ĐẠI HỌC HUẾ

TRƯỜNG ĐẠI HỌC KHOA HỌC

---o0o---

HỌC PHẦN: AN NINH MẠNG

SOCIAL ENGINEERING

Giảng viên giảng dạy: Võ Việt Dũng

Nhóm thực hiện: Nhóm 03

Huế, ngày 05 tháng 01 năm 2026

BẢNG PHÂN CÔNG NHIỆM VỤ

Họ và tên	**MSV**	**Nhiệm vụ**	**Múc độ hoàn thành**
Hoàng Hà Anh Dũng	23T1020123	Phân công nhóm, tìm nội dung phần 1	100%
Nguyễn Công Tình	23T1020544	Tìm nội dung phần 2, làm word	100%
Lê Trần Gia Huy	23T1020232	Tìm nội dung phần 3	100%
Đỗ Văn Thành	23T1020498	Tìm nội dung phần 4	100%

MỤC LỤC

MỞ ĐẦU

Sự phát triển mạnh mẽ của công nghệ thông tin và Internet đã mang lại nhiều tiện ích to lớn, giúp con người kết nối, trao đổi và giao dịch nhanh chóng hơn bao giờ hết. Tuy nhiên, song song với những lợi ích đó là sự gia tăng đáng kể của các hành vi lợi dụng công nghệ để thực hiện hành vi lừa đảo, chiếm đoạt tài sản, xâm phạm dữ liệu cá nhân và gây thiệt hại cho người dùng.

Trong những năm gần đây, các hình thức tấn công lừa đảo ngày càng đa dạng và tinh vi hơn, đặc biệt là các **chiêu thức tấn công xã hội (social engineering)** – nơi kẻ gian không chỉ khai thác lỗ hổng kỹ thuật mà còn tận dụng yếu tố tâm lý, lòng tin và sự chủ quan của con người. Từ các vụ giả danh nhân viên giao hàng, ngân hàng, cơ quan chức năng, đến những chiêu thức tinh vi như mạo danh lãnh đạo, giả giọng bằng trí tuệ nhân tạo hay lừa đảo tình cảm trực tuyến, tất cả đều cho thấy sự biến đổi không ngừng của tội phạm mạng trong kỷ nguyên số.

Trước thực trạng đó, việc **nghiên cứu, nhận diện và nâng cao nhận thức về các hình thức lừa đảo công nghệ cao** trở nên đặc biệt quan trọng. Không chỉ giúp người dùng cá nhân tự bảo vệ mình, mà còn góp phần xây dựng môi trường mạng an toàn, tin cậy và minh bạch hơn cho toàn xã hội.

Bài tiểu luận này nhằm tổng hợp, phân tích những phương thức lừa đảo phổ biến hiện nay, đề xuất một số biện pháp giáo dục phòng ngừa và khuyến nghị giúp giảm thiểu rủi ro trong quá trình sử dụng Internet và các dịch vụ trực tuyến.

CHƯƠNG I. TÌM HIỂU CÁC HÌNH THỨC TẤN CÔNG: PHISHING, VISHING, BAITING

I.1. Khái Quát về Social Engineering

Trong an ninh mạng, social engineering (kỹ nghệ xã hội) là tập hợp các kỹ thuật tấn công dựa trên việc lợi dụng yếu tố con người, thay vì khai thác trực tiếp lỗ hổng kỹ thuật. Kẻ tấn công tìm cách thao túng cảm xúc, thói quen, sự tin tưởng hoặc thiếu hiểu biết của nạn nhân để khiến họ tự nguyện cung cấp thông tin nhạy cảm (mật khẩu, mã OTP, thông tin thẻ), hoặc tự mình thực hiện hành động nguy hiểm như nhấp vào liên kết độc hại, tải phần mềm độc hại, chuyển tiền…

Ba hình thức phổ biến, dễ gặp nhất là phishing, vishing và baiting.

I.2. Phishing

I.2.1. Khái niệm

Phương thức phishing được biết đến lần đầu tiên vào năm 1987. Nguồn gốc của từ Phishing là sự kết hợp của 2 từ: fishing for information (câu thông tin) và phreaking (trò lừa đảo sử dụng điện thoại của người khác không trả phí). Do sự giống nhau giữa việc "câu cá" và "câu thông tin người dùng", nên thuật ngữ Phishing ra đời.

Phishing là một hình thức tấn công social engineering trong đó kẻ tấn công giả mạo một tổ chức hay cá nhân đáng tin cậy (ngân hàng, công ty, trường học, nhà cung cấp dịch vụ, người quen…) thông qua các kênh trực tuyến như email, tin nhắn, mạng xã hội, website giả mạo…, nhằm lừa nạn nhân:

- Cung cấp thông tin nhạy cảm (tài khoản, mật khẩu, mã OTP, thông tin thẻ tín dụng…).
- Nhấp vào liên kết độc hại.
- Tải và chạy tệp đính kèm chứa malware.

Các tổ chức an ninh như CISA và CrowdStrike đều xem phishing là dạng social engineering phổ biến nhất**,** nhấn mạnh rằng mục tiêu chính của phishing là *khiến nạn nhân thực hiện một hành động cụ thể* (click, tải file, tiết lộ dữ liệu) thông qua nội dung lừa đảo trông như đến từ nguồn đáng tin cậy.

I.2.2. Đặc điểm chung

- Giả mạo danh tính**:** dùng tên hiển thị, logo, cách xưng hô giống hệt tổ chức thật.

- Tạo cảm giác khẩn cấp: cảnh báo tài khoản sẽ bị khóa, giao dịch bất thường, thưởng/hậu đãi sắp hết hạn… để nạn nhân vội vàng phản ứng.
- Dẫn dụ bằng liên kết hoặc tệp đính kèm: buộc nạn nhân phải nhấp vào link, mở file thì mới "giải quyết được vấn đề".
- Khai thác cảm xúc: sợ hãi (bị khóa tài khoản), tham (nhận thưởng, trúng quà), tò mò (xem "hóa đơn", "hình ảnh", "tài liệu mật").

