lý khối lượng vụ án lớn.
 - Thiếu kỹ năng chuyên môn: Nhiều sĩ quan chưa được đào tạo chuyên sâu về tội phạm mạng.
 - Thiếu tài nguyên: Ngân sách dành cho đơn vị chống tội phạm mạng không đủ so với quy mô của vấn đề.
- ◆ **Giải pháp tiềm năng:**
 - Đào tạo chuyên môn cho cảnh sát để họ có thể điều tra và xử lý hiệu quả hơn.
 - Cải thiện hệ thống báo cáo và hỗ trợ nạn nhân, giúp họ tiếp cận thông tin dễ dàng hơn.
 - Hợp tác chặt chẽ hơn giữa cơ quan thực thi pháp luật, doanh nghiệp và cộng đồng để phát hiện và ngăn chặn tội phạm mạng sớm hơn.

3.4. Kết luận: làm sao để giảm tội phạm mạng?

◆ **Bước 1: Hiểu rõ động cơ và lợi ích của kẻ tấn công.**

- Ngăn chặn nguồn tài chính cho các nhóm tội phạm có tổ chức.
- Giảm bớt yếu tố kích thích trí tò mò của hacker non trẻ bằng cách tạo ra các sân chơi hợp pháp như các chương trình bug bounty.

◆ **Bước 2: Bảo vệ nhóm có nguy cơ cao khỏi trở thành nạn nhân.**

- Cung cấp giáo dục an toàn mạng, đặc biệt cho người lớn tuổi và những người có hành vi rủi ro cao.
- Xây dựng hệ thống báo cáo tội phạm mạng đơn giản, minh bạch.

◆ **Bước 3: Nâng cao năng lực thực thi pháp luật.**

- Tăng cường đào tạo chuyên sâu về tội phạm mạng.
 - Phân bổ nguồn lực hợp lý để giải quyết các vụ án tội phạm mạng nhanh hơn.
- ◆ **Câu hỏi đặt ra:**
- Làm thế nào để cộng đồng, doanh nghiệp, và chính phủ hợp tác tốt hơn trong việc ngăn chặn tội phạm mạng?
 - Liệu có cách nào giúp giảm động lực phạm tội của hacker ngay từ ban đầu?

Trung Thu Miracle

IV. SOCIAL ENGINEERING: TÂM LÝ HỌC & CÁCH THỨC TẤN CÔNG

4.1. Social engineering là gì?

♦ Social Engineering (Kỹ thuật thao túng tâm lý) là việc sử dụng lừa dối và thao túng con người để khiến họ tiết lộ thông tin nhạy cảm hoặc thực hiện hành động có lợi cho kẻ tấn công. Đây không phải là tấn công vào hệ thống công nghệ mà tấn công vào tâm lý con người – mắt xích yếu nhất trong bảo mật.

♦ Ví dụ:

- Phishing (Lừa đảo qua email): Email giả mạo ngân hàng yêu cầu cập nhật mật khẩu.
- Vishing (Lừa đảo qua điện thoại): Kẻ tấn công giả danh nhân viên IT để lấy thông tin đăng nhập.
- Smishing (Lừa đảo qua tin nhắn SMS): Tin nhắn giả mạo yêu cầu bấm vào đường link độc hại.
- Whaling (Nhắm vào lãnh đạo cấp cao): Kẻ tấn công giả danh CEO yêu cầu chuyển tiền.
- Catfishing (Giả mạo danh tính trên mạng xã hội): Tạo tài khoản giả mạo để lừa đảo tình cảm hoặc chiếm đoạt tài sản.
- CEO Fraud: Mạo danh giám đốc tài chính yêu cầu kế toán chuyển tiền.
- ♦ Theo FBI, 80-90% các vụ vi phạm bảo mật bắt nguồn từ Social Engineering!

4.2. Các hiệu ứng tâm lý mà kẻ tấn công sử dụng

☞ **Những hiệu ứng này khai thác điểm yếu trong nhận thức, cảm xúc và hành vi của con người:**

4.2.1. Hiệu ứng quyền uy (authority bias)

♦ Nguyên lý: Con người có xu hướng tuân theo chỉ dẫn từ những người có vẻ "có quyền lực" (như lãnh đạo, chuyên gia, quan chức).

♦ Thí nghiệm Milgram (1960s):

- Người tham gia được yêu cầu gây sốc điện cho một "học viên" (thực tế là diễn viên).
- Dù biết học viên đang "chịu đau đớn", 65% người tham gia vẫn làm theo lệnh của nhà nghiên cứu.
- Kết luận: Con người dễ bị chi phối bởi quyền uy, ngay cả khi điều đó đi ngược lại đạo đức cá nhân.

♦ Ứng dụng trong tấn công mạng:

- CEO Fraud: Email giả danh giám đốc yêu cầu chuyển tiền gấp.
- Fake IT Support: Hacker giả danh nhân viên IT yêu cầu mật khẩu.

4.2.2. Sự tự tin quá mức (overconfidence bias) và thiên kiến lạc quan (Optimism Bias)

♦ Nguyên lý: Con người thường đánh giá quá cao khả năng bảo vệ bản thân khỏi rủi ro hay tin rằng rủi ro xấu sẽ không xảy ra với mình.

♦ Ví dụ thực tế: Hỏi 100 tài xế: "Bạn lái xe giỏi hơn trung bình không?" → 70% trả lời "Có" (dù thực tế chỉ có 50% giỏi hơn mức trung bình).

♦ Ứng dụng trong tấn công mạng:

- Nạn nhân tin rằng họ không thể bị lừa, dẫn đến mất cảnh giác.
- Hacker tạo ra email lừa đảo với nội dung "Cảnh báo bảo mật", nạn nhân tự tin rằng họ đủ hiểu biết để xử lý nhưng lại vô tình cung cấp thông tin cho hacker.

4.2.3. Hiệu ứng sẵn có (availability bias)

- ◆ Nguyên lý: Con người có xu hướng dựa vào thông tin có sẵn trong tâm trí hơn là tìm hiểu kỹ lưỡng.
- ◆ Ví dụ thực tế: Khi nghe tin về một vụ tai nạn máy bay, nhiều người sợ đi máy bay hơn dù xác suất xảy ra tai nạn thấp hơn ô tô rất nhiều.
- ◆ Ứng dụng trong tấn công mạng: Hacker gieo thông tin trước: Một người giả danh nhân viên IT nhắc về lỗi phần mềm → Khi hacker gọi điện yêu cầu cung cấp mật khẩu, nạn nhân dễ tin hơn.

4.2.4. Cam Kết và Tính Nhất Quán (Commitment & Consistency Bias)

- ◆ Nguyên lý: Con người có xu hướng hành động nhất quán với những gì họ đã làm trước đó.
- ◆ Ví dụ thực tế: Một người tuyên bố trên Facebook rằng họ sẽ bỏ thuốc lá → Họ có xu hướng kiên trì hơn để tránh mất uy tín.
- ◆ Ứng dụng trong tấn công mạng: Hacker tạo dựng lòng tin trước (ví dụ: hỏi han nhẹ nhàng, tạo môi quan hệ) → Khi đã có lòng tin, nạn nhân khó từ chối yêu cầu sau này (như cung cấp mật khẩu).

4.2.5. Hiệu ứng khan hiếm (scarcity bias)

- ◆ Nguyên lý: Con người có xu hướng coi trọng những thứ hiếm hoi hơn.
- ◆ Ví dụ thực tế: "Chỉ còn 2 vé concert!" → Mọi người đặt mua ngay mà không suy nghĩ nhiều.
- ◆ Ứng dụng trong tấn công mạng:
 - Ransomware: Hacker đếm ngược thời gian, yêu cầu trả tiền chuộc trong 24 giờ nếu không dữ liệu sẽ bị xóa vĩnh viễn.
 - Lừa đảo mua sắm: "Chỉ còn 3 suất giảm giá, hãy nhập thông tin thẻ ngay!"