I.2.3. Các hình thức/biến thể chính của Phishing

a) Email Phishing

Hình thức kinh điển: email gửi hàng loạt, nội dung chung chung, giả mạo ngân hàng, mạng xã hội, dịch vụ cloud…

Email chứa liên kết đến website giả hoặc file đính kèm độc hại (PDF, DOC, ZIP, EXE được "ngụy trang").

b) Spear Phishing (phishing có chủ đích)

Nhắm vào một cá nhân hoặc tổ chức cụ thể, email được "may đo" dựa trên thông tin có thật (chức vụ, dự án đang làm, đồng nghiệp…).

Mức độ thuyết phục rất cao vì nội dung tin nhắn tỏ ra hiểu rõ hoàn cảnh của nạn nhân.

c) Whaling (tấn công "cá voi")

Mục tiêu là các vị trí cấp cao trong tổ chức (CEO, CFO, giám đốc, trưởng phòng…).

Nội dung thường liên quan đến hợp đồng lớn, chuyển tiền, thông tin mật, kết hợp kỹ thuật giả mạo email và chữ ký chuyên nghiệp.

d) Smishing (SMS phishing)

Sử dụng tin nhắn SMS/Zalo/OTT để gửi link giả mạo về ngân hàng, bưu điện, công an, thuế…

Lợi dụng tâm lý "tin nhắn từ số tổng đài/đầu số lạ chắc là quan trọng".

I.2.4. Quy trình tấn công điển hình

Một cuộc tấn công phishing thường diễn ra ở mức tổng quát như sau:

1) Thu thập thông tin ban đầu về nạn nhân (từ mạng xã hội, website công ty, rò rỉ dữ liệu…).
2) Soạn nội dung lừa đảo: email/tin nhắn gắn thương hiệu, logo, phong cách giống tổ chức thật, thêm các yếu tố khẩn cấp/hấp dẫn.
3) Gửi đồng loạt hoặc có chọn lọc tới danh sách nạn nhân.
4) Nạn nhân tương tác (click link, điền form, mở file), từ đó:

    - Thông tin đăng nhập/mã OTP bị đánh cắp.
    - Thiết bị bị cài malware/keylogger/ransomware.
    - Tài khoản bị chiếm quyền, sử dụng tiếp để lừa thêm người khác.

I.2.5. Hậu quả

- Mất tiền**,** mất quyền kiểm soát tài khoản ngân hàng, ví điện tử, tài khoản game, tài khoản sàn thương mại.
- Rò rỉ dữ liệu nhạy cảm**:** danh sách khách hàng, dữ liệu nội bộ doanh nghiệp.
- Chiếm quyền email/mạng xã hội → tiếp tục lừa người quen, làm tổn hại uy tín cá nhân/tổ chức.
- Với doanh nghiệp, có thể dẫn đến tấn công sâu hơn vào hệ thống nội bộ**,** cài ransomware, đánh cắp bí mật kinh doanh.

I.2.6. Dấu hiệu nhận biết và phòng chống

Cách nhận biết:

1) Địa chỉ gửi email/tin nhắn gần giống nhưng không hoàn toàn trùng với địa chỉ chính thức.
2) Nội dung quá khẩn cấp, đe dọa hoặc hứa hẹn lợi ích phi lý**.**
3) Đòi hỏi người dùng phải: Cung cấp mật khẩu, mã OTP, thông tin thẻ, nhấp vào link lạ, tải file lạ, thanh toán/phí "nhỏ" để nhận phần thưởng lớn.
4) URL thật khi rê chuột vào liên kết không khớp với tên miền chính thức.

Biện pháp phòng chống (đi từ cá nhân đến tổ chức):

1) Nâng cao nhận thức**:** đào tạo người dùng về social engineering, thường xuyên cập nhật các mẫu phishing mới.
2) Không chia sẻ mật khẩu, mã OTP qua email/tin nhắn/cuộc gọi – tổ chức uy tín *không bao giờ* yêu cầu thông tin này.
3) Kiểm tra kỹ URL trước khi đăng nhập, ưu tiên gõ tay địa chỉ chính thức thay vì click link.
4) Kích hoạt xác thực đa yếu tố (MFA) cho tài khoản quan trọng.

5) Doanh nghiệp triển khai: Bộ lọc email anti-phishing, lọc spam, hệ thống siêu giám sát truy cập, chặn website độc hại, chính sách quy trình xác thực trước các yêu cầu chuyển tiền, chia sẻ dữ liệu (ví dụ gọi lại số đã lưu sẵn, không dùng số trong email).

I.3. Vishing

I.3.1. Khái niệm

Vishing (viết tắt của *voice phishing*) là hình thức tấn công social engineering thông qua cuộc gọi thoại, voicemail, hoặc tin nhắn thoại. Kẻ tấn công sử dụng giọng nói và kịch bản lừa đảo để thuyết phục nạn nhân tiết lộ thông tin nhạy cảm (thông tin ngân hàng, mã OTP, thông tin cá nhân…) hoặc thực hiện các hành vi có hại (cài app lạ, truy cập website độc hại, chuyển tiền).

Các hãng bảo mật như Cisco, Trend Micro, CrowdStrike đều xếp vishing là một dạng social engineering nguy hiểm đang tăng nhanh, vì tận dụng sự tin tưởng vào giọng nói con người và khả năng tạo áp lực tâm lý trực tiếp trong thời gian thực.

I.3.2. Đặc điểm

- Kênh tấn công: cuộc gọi qua điện thoại, VoIP, ứng dụng OTT (Skype, WhatsApp, Zalo…), đôi khi là voicemail ghi sẵn.

- Giả mạo số gọi (caller ID spoofing): số hiển thị giống tổng đài ngân hàng, công an, cơ quan nhà nước, công ty viễn thông…

- Kịch bản được chuẩn bị kỹ: kẻ tấn công nói năng chuyên nghiệp, sử dụng đúng thuật ngữ, xưng danh đúng chức vụ để tạo niềm tin.

- Khai thác cảm xúc mạnh:

  - Sợ hãi (nợ thuế, vi phạm pháp luật, tài khoản bị hack…).
  - Tham (trúng thưởng, hoàn tiền, ưu đãi lớn…).
  - Gấp gáp (phải xử lý "ngay lập tức", "trong vòng vài phút").