4.2.6. Tâm lý bầy đàn (herd mentality & social proof)

- ◆ Nguyên lý: Con người thường làm theo số đông, đặc biệt trong tình huống không chắc chắn.
- ◆ Ví dụ thực tế: Một nhà hàng có đông người xếp hàng → Người khác cũng muốn vào thử vì nghĩ rằng "chắc chắn ngon".
- ◆ Ứng dụng trong tấn công mạng:
 - Hacker giả mạo email đồng nghiệp: "Tất cả nhân viên khác đã hoàn thành khảo sát bảo mật, chỉ còn bạn chưa làm."
 - Bùng nổ tiền ảo (crypto scams): "Ai cũng đang đầu tư, bạn không muốn bỏ lỡ chứ?"

4.2.7. Hiệu ứng đáp lễ (reciprocity bias)

- ◆ Nguyên lý: Con người có xu hướng trả ơn khi nhận được sự giúp đỡ hoặc quà tặng.
- ◆ Ví dụ thực tế: Một nhân viên mời bạn ly cà phê, bạn cảm thấy có nghĩa vụ giúp đỡ họ sau này.
- ◆ Ứng dụng trong tấn công mạng:
 - Hacker gửi email "quà tặng": "Bạn đã trúng thưởng, hãy nhấp vào đây để nhận quà!"
 - Lừa đảo qua mạng xã hội: Người lạ gửi tiền, sau đó nhờ bạn giúp lại bằng cách chuyển khoản số tiền lớn hơn.

4.3. Xây dựng sự tin tưởng và quan hệ với mục tiêu

4.3.1. Kỹ thuật xây dựng sự tin tưởng và quan hệ với mục tiêu

- ◆ Lắng nghe nhiều hơn nói: Một kẻ tấn công xã hội (social engineer) luôn chú trọng vào việc lắng nghe đôi phương nhiều hơn để thu thập thông tin quan trọng.
- ◆ Xác nhận quan điểm của mục tiêu: Khi xác nhận những quan điểm cá nhân của mục tiêu, đặc biệt là quan điểm về chính họ, social engineer có thể thao túng bản ngã (ego) và giá trị bản thân của mục tiêu.
- ◆ Dẫn dắt mục tiêu đến giải pháp có lợi cho kẻ tấn công: Bằng cách điều hướng cuộc trò chuyện, social engineer có thể khiến mục tiêu nghĩ rằng họ là người đưa ra giải pháp (mặc dù đó là giải pháp có lợi cho kẻ tấn công).
- ◆ Reverse social engineering (kỹ thuật đảo ngược): Tạo dựng tình huống để mục tiêu tự tìm đến kẻ tấn công mà không hề nghi ngờ, ví dụ: giả vờ gặp sự cố kỹ thuật để mục tiêu chủ động tìm kiếm sự trợ giúp từ kẻ tấn công.
- ◆ Tận dụng sự cuốn hút tự nhiên: Một số social engineer có sức hút bẩm sinh, biết cách thể hiện sự tự tin hoặc đóng vai người có địa vị cao để thu hút và ảnh hưởng lên người khác.
- ◆ Giữ sự mơ hồ và ẩn giấu động cơ thật: Social engineer không bao giờ để lộ ý định thật sự của họ, mà thay vào đó tỏ ra lạnh lùng, trung lập hoặc thể hiện sự quan tâm một cách tinh tế để không gây nghi ngờ.

4.3.2. Chiến lược xây dựng sự thân quen và tin tưởng

- ◆ Tiết lộ thông tin cá nhân để kích hoạt quy tắc có qua có lại: Khi một người chia sẻ thông tin cá nhân, mục tiêu có xu hướng đáp lại bằng cách cung cấp thêm thông tin về bản thân họ.
- ◆ Tạo sự quen thuộc thông qua giao tiếp liên tục: Khi mục tiêu giao tiếp nhiều lần với một người, họ dần cảm thấy tin tưởng hơn, ngay cả khi đó là một danh tính giả mạo.
- ◆ Giả tạo tình huống để tạo dựng mối quan hệ: Một social engineer có thể tạo ra một tình huống "trùng hợp", như một sự cố kỹ thuật, và xuất hiện đúng lúc để giúp đỡ, từ đó xây dựng lòng tin của mục tiêu.

4.3.3. Dựa trên những thông tin thật để tạo độ tin cậy

- ◆ Sử dụng các sự kiện thật để làm nền tảng cho lời nói dối: Một kẻ lừa đảo không tạo ra câu chuyện hoàn toàn bịa đặt, mà dựa trên những thông tin có thật để tăng tính thuyết phục.
- ◆ Tận dụng hiểu biết về chủ đề để làm cho cuộc hội thoại tự nhiên hơn: Nếu kẻ tấn công am hiểu về một lĩnh vực, họ có thể đưa ra những chi tiết chính xác để khiến mục tiêu tin rằng họ thực sự là chuyên gia hoặc có liên quan đến lĩnh vực đó.

4.3.4. Sử dụng ngôn ngữ cơ thể (body language) và giao tiếp phi ngôn ngữ

- ◆ Giao tiếp phi ngôn ngữ chiếm đến 60% tổng số tương tác giữa con người.
- ◆ Các yếu tố quan trọng trong giao tiếp phi ngôn ngữ:
 - Biểu cảm khuôn mặt (Micro-expressions): Những biểu cảm thoáng qua có thể tiết lộ trạng thái cảm xúc thật.
 - Chuyển động cơ thể (Kinesics): Dáng điệu, tư thế, cử chỉ có thể phản ánh cảm xúc và mức độ thoải mái của một người.
 - Giọng điệu và âm lượng (Paralinguistics): Giọng nói thay đổi có thể tiết lộ sự lo lắng hoặc thiếu thành thật.
 - Hành vi phòng vệ: Khi một người cảm thấy không thoải mái, họ có xu hướng khoanh tay, che chắn cơ thể, hoặc tránh giao tiếp bằng mắt.

4.3.5. Kỹ thuật đọc và tái tạo ngôn ngữ cơ thể để ảnh hưởng mục tiêu

- ◆ Isopraxis (Hiệu ứng gương): Bắt chước cách nói chuyện, nhịp thở, và cử chỉ của mục tiêu để tạo sự gần gũi và kết nối tiềm thức.
- ◆ Sử dụng các rào cản để thể hiện sự phòng thủ: Khi một người cảm thấy bị đe dọa, họ có thể tạo rào cản giữa họ và người khác, ví dụ như đặt một vật gì đó trước mặt hoặc khoanh tay.
- ◆ Dấu hiệu "chống trọng lực" (Gravity-defying behaviors): Những người tự tin hoặc vui vẻ thường có xu hướng mở rộng cơ thể, giơ tay lên cao, trong khi người lo lắng hoặc thất vọng thường co rúm lại.

4.3.6. Các hình thức lừa đảo trực tuyến phổ biến

- ◆ Trolling: Đăng các bình luận gây tranh cãi nhằm kích động mâu thuẫn và khêu khích phản ứng từ người khác.
- ◆ Sock Puppetry: Tạo nhiều tài khoản giả mạo để tạo ra ấn tượng rằng nhiều người đang ủng hộ một quan điểm nào đó (ví dụ: đánh giá giả mạo).
- ◆ Astroturfing: Một dạng sock puppetry có tổ chức để thao túng dư luận chính trị hoặc tiếp thị.
- ◆ Phishing: Giả mạo để lấy thông tin cá nhân hoặc dữ liệu nhạy cảm.

4.3.7. Các lý thuyết về lừa dối và truyền thông

- ◆ Interpersonal Deception Theory: Kẻ nói dối vừa cố gắng đánh lừa vừa cố gắng tránh bị phát hiện, và điều chỉnh chiến thuật tùy theo phản ứng của đối phương.
- ◆ Prominence Interpretation Theory: Đánh giá mức độ đáng tin của một thông tin phụ thuộc vào nền tảng mà nó được đăng tải.
- ◆ Media Richness Theory: Phương tiện truyền thông càng "giàu" (tương tác đa chiều như video call, gấp mặt trực tiếp), thì càng khó để lừa đảo.
- ◆ Cognitive Load Theory: Lừa dối tạo ra áp lực nhận thức cao, điều này có thể được khai thác để phát hiện kẻ nói dối.

4.3.8. Hiệu quả của sự lừa dối và khả năng phát hiện nó

- ◆ Con người nói dối trung bình hai lần một ngày.
- ◆ 90% mọi người mong đợi người khác nói dối khi trực tuyến.
- ◆ Con người chỉ có khả năng phát hiện nói dối tốt hơn một chút so với ngẫu nhiên.
- ◆ Lừa dối hiệu quả có thể được cải thiện thông qua thực hành và động cơ phù hợp.
- ◆ Người ta có xu hướng tin tưởng người giúp đỡ họ và thích xác nhận những niềm tin, định kiến của bản thân.

4.4. Ba kỹ thuật thuyết phục của Aristotle để thao túng nạn nhân

Các hacker sử dụng 3 kỹ thuật thuyết phục của Aristotle để thao túng nạn nhân:

4.4.1. Logos – Sử dụng lý trí và logic

- ◆ Thuyết phục nạn nhân bằng dữ liệu, nghiên cứu, bằng chứng.
- ◆ Ví dụ: "Chúng tôi là ngân hàng XYZ, hệ thống phát hiện giao dịch lạ, vui lòng xác nhận tài khoản để tránh mất tiền."

4.4.2. Pathos – Đánh vào cảm xúc

- ◆ Kích thích cảm xúc lo lắng, sợ hãi, vui mừng, đồng cảm để thao túng.

- ◆ Ví dụ:
 - "Bạn đã trúng thưởng 10.000 USD, vui lòng nhập thông tin để nhận giải!"
 - "Tài khoản của bạn có dấu hiệu bị hack, vui lòng đăng nhập ngay để xác minh!"

4.4. 3. Ethos – Dùng uy tín & danh tiếng

- ◆ Giả danh người có quyền lực hoặc chuyên gia để tạo sự tin tưởng.
- ◆ Ví dụ:
 - "Tôi là nhân viên IT, vui lòng cung cấp mật khẩu để kiểm tra lỗi hệ thống."
 - "Tôi là nhân viên ngân hàng, cần xác minh tài khoản của anh/chị để bảo vệ tài sản."

4.5. Chu trình tấn công social engineering (theo Kevin Mitnick)

Social Engineering không diễn ra ngay lập tức mà có kế hoạch rõ ràng qua 4 bước:

❖ **Bước 1: Nghiên cứu mục tiêu (Reconnaissance)**

- ◆ Mục tiêu: Thu thập thông tin cá nhân/tổ chức để lên kế hoạch tấn công.
- ◆ Kỹ thuật thu thập dữ liệu:
 - OSINT (Open Source Intelligence): Sử dụng Google, LinkedIn, Facebook, WHOIS để thu thập thông tin.
 - Phân tích hành vi trên mạng xã hội: Sở thích, nơi làm việc, lịch trình công tác.
 - Xem xét dữ liệu công khai của tổ chức: Danh sách nhân viên, đối tác, sự kiện.
- ◆ Ví dụ thực tế: Một hacker có thể tìm thấy tên nhân viên IT trên LinkedIn, sau đó giả danh nhân viên IT để lừa nhân viên khác cung cấp thông tin đăng nhập.

❖ **Bước 2: Xây dựng lòng tin (Building Trust & Rapport)**

- ◆ Mục tiêu: Tạo mối quan hệ thân thiện để khiến nạn nhân cảm thấy tin tưởng.
- ◆ Kỹ thuật sử dụng:
 - Pretexting (Lập kịch bản giả mạo): Giả danh nhân viên IT, nhân viên ngân hàng, cảnh sát.
 - Sử dụng thông tin cá nhân thu thập được để tạo sự thân thuộc (VD: "Anh cũng thích xem bóng đá như tôi à?").
 - Tận dụng tâm lý con người:
 - Nguyên tắc quen thuộc: Gặp gỡ nhiều lần khiến nạn nhân tin tưởng.
 - Tâm lý giúp đỡ: Con người có xu hướng giúp đỡ người khác nếu được yêu cầu lịch sự.
 - Lấy lòng tin bằng khen ngợi: "Anh là chuyên gia trong lĩnh vực này, tôi rất ngưỡng mộ!"
- ◆ Ví dụ thực tế: Một hacker gọi điện cho nhân viên lễ tân, tự giới thiệu là "nhân viên IT mới" và yêu cầu cấp quyền truy cập hệ thống.

❖ **Bước 3: Khai thác thông tin (Elicitation & Exploitation)**

- ◆ Mục tiêu: Lừa nạn nhân cung cấp thông tin quan trọng một cách vô thức.
- ◆ Kỹ thuật sử dụng:

- Gợi chuyện gián tiếp: "Hệ thống bảo mật công ty có phức tạp không?"
 - Tạo tình huống khẩn cấp: "Tôi là nhân viên IT, có lỗi nghiêm trọng trên máy tính của anh, vui lòng cung cấp mật khẩu!"
 - Sử dụng kỹ thuật "Bánh Xe Thông Tin": Lấy từng mảnh thông tin nhỏ, sau đó ghép lại để tạo ra bức tranh lớn hơn.
- ◆ Ví dụ thực tế: Một hacker giả danh nhân viên ngân hàng gọi điện, hỏi về "số tài khoản để xác nhận giao dịch bất thường", sau đó tiếp tục hỏi về mã OTP.
-

➡ **Bước 4: Sử dụng thông tin đã có (Execution & Exploitation)**

- ◆ Mục tiêu: Sử dụng thông tin lấy được để thực hiện tấn công thực sự.
 - ◆ Ví dụ các cuộc tấn công có thể xảy ra:
 - Mạo danh nhân viên công ty để lừa đồng nghiệp cung cấp thông tin nhạy cảm.
 - Dùng email giả mạo để yêu cầu chuyển khoản (BEC - Business Email Compromise).
 - Sử dụng tài khoản đánh cắp để truy cập hệ thống công ty.
 - ◆ Ví dụ thực tế: Một hacker giả danh CEO gửi email yêu cầu kê toán chuyển khoản 100.000 USD đến tài khoản lừa đảo.
-

Minh họa qua một tình huống thực tế

Ví dụ sau đây minh họa cách một kẻ tấn công có thể khai thác tâm lý nạn nhân để thực hiện hành vi social engineering:

1. Kẻ tấn công gọi tên một người trong tổ chức bằng tên riêng (ví dụ: "Barry"), tạo ấn tượng rằng họ quen biết nhau.
2. Họ đề cập đến một cuộc trò chuyện cuối tuần, cho thấy mối quan hệ thân thiết hơn mức độ công việc thông thường.
3. Họ tạo ra một vấn đề giả định, chẳng hạn như cần gửi tài liệu gấp nhưng quên mất một trang quan trọng.
4. Họ đóng vai nạn nhân đang gấp khó khăn, thể hiện sự bối rối, lo lắng để kích thích lòng trắc ẩn của mục tiêu.
5. Họ không yêu cầu trực tiếp giải pháp mà để mục tiêu tự đề xuất, chẳng hạn như cho phép sử dụng USB để in tài liệu.
6. Kết quả: nạn nhân tự nguyện giúp đỡ bằng cách cắm USB vào máy tính, vô tình tải mã độc vào hệ thống.

✓ **Những yếu tố giúp thành công trong cuộc tấn công này:**

- Tận dụng cảm xúc của nạn nhân: Cảm giác tội lỗi, thương hại và mong muốn giúp đỡ.
 - Dùng ngôn ngữ phù hợp với ngữ cảnh: Thuật ngữ công việc, thái độ chuyên nghiệp.
 - Sử dụng trang phục, giọng nói, ngôn ngữ cơ thể phù hợp: Thể hiện sự lo lắng và khẩn cấp để tạo cảm giác chân thực.
 - Để nạn nhân tự quyết định giải pháp: Khi họ tự nghĩ ra giải pháp, họ sẽ ít nghi ngờ hơn.
-

4.6. Kết luận & bài học rút ra

- Social engineering dựa vào tâm lý con người nhiều hơn là công nghệ.