Ngày nay, vishing còn đáng lo hơn vì có thể kết hợp AI tạo giọng nói và tạo hình ảnh (*Vishing AI*) để bắt chước tiếng nói, hình ảnh người thật, thậm chí là người thân hoặc lãnh đạo công ty, khiến nạn nhân càng khó phân biệt.

I.3.3. Một số kịch bản Vishing thường gặp

1) Giả mạo ngân hàng/nhân viên chống lừa đảo : Thông báo có giao dịch bất thường, yêu cầu cung cấp mã OTP, số thẻ, CVV để "xác minh" hoặc yêu cầu cài ứng dụng điều khiển từ xa để "hỗ trợ xử lý".

2) Giả mạo cơ quan nhà nước/công an/viện kiểm sát: Gọi thông báo nạn nhân liên quan đến vụ án, rửa tiền… yêu cầu nạn nhân "chứng minh vô tội" bằng cách chuyển tiền vào "tài khoản an toàn", hoặc cung cấp thông tin ngân hàng.

3) Giả mạo nhân sự/giám đốc trong doanh nghiệp: Dùng giọng deepfake giả lãnh đạo yêu cầu nhân viên kế toán chuyển gấp một khoản tiền, hoặc cung cấp dữ liệu nhạy cảm cho đối tác.

I.3.4. Hậu quả

- Nạn nhân có thể mất sạch tiền trong tài khoản, vay nợ đứng tên mà không hay biết.
- Bị chiếm đoạt danh tính (identity theft): kẻ tấn công dùng thông tin thu được để mở tài khoản, vay tiền, đăng ký dịch vụ trái phép.
- Ở cấp tổ chức, vishing có thể dẫn đến tấn công lừa chuyển tiền (business email compromise/vishing) gây thiệt hại hàng triệu đô.

I.3.5. Dấu hiệu nhận biết và phòng chống

Cách nhận biết:

1) Cuộc gọi/tin nhắn thoại không mong đợi**,** nhưng yêu cầu: Cung cấp thông tin nhạy cảm (mật khẩu, OTP, mã PIN…), cài đặt phần mềm lạ, truy cập link lạ, chuyển tiền gấp, tuyệt đối không được chậm trễ.
2) Người gọi tạo áp lực mạnh: đe dọa liên quan đến pháp luật, tài khoản bị khóa, bị trừ tiền.
3) Số gọi không trùng hoàn toàn với số công bố chính thức (hoặc trùng nhưng vẫn phải cẩn trọng vì số có thể bị spoof).

Biện pháp phòng chống:

1) Nguyên tắc vàng**:** Không cung cấp mật khẩu, mã OTP, mã PIN qua điện thoại trong bất kỳ trường hợp nào.
2) Khi nhận cuộc gọi khả nghi: Cúp máy, tự gọi lại vào số tổng đài chính thức được ghi trong website/ứng dụng chính thức, *không dùng số trong cuộc gọi/tin nhắn.*
3) Không cài đặt ứng dụng điều khiển từ xa/ứng dụng tài chính không rõ nguồn gốc theo yêu cầu của người gọi.

4) Doanh nghiệp cần: Ban hành quy trình xác thực nội bộ trước khi thực hiện yêu cầu chuyển tiền, chia sẻ dữ liệu (yêu cầu xác nhận qua nhiều kênh, nhiều cấp). Đào tạo nhân viên về vishing và deepfake voice, đưa ví dụ thực tế để họ dễ nhận diện.

I.4. Baiting

I.4.1. Khái niệm

Baiting là một hình thức tấn công social engineering trong đó kẻ tấn công dùng "mồi nhử" hấp dẫn (quà tặng, phần mềm miễn phí, ưu đãi lớn, thông tin "nóng", tài liệu "mật") để kích thích lòng tham, sự tò mò hoặc nhu cầu của nạn nhân, khiến họ thực hiện hành động dẫn đến: Cài đặt malware, tiết lộ thông tin hoặc truy cập vào hệ thống/thiết bị trái phép.

Các tài liệu về an ninh mạng mô tả baiting là một trong những kỹ thuật tận dụng mạnh nhất tâm lý tò mò và ham lợi, thường núp dưới các đề nghị như "miễn phí", "giảm giá lớn", "nội dung độc quyền".

I.4.2. Đặc điểm

- Luôn có "mồi": thứ gì đó có vẻ có lợi, hấp dẫn, khó cưỡng (phần mềm trả phí nhưng được cho tải miễn phí, USB ghi "data lương tháng", "bảng điểm", "hình nóng", "hợp đồng khách hàng"…).
- Hành động do chính nạn nhân tự làm: tự cắm USB, tự tải file, tự nhập thông tin vì nghĩ mình đang hưởng lợi.
- Có thể ở dạng vật lý hoặc dạng số (online).

I.4.3. Các dạng Baiting phổ biến

a) Baiting dạng vật lý (physical baiting)

- Kẻ tấn công cố ý để lại USB, ổ cứng di động, CD/DVD ở nơi có nhân viên mục tiêu (bãi xe, thang máy, phòng họp, quán café gần công ty...).
- Thiết bị được dán nhãn hấp dẫn:
    - "Danh sách lương tháng 12"
    - "Thông tin khách hàng – bảo mật"
    - "Ảnh nội bộ – không chia sẻ"
- Khi một nhân viên tò mò nhặt lên và cắm vào máy công ty, malware từ USB có thể lây lan vào hệ thống nội bộ.

b) Baiting dạng số (digital baiting)

- Website/ứng dụng/email chào mời:
    - Download phần mềm trả phí nhưng free, bản crack game, phần mềm văn phòng.
    - Nhận voucher, phiếu giảm giá, thẻ quà tặng nếu đăng nhập/tải file.
    - Xem nội dung "nóng", "tin nội bộ", "tài liệu leak" nếu click link.
- Thực chất liên kết đó:
    - Cài malware vào máy.
    - Thu thập thông tin tài khoản khi người dùng đăng nhập.
    - Gắn cookie theo dõi hoặc thêm vào botnet.