- Con người là mắt xích yếu nhất trong bảo mật: Tân công kỹ thuật có thể bị chặn, nhưng thao túng tâm lý thì khó đề phòng hơn.
- Nguyên tắc quan trọng để tự bảo vệ bản thân:
 - Kiểm tra danh tính trước khi làm theo yêu cầu của người lạ.
 - Không cắm USB hoặc mở file từ nguồn không xác minh.
 - Không để cảm xúc chi phối quyết định.
 - Nhận thức về kỹ thuật thao túng tâm lý để tránh trở thành nạn nhân.

● Social engineering là một trong những mối đe dọa nguy hiểm nhất trong an ninh mạng. Hiểu cách nó hoạt động giúp chúng ta tránh được những cạm bẫy tinh vi mà kẻ tấn công giăng ra.

Trung Thu Miracle

V. GIẢI PHÁP BẢO VỆ BẢN THÂN NHẰM PHÒNG CHỐNG SOCIAL ENGINEERING

- ◆ Nhận diện các dấu hiệu lừa đảo:
 - Email hoặc cuộc gọi yêu cầu cung cấp thông tin cá nhân.
 - Lời đe nghi quá hấp dẫn hoặc tình huống khẩn cấp.
 - Người gửi email có địa chỉ lạ, sai chính tả, hoặc giả mạo công ty.
 - ◆ Kiểm tra tính xác thực:
 - Không cung cấp thông tin cá nhân qua email, điện thoại.
 - Gọi lại số chính thức của công ty/ngân hàng để kiểm tra.
 - ◆ Đào tạo nhân viên:
 - Tổ chức các buổi huấn luyện về Social Engineering.
 - Kiểm tra định kỳ khả năng nhận diện lừa đảo.
 - ◆ Sử dụng bảo mật mạnh mẽ:
 - Kích hoạt xác thực hai yếu tố (2FA).
 - Không nhấp vào liên kết hoặc mở tệp đính kèm từ nguồn không xác định.
- 💡 Nhớ rằng, công nghệ có thể được bảo mật – nhưng con người thì dễ bị thao túng! 🚨
- 💡 An toàn trên không gian mạng là trách nhiệm của mỗi cá nhân. Hãy luôn tinh táo và chủ động bảo vệ mình! 🌟

VI. CÁC CÂU HỎI LIÊN QUAN ĐẾN SOCIAL ENGINEERING

Câu 1: Social engineering là gì?

- ◆ Kỹ thuật lừa đảo tâm lý nhằm thao túng con người để lấy thông tin nhạy cảm mà không cần xâm nhập hệ thống kỹ thuật.

💡 Ví dụ thực tế:

- ✓ Giả danh IT support để yêu cầu nhân viên cung cấp mật khẩu.
- ✓ Lừa đảo qua điện thoại (vishing) – Giả danh ngân hàng để lấy mã OTP.

Câu 2: Thuật ngữ nào dùng để tạo ra nhu cầu hoặc vấn đề trong pretexting của Social Engineering?

- ◆ Reverse Social Engineering là kỹ thuật tạo ra một vấn đề giả mạo hoặc một nhu cầu cấp thiết, khiến nạn nhân chủ động tìm đến kẻ tấn công để được giúp đỡ.

💡 Ví dụ thực tế:

- ✓ Kẻ tấn công cố tình làm gián đoạn mạng nội bộ, sau đó giả làm nhân viên IT để "hỗ trợ khắc phục sự cố".
- ✓ Một hacker tạo email giả mạo thông báo tài khoản ngân hàng bị khóa, buộc nạn nhân phải nhập thông tin đăng nhập để mở lại tài khoản.

Câu 3: Mục tiêu tâm lý chính của Social Engineer khi nói chuyện với nhân viên lừa tân là gì?

- ◆ Social Engineer sử dụng Pathos (cảm xúc) để thao túng nạn nhân.

💡 Các chiến thuật tâm lý được sử dụng:

- ✓ Gây sự đồng cảm (Sympathy): Kể một câu chuyện buồn hoặc tạo ra tình huống khẩn cấp để khiến lừa tân muốn giúp đỡ.
- ✓ Tận dụng sự thương hại: "Tôi quên thẻ nhân viên ở nhà, tôi sẽ bị khiển trách nếu không vào được phòng họp!"
- ✓ Tạo cảm giác cấp bách: "Tôi có một cuộc họp quan trọng với sếp trong 5 phút nữa, bạn có thể giúp tôi vào được không?"
- ➡ Ví dụ thực tế: Một hacker giả danh khách hàng VIP, phàn nàn về dịch vụ kém để nhân viên khách sạn đồng cảm và cung cấp thông tin quan trọng.

Câu 4: Kỹ thuật nào được sử dụng để tạo ra sự quen thuộc với Dr. Gordon?

- ◆ Insinuation là kỹ thuật ngụ ý rằng kẻ tấn công có quen biết với người có thẩm quyền, khiến nạn nhân mất cảnh giác.

💡 Ví dụ thực tế:

- ✓ "Dr. Gordon nói tôi có thể đến thăm văn phòng của ông ấy, nhưng tôi quên mang thẻ ra vào."
- ✓ "Tôi đã từng làm việc với Dr. Gordon trong dự án trước, chắc anh ấy vẫn nhớ tôi!"
- ➡ Mục đích: Khiến nhân viên tin rằng kẻ tấn công thực sự có mối quan hệ với Dr. Gordon và hợp pháp hóa yêu cầu của họ.

Câu 5: Vai trò của nhân viên lừa tân trong kế hoạch của Social Engineer là gì?

- ◆ Nhân viên lễ tân thường là mục tiêu dễ bị thao túng nhất vì họ có nhiệm vụ hỗ trợ khách hàng và nhân viên.
- 💡 Cách hacker lợi dụng nhân viên lễ tân:
- ✓ Đặt câu hỏi vô hại: "Dr. Gordon có ở văn phòng không?"
 - ✓ Gây áp lực: "Tôi có hẹn với anh ấy nhưng quên mất thời gian, bạn có thể kiểm tra giúp tôi không?"
 - ✓ Tạo sự quen thuộc: "Tôi mới gặp Dr. Gordon hôm qua, nhưng quên số phòng của anh ấy rồi."
- 📌 Ví dụ thực tế: Hacker có thể hỏi nhân viên lễ tân về sơ đồ văn phòng, thời gian làm việc của sếp, hoặc cách truy cập mạng nội bộ.
-

Câu 6: "Malware for the human brain" có nghĩa là gì?

- ◆ "Malware for the human brain" là cách so sánh giữa Social Engineering và phần mềm độc hại (malware).
 - ◆ Kẻ tấn công không hack máy tính, mà hack tâm trí của nạn nhân!
- 💡 Chiêu thuật thao túng nhận thức:
- ✓ Gài gắm thông tin một cách vô thức: Nhắc đi nhắc lại một điều để khiến nạn nhân chấp nhận đó là sự thật.
 - ✓ Tạo sự quen thuộc giả tạo: Gặp gỡ nhiều lần để nạn nhân tin tưởng hơn.
 - ✓ Tận dụng hiệu ứng mồi nhử (Priming Effect): Đưa ra gợi ý liên tiếp khiến nạn nhân có xu hướng tiết lộ thông tin quan trọng.
- 📌 Ví dụ thực tế: Một hacker hỏi nhân viên IT: "Bạn có nhớ chính sách đặt lại mật khẩu không?" → Sau đó tiếp tục khai thác để có được quyền truy cập hệ thống.
-

Câu 7: Pretexting trong Social Engineering là gì?

- ◆ Pretexting là kỹ thuật dựng lên một kịch bản giả để đánh lừa nạn nhân cung cấp thông tin nhạy cảm.
- 💡 Ví dụ thực tế:
- ✓ Giả làm nhân viên IT gọi điện để yêu cầu nạn nhân cung cấp mật khẩu.
 - ✓ Mạo danh nhân viên ngân hàng yêu cầu khách hàng xác nhận thông tin tài khoản.
-

Câu 8: Mục tiêu chính của tấn công Phishing là gì?

- ◆ Phishing không tấn công trực tiếp vào hệ thống máy tính mà lừa người dùng tự nguyện cung cấp thông tin như mật khẩu, số thẻ tín dụng.
- 💡 Ví dụ thực tế:
- ✓ Email giả mạo ngân hàng yêu cầu người dùng đăng nhập để xác minh tài khoản.
 - ✓ Tin nhắn SMS mạo danh bưu điện yêu cầu cung cấp thông tin cá nhân.
-

Câu 9: Thuật ngữ nào mô tả hành vi lừa đảo khiến mục tiêu nhấp vào liên kết độc hại?