I.4.4. Hậu quả

- Máy tính, thiết bị bị nhiễm malware (trojan, spyware, ransomware…).
- Mất dữ liệu, rò rỉ thông tin cá nhân hoặc thông tin doanh nghiệp.
- Trong môi trường doanh nghiệp, một hành vi baiting thành công có thể trở thành điểm xâm nhập đầu tiên (entry point) cho các cuộc tấn công lớn hơn.

I.4.5. Dấu hiệu nhận biết và phòng chống

Cách nhận biết:

1) Đề nghị "quá tốt để là thật": phần mềm đắt tiền nhưng cho miễn phí, quà tặng giá trị lớn với yêu cầu rất nhỏ.
2) Thiết bị lạ xuất hiện ở vị trí nhạy cảm, kèm nhãn mác "giật gân".
3) Website/tin quảng cáo yêu cầu tải file từ nguồn không chính thức, hoặc yêu cầu đăng nhập tài khoản để "nhận quà".

Biện pháp phòng chống:

1) Không bao giờ cắm USB/thiết bị lạ vào máy tính làm việc, đặc biệt là trong môi trường doanh nghiệp.
2) Chỉ tải phần mềm từ nguồn chính thống (trang nhà sản xuất, store uy tín), không dùng crack, keygen.
3) Tổ chức cần: Xây dựng quy định sử dụng thiết bị lưu trữ, áp dụng cơ chế quét tự động khi cắm USB. Đào tạo nhân viên về rủi ro của "mồi miễn phí", đưa ví dụ thực tế để nhận diện tốt hơn. Triển khai các giải pháp bảo mật như antivirus, EDR, DLP, phân quyền truy cập để hạn chế thiệt hại khi một máy bị nhiễm.

CHƯƠNG II. MỘT SỐ VÍ DỤ THỰC TẾ TẠI VIỆT NAM

II.1. Social Engineering trong đời sống hằng ngày

II.1.1. Giả mạo nhân viên giao hàng

Trong thời gian gần đây, các hành vi lừa đảo thông qua hình thức mạo danh nhân viên giao hàng (shipper) đang có xu hướng gia tăng, đặc biệt trong lĩnh vực mua sắm trực tuyến. Lợi dụng thói quen mua hàng online của người dân, các đối tượng đã nghĩ ra nhiều cách tinh vi nhằm chiếm đoạt tài sản hoặc đánh cắp thông tin ngân hàng của nạn nhân.

Mặc dù hình thức giả danh shipper từng xuất hiện trước đây, song những thủ đoạn này liên tục được thay đổi và kết hợp với nhiều yếu tố tâm lý, khiến người tiêu dùng khó nhận biết và dễ bị đánh lừa.

Quá trình lừa đảo thường diễn ra khi nạn nhân – thường là người đang chờ đơn hàng – nhận được cuộc gọi hoặc tin nhắn từ một người tự xưng là nhân viên giao hàng. Đối tượng sẽ thông báo rằng đơn hàng đang trong quá trình vận chuyển và yêu cầu người nhận thanh toán trước một khoản phí nhỏ, dao động từ vài chục đến vài trăm nghìn đồng. Những lý do được đưa ra nghe có vẻ hợp lý, chẳng hạn như "phí xác nhận đơn" hoặc "phí bắt buộc theo quy định mới của bưu cục".

Trên thực tế, các khoản phí này chỉ là cái bẫy được dựng lên nhằm tạo lòng tin và đánh vào tâm lý người mua. Từ đó, kẻ gian dễ dàng lợi dụng sơ hở để chiếm đoạt tài sản hoặc truy cập trái phép vào tài khoản ngân hàng của nạn nhân.

Giả mạo nhân viên shipper

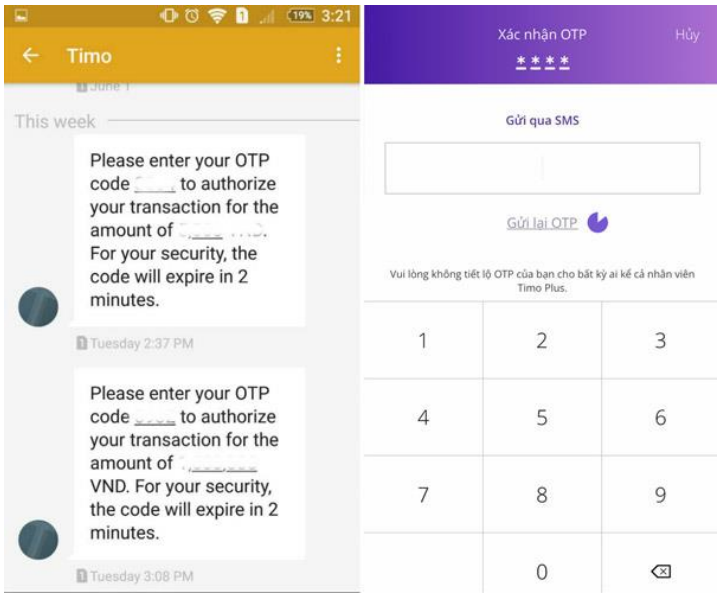
Để tạo sự tin tưởng nơi nạn nhân, các đối tượng lừa đảo thường sử dụng những thủ đoạn tinh vi như giả mạo hóa đơn, mã vận đơn hoặc đường dẫn đến các trang web được thiết kế giống hệt website của những đơn vị vận chuyển uy tín như GHTK hay Viettel Post. Tất cả đều được chuẩn bị một cách chuyên nghiệp nhằm đánh lừa thị giác và tâm lý người dùng.

Do số tiền yêu cầu thường nhỏ và người mua đang trong tâm thế mong chờ nhận hàng, nhiều người đã mất cảnh giác, dễ dàng thực hiện chuyển khoản theo hướng dẫn của kẻ gian.