- ◆ Phishing dụ dỗ nạn nhân nhấp vào liên kết độc hại hoặc tải về phần mềm độc hại để đánh cắp thông tin.
- 💡 Ví dụ thực tế:
-

- ✓ Email giả mạo Google thông báo tài khoản Gmail bị khóa và yêu cầu đăng nhập qua một liên kết giả.
 - ✓ Website giả mạo Facebook yêu cầu đăng nhập lại do "vi phạm điều khoản".
-

Câu 10: Kỹ thuật Social Engineering nào diễn ra trực tiếp, mặt đối mặt?

- ◆ Iso-praxis là kỹ thuật bắt chước hành vi, ngôn ngữ cơ thể và cách nói chuyện của nạn nhân để tạo sự tin tưởng.
- 💡 Ví dụ thực tế:
- ✓ Một hacker bắt chước phong cách nói chuyện của nhân viên ngân hàng khi mạo danh gọi điện.
 - ✓ Giả làm nhân viên kĩ thuật và copy cách đi đứng, cử chỉ của nhân viên thật để không bị nghi ngờ.
-

Câu 11: Nguyên tắc tâm lý nào giải thích tại sao con người cung cấp niềm tin sau khi đưa ra quyết định?

- ◆ Khi con người cam kết một điều gì đó, họ có xu hướng giữ vững quan điểm để duy trì sự nhất quán trong hành vi của mình.
- 💡 Ví dụ thực tế:
- ✓ Nếu ai đó công khai ủng hộ một sản phẩm, họ sẽ ít có khả năng thay đổi ý kiến ngay cả khi có thông tin tiêu cực về nó.
 - ✓ Khi đã nhấn "Thích" một trang trên Facebook, bạn có xu hướng tin rằng mình thực sự thích nó và tiếp tục theo dõi.
-

Câu 12: Tại sao nguyên tắc "Reciprocation" (cố gắng trả lại) lại có sức mạnh thao túng?

- ◆ Khi ai đó cho bạn thứ gì đó, bạn cảm thấy có nghĩa vụ phải đáp lại – đây là nguyên tắc tâm lý rất mạnh mẽ trong Social Engineering.
- 💡 Ví dụ thực tế:
- ✓ Một hacker giả làm nhân viên hỗ trợ kỹ thuật, giúp nhân viên công ty khắc phục lỗi máy tính → Nhân viên cảm thấy biết ơn và dễ dàng cung cấp thông tin nhạy cảm.
 - ✓ Một kẻ lừa đảo gửi quà miễn phí, sau đó yêu cầu nạn nhân "đáp lại" bằng cách điền thông tin cá nhân vào một biểu mẫu giả.
-

Câu 13: Một Social Engineer có thể khai thác tháp nhu cầu của Maslow như thế nào?

- ◆ Maslow's Pyramid mô tả các nhu cầu cơ bản của con người, từ sinh lý đến tự thể hiện.
 - ◆ Kẻ tấn công có thể xác định và khai thác nhu cầu này để thao túng nạn nhân.
- 💡 Ví dụ thực tế:
- ✓ Một hacker khai thác nhu cầu an toàn bằng cách giả làm cảnh sát, yêu cầu cung cấp thông tin cá nhân để "bảo vệ tài khoản".
 - ✓ Một kẻ lừa đảo sử dụng nhu cầu kết nối xã hội bằng cách giả làm bạn bè trên mạng để lấy lòng tin.
-

Câu 14: "Isopraxis" trong Social Engineering là gì?

- ◆ Isopraxis là kỹ thuật bắt chước ngôn ngữ cơ thể, nhịp điệu thở và giọng nói để tạo sự đồng điệu và tin tưởng.

 Ví dụ thực tế:

- ✓ Nếu nạn nhân nói chuyện chậm rãi, hacker cũng nói chậm rãi để tạo sự thân thiện.
 - ✓ Nếu nạn nhân có thói quen khoanh tay khi nói chuyện, hacker cũng làm vậy để tạo sự đồng cảm.
-

Câu 15: Mục tiêu chính của một Social Engineer là gì?

◆ Mục tiêu chính của Social Engineering là lừa nạn nhân tiết lộ thông tin nhạy cảm mà họ không hề nhận ra.

 Ví dụ thực tế:

- ✓ Giả danh nhân viên IT để lấy thông tin đăng nhập của nhân viên công ty.
 - ✓ Gửi email giả mạo CEO yêu cầu phòng tài chính chuyển khoản tiền lớn.
-

Câu 16: Mục tiêu chính của "Elicitation" trong Social Engineering là gì?

◆ Elicitation là nghệ thuật khai thác thông tin một cách tinh vi mà nạn nhân không nhận ra rằng mình đang bị hỏi cung.

 Ví dụ thực tế:

- ✓ Một hacker giả làm khách hàng thân thiện, tán gẫu với nhân viên ngân hàng để moi thông tin về hệ thống bảo mật.
 - ✓ Một kẻ lừa đảo đóng giả đồng nghiệp cũ, hỏi về cấu trúc nội bộ công ty mà không gây nghi ngờ.
-

Câu 17: Thuật ngữ nào mô tả việc tạo ra nhu cầu hoặc một vấn đề trong pretexting của Social Engineering?

◆ Orchestrating là kỹ thuật dàn dựng một tình huống hoặc vấn đề giả để khiến nạn nhân cảm thấy họ cần giải quyết ngay lập tức, từ đó bị thao túng để tiết lộ thông tin hoặc thực hiện hành động có lợi cho hacker.

 Ví dụ thực tế:

- ✓ Hacker giả làm nhân viên IT gọi điện cho nhân viên công ty và nói rằng có lỗi bảo mật trong hệ thống, yêu cầu cung cấp thông tin đăng nhập để "khắc phục".
 - ✓ Kẻ tấn công mạo danh ngân hàng, thông báo tài khoản của bạn có giao dịch bất thường, yêu cầu bạn đăng nhập vào một trang web giả mạo để xác minh thông tin.
-

Câu 18: Trong kịch bản được đề cập, mục tiêu tâm lý chính của Social Engineer khi nói chuyện với lẽ tân là gì?

◆ Pathos là một trong ba kỹ thuật thuyết phục của Aristotle (Logos – Lý trí, Ethos – Đạo đức, Pathos – Cảm xúc).

◆ Kẻ tấn công thường tạo ra một câu chuyện cảm động, khẩn cấp hoặc đáng thương để khiến nạn nhân đồng cảm và dễ bị thao túng.

 Ví dụ thực tế:

- ✓ Một hacker giả vờ là người nhà của bệnh nhân cấp cứu, khẩn khoản yêu cầu lẽ tân cung cấp thông tin về bác sĩ điều trị.
- ✓ Kẻ tấn công mạo danh nhân viên bị khóa tài khoản email, nài nỉ nhân viên IT cấp lại mật khẩu ngay lập tức vì "công việc rất quan trọng".

Câu 19: Trong kịch bản trên, Social Engineer đã sử dụng kỹ thuật nào để ám chỉ rằng họ quen biết Dr. Gordon?

- ◆ Insinuation là kỹ thuật gợi ý một cách tinh tế rằng họ có mối quan hệ hoặc kiến thức đặc biệt về mục tiêu, mà không cần chứng minh rõ ràng.
- ◆ Điều này khiến nạn nhân tự động lấp đầy khoảng trống trong câu chuyện và tin rằng hacker thực sự có liên hệ với Dr. Gordon.

💡 Ví dụ thực tế:

- ✓ Kẻ tấn công nói: "*Tôi có cuộc hẹn với Dr. Gordon, nhưng tôi quên mất giờ. Ông ấy bảo tôi ghé qua văn phòng để lấy tài liệu. Tôi tin rằng ông ấy đã để lại cho tôi rồi?*" → Lẽ tân có thể tự suy luận rằng hacker thực sự quen Dr. Gordon.
 - ✓ Một hacker giả danh khách hàng VIP nói: "*Tôi từng làm việc với CEO của bạn vài tháng trước, anh ấy nói tôi có thẻ liên hệ trực tiếp với bạn.*"
-

Câu 20: Vai trò của lẽ tân trong kế hoạch của Social Engineer là gì?