Sau khi giao dịch hoàn tất, đối tượng lừa đảo tiếp tục triển khai bước tiếp theo của kịch bản. Chúng sẽ liên hệ lại với nạn nhân, giả vờ lo lắng và thông báo rằng việc chuyển tiền vừa rồi đã xảy ra nhầm lẫn, đe dọa việc này sẽ làm mất tiền trong tài khoản ngân hàng của nạn nhân.

Khi nạn nhân rơi vào trạng thái hoang mang trước nguy cơ phải chịu một khoản tiền có thể bị mất quá lớn, thủ phạm nhanh chóng chuyển vai thành "người giúp đỡ" và đề xuất một biện pháp xử lý tức thì: yêu cầu nạn nhân truy cập vào một đường dẫn để "hủy" hay "vô hiệu hóa" giao dịch.

Mục tiêu thực sự của kẻ gian là dẫn dắt nạn nhân tới một trang web giả mạo, nơi họ bị bắt buộc cung cấp các thông tin nhạy cảm — bao gồm dữ liệu cá nhân, tên đăng nhập, mật khẩu và đặc biệt là mã xác thực giao dịch (OTP) của ngân hàng. Một khi **mã OTP** bị lộ, kẻ lừa đảo có thể chiếm quyền kiểm soát tài khoản, thực hiện các giao dịch bất hợp pháp và rút hết tiền của nạn nhân.



Mã OTP ngân hàng cần bảo mật cẩn thận

II.1.2. Câu chuyện "ngân hàng gọi điện"

Một hình thức lừa đảo khác cũng đang được các đối tượng tội phạm mạng sử dụng phổ biến là **mạo danh nhân viên ngân hàng**. Trong kịch bản này, kẻ tấn công thường gọi điện hoặc nhắn tin cho nạn nhân, tự xưng là nhân viên của một ngân hàng uy tín và thông báo rằng "tài khoản của quý khách đang có dấu hiệu bị xâm nhập".

Bằng giọng điệu khẩn trương và thuyết phục, chúng tạo cảm giác cấp bách, khiến nạn nhân tin rằng tài khoản của mình thật sự đang gặp nguy hiểm. Sau đó, chúng yêu cầu nạn nhân cung cấp **mã OTP** với lý do "xác minh danh tính" hoặc

“ngăn chặn giao dịch lạ”. Do lo sợ bị mất tiền, nhiều người đã vội vàng làm theo hướng dẫn mà không kịp kiểm chứng thông tin.

Giả danh nhân viên ngân hàng

Thực chất, mã OTP là lớp bảo mật cuối cùng để xác nhận giao dịch trực tuyến. Một khi nạn nhân tiết lộ mã này, kẻ lừa đảo có thể ngay lập tức truy cập vào tài khoản ngân hàng, thực hiện chuyển khoản hoặc chiếm đoạt toàn bộ số dư. Không ít trường hợp, chỉ trong vài phút sau khi đọc mã OTP, nạn nhân đã bị rút sạch tiền mà không thể kịp can thiệp.

Hình thức lừa đảo này nguy hiểm ở chỗ nó **khai thác tâm lý sợ hãi và tin tưởng vào uy tín của ngân hàng**, khiến người dùng khó nhận ra mình đang bị thao túng. Việc nhận diện và cảnh giác trước những cuộc gọi hay tin nhắn bất thường là vô cùng cần thiết để bảo vệ an toàn thông tin tài chính cá nhân.

II.1.3. Giả mạo cơ quan nhà nước

Một chiêu thức lừa đảo khác lợi dụng uy tín của các cơ quan chức năng là **mạo danh “Công an điều tra”** qua thư điện tử. Trong kịch bản này, nạn nhân nhận được một email giả mạo mang tính chính thức, thông báo về việc bị “gửi giấy mời” hoặc “bị truy thu/nợ phạt”, kèm theo một đường liên kết được gắn nhãn là “tra cứu hồ sơ” hoặc “xem chi tiết quyết định”. Giao diện email và nội dung thường được soạn thảo cẩn thận, mô phỏng ngôn ngữ hành chính và các yếu tố nhận diện (logo, con dấu, chữ ký) để tăng mức độ thuyết phục.

Khi người nhận bấm vào đường link, họ được dẫn đến một trang web giả mạo có giao diện gần giống trang của cơ quan nhà nước. Tại đây, nạn nhân được yêu cầu nhập các thông tin cá nhân nhạy cảm (họ tên, số CMND/CCCD, ngày sinh), thậm chí thông tin tài khoản ngân hàng hoặc mã OTP với lý do “xác minh hồ sơ” hoặc “nộp phạt trực tuyến”. Một khi thông tin này bị lộ, kẻ gian có thể sử dụng để thực hiện hành vi đăng nhập, mạo danh, hoặc rút tiền, đồng thời tiến hành các hành vi lừa đảo tiếp theo nhắm vào mạng lưới quan hệ của nạn nhân.

Tải app Vneid giả mạo

Về mặt phân tích tâm lý, thủ đoạn này khai thác hai yếu tố chính: niềm tin vào thẩm quyền nhà nước và nỗi sợ hệ quả pháp lý. Sự kết hợp giữa ngôn ngữ hành chính nghiêm túc và yếu tố đe dọa (ví dụ: "hạn chót", "hình phạt") làm tăng áp lực khiến người nhận ít kiểm chứng kỹ lưỡng trước khi hành động. Về hậu quả, ngoài thiệt hại về tài chính trực tiếp, nạn nhân còn phải đối mặt với nguy cơ bị lợi dụng danh tính trong các tội phạm khác, tổn hại uy tín cá nhân và phức tạp trong quá trình phục hồi quyền lợi, tố tụng hoặc khôi phục tài khoản.

II.2. Social Engineering trong môi trường công sở hoặc tổ chức

II.2.1. Tấn công qua email (phishing email)

Kịch bản tấn công thông qua email mạo danh lãnh đạo hoặc đối tác thường đi kèm với một tệp đính kèm tinh vi được ngụy trang dưới dạng "hợp đồng", "báo giá" hoặc "tài liệu dự án". Khi nhân viên mở tệp này, mã độc (ví dụ: backdoor, ransomware, hoặc trình ghi phím) có thể được kích hoạt và cài đặt âm thầm vào hệ thống nội bộ. Sau khi mã độc triển khai thành công, kẻ tấn công có thể mở cửa hậu truy cập, theo dõi trao đổi nội bộ, đánh cắp dữ liệu nhạy cảm, can thiệp vào quy trình tài chính hoặc mã hóa hệ thống để tống tiền.