- ◆ Lẽ tân thường có quyền truy cập vào lịch làm việc, số liên lạc, danh sách nhân sự – những thông tin có thể bị khai thác để tiếp tục tấn công.
- ◆ Trong nhiều trường hợp, lẽ tân bị hacker thao túng mà không hề nhận ra mình đang cung cấp thông tin quan trọng.

💡 Ví dụ thực tế:

- ✓ Hacker giả làm đối tác kinh doanh hỏi: "*Tôi có cuộc hẹn với giám đốc IT, anh ấy có rảnh lúc 2 giờ không?*" → Lẽ tân vô tình tiết lộ lịch trình của giám đốc IT.
 - ✓ Một kẻ giả danh nhân viên mới hỏi: "*Ai trong công ty có quyền cấp quyền truy cập hệ thống?*" → Nếu lẽ tân trả lời, hacker sẽ biết được người nào có quyền quan trọng.
-

Câu 21: Làm thế nào để một Social Engineer xây dựng quan hệ và tạo lòng tin với mục tiêu?

- ◆ Con người có xu hướng tin tưởng những người thực sự lắng nghe họ.
- ◆ Một hacker xã hội (Social Engineer) không cần nói quá nhiều mà chỉ cần dồn dắt cuộc trò chuyện một cách khéo léo, khiến mục tiêu cảm thấy họ được thấu hiểu.
- ◆ Lắng nghe nhiều hơn giúp hacker thu thập thông tin quan trọng mà nạn nhân vô tình tiết lộ.

💡 Ví dụ thực tế:

- ✓ Một hacker đóng vai nhân viên IT, lắng nghe nhân viên công ty than phiền về hệ thống bảo mật chậm chạp, sau đó đề nghị "giúp đỡ" bằng cách lấy thông tin đăng nhập của họ.
 - ✓ Trong một cuộc gọi giả danh, hacker để mục tiêu nói nhiều hơn và chỉ đặt câu hỏi gợi mở để thu thập dữ liệu.
-

Câu 22: Làm thế nào để hacker dẫn dắt mục tiêu nghĩ rằng giải pháp là do họ tự đề xuất?

- ◆ Con người có xu hướng tin vào ý tưởng của chính mình hơn là nghe theo người khác.
- ◆ Một Social Engineer có thể định hướng cuộc trò chuyện sao cho nạn nhân tự đi đến kết luận mà hacker mong muốn.

 Ví dụ thực tế:

- ✓ Hacker giả danh nhân viên bảo mật công ty, đặt câu hỏi như:

 "Anh/chị có bao giờ thấy hệ thống email này có vấn đề không?"

 "Nếu có ai đó muốn truy cập trái phép, họ sẽ làm thế nào nhỉ?"

→ Nhân viên có thể tự động đề xuất cách giải quyết và vô tình tiết lộ điểm yếu bảo mật.

Câu 23: Làm thế nào để hacker nuôi dưỡng cảm giác độc lập của mục tiêu?

- ◆ Hacker không áp đặt, mà khiến nạn nhân cảm thấy họ tự chủ trong quyết định của mình.
- ◆ Kỹ thuật này dựa trên nguyên tắc "Fostering Autonomy" (Nuôi dưỡng sự tự chủ), khiến nạn nhân nghĩ rằng họ không bị thao túng mà đang hành động theo ý mình.

 Ví dụ thực tế:

- ✓ Hacker đóng vai nhân viên hỗ trợ IT, nói với nạn nhân:

 "Anh/chị có thể thay đổi mật khẩu theo cách này, nhưng nếu anh/chị thích cách khác, tôi có thể hướng dẫn thêm."

→ Nạn nhân cảm thấy được kiểm soát và dễ dàng hợp tác hơn.

Câu 24: Loại giao tiếp nào chiếm phần lớn trong giao tiếp giữa người với người?

- ✓ Theo nghiên cứu của Albert Mehrabian, 93% giao tiếp giữa người với người không nằm ở lời nói, mà ở:
- ◆ Ngôn ngữ cơ thể (Body Language) – 55%
 - ◆ Âm điệu, giọng điệu (Tone of Voice) – 38%
 - ◆ Nội dung lời nói (Words) – 7%

 Ứng dụng trong Social Engineering:

- ✓ Hacker bắt chước cử chỉ, giọng điệu, nhịp điệu hơi thở của mục tiêu để tạo sự quen thuộc.
- ✓ Nếu hacker bắt chéo tay khi nói chuyện, họ có thể khiến nạn nhân vô thức bắt chước, tạo cảm giác đồng điệu và tin tưởng.
-

Câu 25: Micro-expressions là gì?

- ◆ Micro-expressions là biểu cảm thoáng qua trên khuôn mặt khi con người trải qua một cảm xúc mạnh.
- ◆ Chúng chỉ xuất hiện trong 1/25 đến 1/5 giây, gần như không thể kiểm soát.

 Ứng dụng trong Social Engineering:

- ✓ Một hacker có thể quan sát micro-expressions để xác định liệu nạn nhân có nghi ngờ không.
- ✓ Ví dụ, nếu hacker giả danh IT và yêu cầu mật khẩu, nạn nhân có thể nhíu mày trong 1/5 giây → Dấu hiệu họ đang nghi ngờ.
- ✓ Hacker có thể ngay lập tức đổi chiến thuật, nói:
-  "Tôi chỉ cần kiểm tra quyền truy cập, anh/chị có thể thay đổi mật khẩu ngay sau khi tôi hoàn thành."
-

Câu 26: Mục đích chính của "Elicitation" trong chu trình tấn công Social Engineering là gì?

- ◆ Elicitation (khai thác thông tin) là kỹ thuật gợi mở thông tin một cách tinh vi thông qua những cuộc trò chuyện tưởng như vô hại.
- ◆ Hacker không trực tiếp yêu cầu thông tin, mà dẫn dắt để nạn nhân tự nguyện tiết lộ.

💡 Ví dụ thực tế:

- ✓ Hacker giả danh nhân viên IT và nói:

👉 "Tôi thấy nhiều người quên đổi mật khẩu sau khi chính sách bảo mật mới được áp dụng. Anh/chị có giữ nguyên mật khẩu cũ không?"

- ✓ Nếu nạn nhân trả lời "Vẫn dùng mật khẩu cũ", hacker đã có một phần dữ kiện quan trọng.

Câu 27: Loại thông điệp thuyết phục nào nhắm đến cảm xúc của mục tiêu?

- ✓ Pathos là kỹ thuật tác động vào cảm xúc, khiến nạn nhân dễ bị thao túng.

- ✓ Các cảm xúc thường được khai thác:

- ◆ Sợ hãi ("Nếu không cập nhật ngay, tài khoản của anh/chị có thể bị khóa!")
- ◆ Lòng trắc ẩn ("Chúng tôi là tổ chức từ thiện giúp trẻ em bị ung thư, bạn có thể ủng hộ chúng ta?")
- ◆ Cảm giác cấp bách ("Chỉ còn 10 suất cuối cùng, hãy đăng ký ngay!")

💡 Ví dụ thực tế:

- ✓ Email lừa đảo:

👉 "Tài khoản ngân hàng của bạn có giao dịch bất thường! Hãy đăng nhập ngay để kiểm tra!"
→ Kích hoạt nỗi sợ hãi, khiến nạn nhân mất cảnh giác và nhấp vào liên kết giả mạo.

Câu 28: Một hacker sử dụng "Ethos" để tác động đến mục tiêu như thế nào?

- ◆ Ethos dựa vào quyền lực, danh tiếng, uy tín để thao túng nạn nhân.
- ◆ Nếu hacker đóng vai một nhân vật có quyền lực, nạn nhân sẽ dễ bị thuyết phục hơn.

💡 Ví dụ thực tế:

- ✓ Giả danh sếp công ty để yêu cầu nhân viên kê toán chuyển tiền.