Phishing email

Về phương thức kỹ thuật, tệp đính kèm có thể khai thác lỗ hổng phần mềm (macro trong tài liệu Office, lỗ hổng trong trình đọc PDF, hoặc payload thực thi qua file nén) để giảm thiểu tương tác của nạn nhân và tránh bị phát hiện. Ở mức chiến lược, BEC kết hợp yếu tố xã hội—mạo danh người có thẩm quyền, sử dụng ngôn ngữ vội vàng và chỉ rõ nhiệm vụ—để khiến nhân viên bỏ qua các quy trình xác thực thông thường.

Hệ quả đối với tổ chức bao gồm: mất mát tài sản và dữ liệu, gián đoạn hoạt động, tổn hại uy tín và chi phí phục hồi cao (khôi phục hệ thống, điều tra pháp lý, đền bù khách hàng).

II.2.2. "Dumpster diving" (lục thùng rác lấy thông tin)

Kẻ tấn công thường khai thác các tài liệu bị vứt bỏ không đúng cách — chẳng hạn hóa đơn, ghi chú chứa mật khẩu, bản in nháp hoặc các giấy tờ có thông tin nhạy cảm. Bằng cách thu thập và phân tích những mảnh thông tin này, chúng có thể phục hồi dữ liệu đăng nhập, chi tiết tài khoản hoặc manh mối dẫn tới các hệ thống quan trọng của tổ chức. Hành động tưởng chừng đơn giản này thường là bước đầu trong một chuỗi tấn công phức hợp, vì thông tin thu được từ rác thải có thể được sử dụng để thực hiện tấn công kỹ thuật (đăng nhập trái phép, tấn công giả mạo) hoặc để xã hội hóa, mạo danh nhằm vượt qua các cơ chế bảo mật khác.

II.3. Social Engineering trên mạng xã hội

II.3.1. Lừa đảo qua quà tặng hoặc mini game

Các trang Facebook, tài khoản Zalo lạ giả mạo mạo danh các thương hiệu lớn (ví dụ: Shopee, Tiki, FPT) thường tổ chức các chương trình "minigame" tuyển người nhận quà nhằm thu hút tương tác. Những chiến dịch này yêu cầu người tham gia cung cấp thông tin cá nhân như số điện thoại và địa chỉ, thậm chí yêu cầu nhập mã xác thực (OTP) dưới danh nghĩa "xác nhận trúng thưởng". Khi người dùng

cung cấp các dữ liệu này, kẻ gian có thể thu thập và khai thác để chiếm đoạt tài khoản, thực hiện hành vi lừa đảo tiếp theo hoặc truy cập các dịch vụ tài chính liên quan.

Lừa đảo bằng minigame

II.3.2. Deepfake video / giọng nói

Sự tiến bộ nhanh chóng của các công nghệ tạo nội dung nhân tạo (AI-generated content) đã mở ra kênh tấn công mới cho tội phạm: tạo video hoặc giọng nói mô phỏng chính xác người thật — thường là lãnh đạo, đồng nghiệp hoặc người thân của nạn nhân. Kẻ tấn công khai thác các mẫu âm thanh, video công khai hoặc dữ liệu thu thập được để huấn luyện mô hình, từ đó tạo ra các bản sao giọng nói hoặc đoạn phim có vẻ chân thực.

Trong kịch bản tấn công, kẻ gian có thể phát tán một đoạn gọi thoại/clip video giả mạo yêu cầu chuyển tiền gấp, phê duyệt giao dịch, hoặc yêu cầu gửi tài liệu mật. Do thông điệp xuất phát từ "giọng nói / hình ảnh" của người có thẩm quyền, nạn nhân hoặc nhân viên có khuynh hướng hành động mà không kiểm chứng kỹ lưỡng. Mức độ nguy hiểm của phương thức này nằm ở tính thuyết phục

cao (giảm khả năng nghi ngờ) và tốc độ triển khai — các quyết định tài chính hoặc chia sẻ thông tin có thể diễn ra trong vài phút sau khi nhận được yêu cầu.

Deepfake video/giọng nói

Về mặt kỹ thuật, hai dạng chính thường gặp là:

- Giả giọng (voice cloning): tái tạo màu giọng, ngữ điệu và cách phát âm bằng mô hình chuyển đổi giọng nói;

- Giả video (deepfake): hoán đổi khuôn mặt hoặc tổng hợp chuyển động môi để khớp với âm thanh, tạo ấn tượng rằng người thật đang phát ngôn.

Ngoài thiệt hại tài chính trực tiếp (chuyển tiền, lộ thông tin ngân hàng), deepfake còn có thể dẫn tới: mất mát thông tin nhạy cảm, phá hoại uy tín cá nhân/đơn vị, leo thang xung đột nội bộ do mạo danh phát ngôn, và làm suy giảm niềm tin vào kênh giao tiếp điện tử trong tổ chức. Việc truy vết và chứng minh nguồn gốc nội dung giả mạo đôi khi phức tạp và tốn kém, làm chậm phản ứng khắc phục.

II.3.3. Lừa tình cảm (romance scam)

Kịch bản điển hình bắt đầu khi kẻ gian tiếp cận nạn nhân qua các nền tảng hẹn hò hoặc mạng xã hội, xây dựng mối quan hệ thân mật bằng cách trò chuyện thường xuyên, tỏ ra quan tâm và chia sẻ cảm xúc nhằm tạo dựng lòng tin. Sau khi chiếm được vị trí tình cảm trong lòng nạn nhân, họ dần chuyển sang kịch bản đòi hỏi hỗ trợ tài chính với những lý do dễ đồng cảm như đang bệnh nặng, cần tiền chữa trị, muốn gửi quà nhưng gặp rắc rối ở khâu vận chuyển, hoặc cần kinh phí làm visa/giấy tờ. Nhân tố cảm xúc—niềm tin, thương cảm và hy vọng—làm suy giảm khả năng phán đoán, khiến nhiều người sẵn sàng chuyển tiền hoặc cung cấp thông tin nhạy cảm.

Lừa tình cảm (romance scam)

Về hậu quả, ngoài tổn thất tài chính trực tiếp, nạn nhân còn phải chịu tổn thương tinh thần, xâm phạm quyền riêng tư và nguy cơ bị lợi dụng thông tin cá nhân cho các hành vi phạm pháp tiếp theo (ví dụ: mạo danh, rửa tiền). Hình thức này thường được thực hiện tinh vi, kéo dài nhiều tháng để tối đa hóa lợi ích cho kẻ gian và làm cho việc thu hồi thiệt hại càng trở nên khó khăn.

CHƯƠNG III. PHÂN TÍCH YẾU TỐ TÂM LÝ BỊ KHAI THÁC

III.1. Cơ sở thần kinh học và hành vi tư duy

III.1.1. Mô hình tư duy kép của Kahneman và Hệ thống xử lý thông tin (Dual-Process Theory)

Đây là nền tảng cốt lõi để hiểu sự dễ bị tổn thương của con người.

- Hệ thống 1 (Tư duy nhanh, Cảm tính): Hoạt động tự động, bản năng, dựa trên kinh nghiệm và cảm xúc. Nó cực kỳ hiệu quả cho các tác vụ hàng ngày nhưng dễ mắc lỗi khi đối mặt với thông tin mới hoặc bị làm sai lệch.

- **Cơ chế thần kinh:** Chủ yếu liên quan đến Amygdala (phản ứng cảm xúc), Hạch nền (thói quen) và vỏ não cảm giác.
- **Cách bị khai thác:** Kẻ tấn công thiết kế các kịch bản kích hoạt Hệ thống 1 bằng cách sử dụng các hình ảnh quen thuộc, các câu lệnh khẩn cấp, hoặc các yếu tố gây sốc để tránh tư duy phản biện.

- Hệ thống 2 (Tư duy chậm, Logic): Đòi hỏi sự tập trung, phân tích, tính toán và tốn nhiều năng lượng nhận thức. Đây là "người gác cổng" của lý trí.

- **Cơ chế thần kinh:** Chủ yếu liên quan đến vỏ não trước trán (Prefrontal Cortex) – trung tâm ra quyết định, giải quyết vấn đề.
- **Cách bị khai thác:** Mọi kỹ thuật Social Engineering đều nhắm vào việc **vô hiệu hóa hoặc làm quá tải Hệ thống 2**, khiến nạn nhân phải hành động dựa trên Hệ thống 1 đầy sơ hở.

III.1.2. Phản ứng "Chiến đấu hoặc Bỏ chạy" (Fight-or-Flight Response) và sự "Bắt cóc" Amygdala (Amygdala Hijack)

Đây là cơ chế sinh học mạnh mẽ nhất mà kẻ tấn công khai thác.

- Bản chất: Khi đối mặt với nguy hiểm, tuyến thượng thận giải phóng hormone cortisol và adrenaline. Những hormone này làm tăng nhịp tim, huyết áp và chuyển máu từ các vùng não lý trí (vỏ não trước trán) đến các vùng não nguyên thủy (hạch hạnh nhân - Amygdala).

- Yếu tố bị khai thác: Sự sợ hãi tột độ và **áp lực thời gian**.

- Phân tích sâu: Kẻ tấn công tạo ra các kịch bản đe dọa trực tiếp đến an toàn tài chính, danh tiếng, hoặc thậm chí là pháp luật. Khi nạn nhân nhận được thông báo *"Tài khoản của bạn sẽ bị khóa vĩnh viễn trong 5 phút nếu không xác thực"* hoặc *"Bạn bị cáo buộc rửa tiền, hãy chuyển tiền vào tài khoản an toàn để điều tra"*, cơ thể sẽ phản ứng như thể đang gặp nguy hiểm vật lý. Lý trí bị "tắt", và nạn nhân hành động theo bản năng để thoát khỏi mối đe dọa ngay lập tức, thường là làm theo chỉ dẫn của kẻ tấn công.

III.2. Các thiên kiến nhận thức và lỗ hổng xử lý thông tin

III.2.1. Thiên kiến xác nhận (Confirmation Bias)

- **Bản chất:** Con người có xu hướng tìm kiếm, diễn giải và ghi nhớ thông tin theo cách xác nhận những gì họ đã tin hoặc mong đợi.
- **Yếu tố bị khai thác:** Sự kỳ vọng và niềm tin nội tại của cá nhân.
- **Phân tích sâu:** Nếu một nhân viên đang mong chờ một email quan trọng về dự án, họ sẽ dễ dàng bỏ qua các dấu hiệu bất thường (lỗi chính tả, địa chỉ email lạ) trong một email giả mạo có tiêu đề tương tự. Não bộ của họ đã "tiền xử lý" thông tin là hợp lệ vì nó khớp với mong muốn.

III.2.2. Thiên kiến lạc quan (Optimism Bias)

- **Bản chất:** Con người có xu hướng tin rằng mình ít có khả năng gặp phải những điều tồi tệ hơn người khác.
- **Yếu tố bị khai thác:** Sự tự tin thái quá và cảm giác "miễn nhiễm" với rủi ro.

- **Phân tích sâu:** Nhiều người dùng nghĩ rằng: "Tôi đủ thông minh để không bị lừa đâu", hoặc "Những vụ hack chỉ xảy ra với công ty lớn". Sự tự mãn này dẫn đến việc bỏ qua các biện pháp bảo mật cơ bản như cập nhật phần mềm, sử dụng mật khẩu mạnh, hoặc cẩn trọng khi mở link lạ.