- ✓ Giả mạo chuyên gia bảo mật và nói:

👉 "Tôi là chuyên gia IT, anh/chị có thể đọc số OTP để tôi xác minh giúp không?"

- ✓ Vì hacker tạo ra hình ảnh có uy tín, nạn nhân sẽ dễ tin tưởng hơn.

Câu 29: Đặc điểm của các kênh giao tiếp phong phú và đồng bộ (rich & synchronous communication) trong Social Engineering là gì?

- ◆ Giao tiếp đồng bộ (ví dụ: gặp mặt trực tiếp, gọi video) có nhiều dữ liệu phi ngôn ngữ hơn, giúp phát hiện dấu hiệu lừa đảo dễ dàng hơn.
- ◆ Ví dụ: Nếu hacker căng thẳng, có micro-expressions (biểu cảm thoáng qua trên mặt) khi nói dối, có thể bị phát hiện.

 **Ứng dụng thực tế:**

- ✓ Gọi video để xác minh danh tính thay vì chỉ tin vào email hoặc tin nhắn.
 - ✓ Quan sát ngôn ngữ cơ thể và giọng điệu khi giao tiếp với người lạ.
-

Câu 30: Dấu hiệu nào có thể cho thấy ai đó đang nói dối hoặc có ý đồ lừa đảo?

- ✓ Khi nói dối, bộ não phải xử lý nhiều thông tin cùng lúc, tạo ra căng thẳng và mệt mỏi nhận thức.
 - ✓ Dấu hiệu của cognitive load (tải nhận thức cao):
 - ◆ Nói lắp, nói nhanh hoặc chậm bất thường.
 - ◆ Đỏ mồ hôi, chạm vào mặt hoặc cổ nhiều lần.
 - ◆ Tránh giao tiếp bằng mắt hoặc chớp mắt quá nhanh.
 -  Ví dụ thực tế: Khi một hacker giả danh nhân viên IT, nếu bị đặt câu hỏi bất ngờ, họ có thể ngập ngừng hoặc lặp lại câu hỏi trước khi trả lời.
-

Câu 31: Những đặc điểm tính cách nào được bao gồm trong "Dark Triad" (Bộ Ba Bóng Tối)?

- ◆ Dark Triad là một khái niệm trong tâm lý học mô tả ba đặc điểm tính cách độc hại thường liên quan đến hành vi thao túng, vô cảm và khai thác người khác:
 - ✓ Machiavellianism – Chủ nghĩa thực dụng, thao túng người khác để đạt mục tiêu cá nhân.
 - ✓ Narcissism – Tự yêu bản thân quá mức, coi mình là trung tâm và tìm kiếm sự ngưỡng mộ từ người khác.
 - ✓ Psychopathy – Thiếu cảm xúc, vô cảm với nỗi đau của người khác, hành vi bốc đồng và liều lĩnh.
-  **Ứng dụng thực tế:** Những cá nhân có Dark Triad có khả năng tham gia vào tội phạm mạng do họ thiếu đạo đức, thích thao túng và không quan tâm đến hậu quả.
-

Câu 32: Nhóm người nào dễ trở thành nạn nhân của lừa đảo trực tuyến theo nghiên cứu?

- ◆ Người lớn tuổi thường là mục tiêu chính vì họ ít cập nhật kiến thức về bảo mật và dễ bị các chiêu trò lừa đảo thao túng.
 - ◆ Hành vi trực tuyến rủi ro (như nhấp vào liên kết lạ, chia sẻ thông tin cá nhân) làm tăng nguy cơ bị tấn công.
 -  Ví dụ thực tế: Các vụ lừa đảo qua điện thoại và email nhắm vào người lớn tuổi để đánh cắp thông tin tài chính.
-

Câu 33: Yếu tố chính khiến tội phạm mạng khó bị phát hiện bởi cơ quan thực thi pháp luật là gì?

- ◆ Nhiều nạn nhân không báo cáo do thiếu hiểu biết hoặc sợ bị đổ lỗi.
 - ◆ Hệ thống pháp luật chưa hoàn thiện để xử lý các vụ án mạng.
 - ◆ Tội phạm mạng có thể ẩn danh, khiến việc điều tra khó khăn hơn.
-  Ví dụ thực tế: Các vụ lừa đảo qua email (phishing) thường không được báo cáo, dẫn đến nhiều cá nhân khác tiếp tục trở thành nạn nhân.
-

Câu 34: Tại sao cần nghiên cứu động cơ của tội phạm mạng?

- ◆ Nghiên cứu giúp dự đoán và ngăn chặn hành vi tội phạm bằng cách hiểu lý do và yếu tố thúc đẩy.
 - ◆ Hiểu động cơ giúp thiết kế biện pháp bảo mật hiệu quả hơn.
- 💡 Ví dụ thực tế: Những kẻ tấn công ransomware thường có động cơ tài chính → doanh nghiệp cần tập trung vào bảo vệ dữ liệu và hệ thống thanh toán.
-

Câu 35: Điều gì giúp giảm thiểu các cuộc tấn công ransomware trong một tổ chức?

- ◆ Văn hóa an ninh mạnh mẽ giúp nhân viên nhận thức về rủi ro và tránh trở thành nạn nhân.
 - ◆ Cơ chế khôi phục sự cố giúp tổ chức phục hồi sau cuộc tấn công ransomware mà không cần trả tiền chuộc.
- 💡 Ví dụ thực tế: Công ty Maersk bị tấn công bởi ransomware NotPetya, nhưng nhờ có backup mạnh, họ không phải trả tiền chuộc mà vẫn khôi phục hệ thống.
-

Câu 36: Những yếu tố nào cấu thành văn hóa an ninh mạng trong tổ chức?

- ◆ Thái độ (Attitudes) – Mức độ nhân viên coi trọng bảo mật.
 - ◆ Hành vi (Behaviours) – Cách nhân viên thực hiện các biện pháp an ninh.
 - ◆ Nhận thức (Cognition) – Mức độ hiểu biết về các mối đe dọa.
 - ◆ Giao tiếp (Communication) – Cách tổ chức truyền đạt thông tin bảo mật.
- 💡 Ví dụ thực tế: Google tổ chức các khóa huấn luyện an ninh định kỳ để nhân viên luôn cảnh giác với các mối đe dọa mạng.
-

Câu 37: Những thực thể nào liên quan đến tội phạm mạng?

- ◆ Kẻ tấn công (Attackers) – Hacker, nhóm tội phạm mạng, gián điệp công nghệ.
 - ◆ Nạn nhân (Victims) – Cá nhân, tổ chức, chính phủ.
 - ◆ Cơ quan thực thi pháp luật (Law enforcement) – FBI, Europol, các cơ quan an ninh mạng.
- 💡 Ví dụ thực tế: Vụ tấn công SolarWinds 2020 cho thấy cả chính phủ và công ty tư nhân đều có thể là mục tiêu.
-

Câu 38: Mục tiêu của việc nghiên cứu khía cạnh con người trong tội phạm mạng là gì?

- ◆ Tìm hiểu động cơ và cách ra quyết định của hacker giúp thiết kế biện pháp phòng thủ tốt hơn.
 - ◆ Giúp dự đoán xu hướng tấn công trong tương lai.
- 💡 Ví dụ thực tế: Nhóm hacker Lazarus của Triều Tiên chủ yếu tấn công để thu lợi tài chính.
-

Câu 39: Điểm giống nhau giữa tội phạm mạng và tội phạm truyền thống là gì?

- ◆ Cả hai loại tội phạm đều tìm cách tránh bị bắt, dù là lừa đảo trực tuyến hay cướp ngân hàng.
 - ◆ Tội phạm mạng sử dụng VPN, địa chỉ IP giả, dark web để che giấu danh tính.
- 💡 Ví dụ thực tế: Hacker sử dụng Bitcoin để tránh bị theo dõi trong các vụ tấn công ransomware.
-

Câu 40: Vấn đề trong cách cảnh sát nhìn nhận nạn nhân của tội phạm mạng là gì?

- ◆ Cảnh sát có thể coi tội phạm mạng là "lỗi do nạn nhân bát cẩn", thay vì xem họ là nạn nhân thực sự.
- ◆ Điều này khiến nhiều người không báo cáo tội phạm mạng, làm cho vấn đề càng nghiêm trọng hơn.
 - 💡 Ví dụ thực tế: Một người bị mất tiền trong vụ lừa đảo email có thể bị xem là "không cẩn thận", trong khi nếu bị trộm ngoài đời, họ sẽ được hỗ trợ ngay.

Câu 41: Malware là gì?

- ◆ Malware (Malicious Software) là phần mềm độc hại được thiết kế để gây hại, đánh cắp dữ liệu hoặc kiểm soát hệ thống.
- ◆ Bao gồm virus, trojan, worm, spyware, ransomware, rootkit, adware.
- 💡 Ví dụ thực tế: WannaCry ransomware (2017) mã hóa dữ liệu của hàng trăm ngàn máy tính trên toàn thế giới và yêu cầu tiền chuộc.

Câu 42: Đặc điểm của Malware là gì?

✓ Malware có thể:

- ◆ Tấn công tính bảo mật (Confidentiality) – Đánh cắp dữ liệu.
- ◆ Tấn công tính toàn vẹn (Integrity) – Làm hỏng hoặc sửa đổi dữ liệu.
- ◆ Tấn công tính khả dụng (Availability) – Làm hệ thống không hoạt động (DDoS, Ransomware).
- 💡 Ví dụ thực tế: NotPetya (2017) – Làm sập hệ thống máy tính của Maersk, gây thiệt hại hơn 10 tỷ USD.

Câu 43: Hacking là gì?

- ◆ Hacking là hành vi xâm nhập trái phép vào hệ thống bằng cách tận dụng lỗ hổng bảo mật hoặc vượt qua kiểm soát an ninh.
- ◆ Có thể là mũ trắng (White Hat – Ethical Hacking), mũ đen (Black Hat – Cracker), mũ xám (Gray Hat – Ethical nhưng trái phép).
- 💡 Ví dụ thực tế: Kevin Mitnick – Hacker nổi tiếng bị bắt vì tấn công vào hệ thống của Nokia và IBM.

Câu 44: Hành vi nào là tội phạm liên quan đến con người trên không gian mạng (Interpersonal offense)?

- ◆ Cyber-stalking là quấy rối, theo dõi hoặc đe dọa người khác trực tuyến.
- ◆ Liên quan đến quấy rối qua email, mạng xã hội, hoặc phần mềm giám sát (stalkerware).
- 💡 Ví dụ thực tế: CEO của Reddit bị theo dõi trên mạng bởi một hacker sau khi công ty áp dụng chính sách bảo mật nghiêm ngặt.

Câu 45: Nội dung trực tuyến nào thể hiện sự thù ghét dựa trên chủng tộc, tôn giáo, giới tính...?

- ◆ Hate speech (Phát ngôn thù ghét) – Nội dung bạo lực, kỳ thị.
- ◆ Hate crimes (Tội ác thù ghét) – Hành động bạo lực dựa trên định kiến.
- 💡 Ví dụ thực tế: Facebook và Twitter đã thực hiện chính sách xóa bỏ nội dung phát ngôn thù ghét vào năm 2020.

Câu 46: Gian lận mạng (Cyber-enabled fraud) tập trung vào điều gì?

- ◆ Lừa đảo tài chính – Dùng thông tin của nạn nhân để thực hiện giao dịch bất hợp pháp.
 - ◆ Lừa đảo đầu tư, mua hàng online – Tạo trang web giả mạo, dụ người dùng chuyển tiền.
- 💡 Ví dụ thực tế: Lừa đảo qua email CEO (Business Email Compromise - BEC) – Kẻ tấn công giả danh CEO để lừa nhân viên chuyển tiền.
-

Câu 47: Hình thức nào liên quan đến thu thập và phân tích dữ liệu về mối đe dọa mạng?

- ◆ Cyber threat intelligence (CTI) giúp tổ chức phân tích dữ liệu từ hacker, diễn đàn chợ đen, và mạng botnet để dự đoán các cuộc tấn công.
- 💡 Ví dụ thực tế: IBM X-Force Threat Intelligence chuyên nghiên cứu về các nhóm hacker toàn cầu.
-

Câu 48: Đặc điểm chính của Cyber-stalking là gì?

- ◆ Cyber-stalking liên quan đến nhắn tin liên tục, đe dọa, hoặc theo dõi nạn nhân qua Internet.
- 💡 Ví dụ thực tế: Một người phụ nữ tại Mỹ đã bị bắt vì gửi hơn 65.000 tin nhắn đe dọa sau một cuộc hẹn hò trực tuyến.
-

Câu 49: Mục đích của Grooming là gì?

- ◆ Online grooming là quá trình kẻ tấn công xây dựng mối quan hệ với trẻ em để lợi dụng hoặc lạm dụng.
- 💡 Ví dụ thực tế: Gã khổng lồ công nghệ Facebook đã triển khai AI để phát hiện grooming trên Messenger.
-

Câu 50: Đặc điểm chung của các cuộc tấn công Phishing là gì?

- ◆ Phishing là tấn công lừa đảo bằng cách giả mạo email, tin nhắn, trang web... để dụ nạn nhân nhập thông tin cá nhân.
 - ◆ Tấn công dựa trên tâm lý – Đánh vào sự tin tưởng, nỗi sợ hãi hoặc lòng tham.
- 💡 Ví dụ thực tế: Vụ tấn công vào Twitter năm 2020 – Hacker sử dụng phishing để chiếm quyền điều khiển tài khoản của Elon Musk, Bill Gates, Apple...
-

Câu 51: CaaS có nghĩa là gì?

- ◆ "(Cyber)crime-as-a-Service.": Tội phạm như một dịch vụ – Hacker cung cấp công cụ hoặc dịch vụ tấn công mạng cho người khác.
- 💡 Ví dụ thực tế: Dark Web cung cấp botnet thuê bao để tấn công DDoS.

VII. TÀI LIỆU THAM KHẢO

Khóa học Cybercrime trên Coursera. Instructor: Konstantinos Mersinas, University of London. Available at: <https://www.coursera.org/learn/cybercrime?>

Bada, M. and Nurse, J.R.C. (2020) ‘The social and psychological impact of cyberattacks’, *Emerging Cyber Threats and Cognitive Vulnerabilities*, pp. 73–92. Available at: <https://doi.org/10.1016/b978-0-12-816203-3.00004-6>.

Cabinet Office (2021) *National Cyber Strategy 2022*, GOV.UK. Available at: <https://www.gov.uk/government/publications/national-cyber-strategy-2022>.

Crown Prosecution Service (2024) *Cybercrime - Prosecution Guidance*, Cps.gov.uk. Crown Prosecution Service. Available at: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>.

Cyber crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75 (2013). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

Cyber crime: a review of the evidence (no date) GOV.UK. Available at: <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence>.

Department for Digital, Culture, Media & Sport (2022) *Cyber Security Breaches Survey 2022*, GOV.UK. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>.

ENISA (2021) *ENISA Threat Landscape 2021*, ENISA. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

Essays: The Psychology of Security (Part 1) - Schneier on Security (no date) www.schneier.com. Available at: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html.

Europol (2021) *Serious and Organised Crime Threat Assessment (SOCTA)*, Europol. Available at: <https://www.europol.europa.eu/publications-events/main-reports/socata-report>.

Federal Bureau of Investigation (2022) Internet Crime Report. Available at: https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf

Forum, W.E. (no date) *Strategic Intelligence | World Economic Forum, Strategic Intelligence*. Available at: <https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE/key-issues/a1Gb00000015QG1EAM>

Internet Organised Crime Threat Assessment (IOCTA) 2021 (no date) Europol. Available at: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>.

Jason (2018) *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*, ResearchGate. unknown. Available at: https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit.

Public Awareness and Prevention Guides (no date) Europol. Available at: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides>.

Stringhini, G. et al. (no date) *Adversarial Behaviours Knowledge Area Issue*. Available at: https://www.cybok.org/media/downloads/Adversarial_Behaviours_issue_1.0.pdf.

The Psychology of Security (Part 2) - Schneier on Security (2020) Schneier on Security. Available at: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se2.html (Accessed: 25 March 2025).