III.2.3. Hiệu ứng Dunning-Kruger (Dunning-Kruger Effect)

- **Bản chất:** Những người có năng lực thấp trong một lĩnh vực thường có xu hướng đánh giá quá cao khả năng của mình, trong khi những người có năng lực cao lại có xu hướng đánh giá thấp hơn.
- **Yếu tố bị khai thác:** Sự thiếu hiểu biết kèm theo tự mãn.
- **Phân tích sâu:** Người dùng có ít kiến thức về an ninh mạng có thể không nhận ra sự phức tạp của các mối đe dọa, dẫn đến việc họ tin rằng mọi email có thể dễ dàng được phân biệt là thật hay giả. Điều này khiến họ trở thành mục tiêu dễ dàng cho các cuộc tấn công tinh vi.

III.2.4. Sự suy giảm ý chí (Decision Fatigue)

- **Bản chất:** Khả năng ra quyết định đúng đắn của con người là một tài nguyên có hạn và có thể cạn kiệt theo thời gian hoặc khi đối mặt với nhiều lựa chọn.
- **Yếu tố bị khai thác:** Trạng thái mệt mỏi tinh thần do công việc hoặc căng thẳng.
- **Phân tích sâu:** Cuối một ngày làm việc dài, khi đã phải đưa ra hàng trăm quyết định lớn nhỏ, người dùng dễ dàng lơ là cảnh giác. Một thông báo yêu cầu "xác thực" tài khoản vào lúc này sẽ được xử lý nhanh chóng bằng Hệ thống 1, vì Hệ thống 2 đã "cạn pin".

III.3. Các yếu tố tâm lý xã hội và hành vi ảnh hưởng

III.3.1. Các nguyên tắc thuyết phục của Robert Cialdini

Các nguyên tắc này là nền tảng của mọi hành vi thao túng xã hội và bị khai thác triệt để trong Social Engineering.

III.3.1.1. Sự đáp đền (Reciprocity)

- **Bản chất:** Con người cảm thấy có nghĩa vụ phải trả ơn khi nhận được một đặc ân hoặc món quà.
- **Yếu tố bị khai thác:** Sự tử tế giả tạo hoặc cung cấp thông tin/lợi ích nhỏ.
- **Phân tích sâu:** Kẻ tấn công có thể giả vờ giúp đỡ nạn nhân giải quyết một vấn đề (ví dụ: cung cấp "phần mềm miễn phí" để sửa lỗi máy tính) và sau đó yêu cầu một "ân huệ nhỏ" đổi lại (ví dụ: thông tin đăng nhập để "kiểm tra hệ thống").

III.3.1.2. Sự cam kết và nhất quán (Commitment and Consistency)

- **Bản chất:** Con người có nhu cầu tâm lý mạnh mẽ để duy trì sự nhất quán với những gì họ đã nói hoặc làm trước đó.
- **Yếu tố bị khai thác:** Các cam kết nhỏ ban đầu.
- **Phân tích sâu:** Một kẻ tấn công qua điện thoại có thể bắt đầu bằng việc hỏi những câu hỏi đơn giản như "Bạn có khỏe không?", "Công việc của bạn có tốt không?". Khi nạn nhân đã trả lời "có" một vài lần, họ sẽ khó lòng từ chối các yêu cầu tiếp theo vì muốn duy trì hình ảnh "hợp tác" của mình.

III.3.1.3. Bằng chứng xã hội (Social Proof)

- **Bản chất:** Khi không chắc chắn, chúng ta nhìn vào hành vi của người khác để định hướng hành vi của mình.
- **Yếu tố bị khai thác:** Sự đồng thuận giả mạo hoặc thông tin sai lệch về số đông.
- **Phân tích sâu:** Các trang web lừa đảo thường hiển thị "hàng ngàn người đã trúng thưởng" hoặc "x người đã đầu tư thành công" để tạo cảm giác an toàn và khuyến khích nạn nhân tham gia.

III.3.1.4. Sự thiện cảm (Liking)

- **Bản chất:** Chúng ta dễ dàng bị thuyết phục bởi những người mà chúng ta thích, quen biết hoặc thấy có điểm chung.
- **Yếu tố bị khai thác:** Mối quan hệ giả tạo và sự tương đồng.
- **Phân tích sâu:** Kẻ tấn công dành thời gian tìm hiểu sở thích, quan điểm của mục tiêu qua mạng xã hội, sau đó giả vờ là một người có cùng sở thích, cùng hoàn cảnh để xây dựng mối quan hệ "bạn bè".

III.3.1.5. Sự khan hiếm (Scarcity)

- **Bản chất:** Con người có xu hướng khao khát những thứ hiếm có hoặc có giới hạn.
- **Yếu tố bị khai thác:** Tạo cảm giác "cơ hội duy nhất" hoặc "số lượng có hạn".
- **Phân tích sâu:** Các thông báo như "Chỉ còn 3 suất học bổng cuối cùng" hoặc "Mã giảm giá chỉ có hiệu lực trong 1 giờ" kích hoạt bản năng sợ mất mát (Loss Aversion), khiến nạn nhân hành động vội vàng mà không cân nhắc kỹ.

III.3.2. Hiệu ứng người đứng xem (Bystander Effect) và sự phân tán trách nhiệm

- **Bản chất:** Trong một nhóm, trách nhiệm của mỗi cá nhân giảm đi khi có nhiều người khác có thể hành động.
- **Yếu tố bị khai thác:** Môi trường tổ chức lớn, nơi trách nhiệm bảo mật không được cá nhân hóa.
- **Phân tích sâu:** Trong một công ty, khi một email đáng ngờ được gửi tới toàn thể nhân viên, mỗi người có thể nghĩ rằng "chắc chắn bộ phận IT hoặc đồng nghiệp khác đã kiểm tra rồi". Điều này tạo ra một "điểm mù tập thể" mà kẻ tấn công có thể lợi dụng để thâm nhập.

III.4. Các yếu tố hóc-môn và cảm xúc

III.4.1. Vai trò của Dopamine trong việc kích thích lòng tham và sự tò mò

- **Bản chất:** Dopamine là hormone "mong đợi phần thưởng". Nó được giải phóng khi chúng ta dự đoán một điều gì đó thú vị hoặc có lợi.
- **Yếu tố bị khai thác: Lòng tham (Greed)** và **Sự tò mò (Curiosity)**.
- **Phân tích sâu:** Khi nạn nhân nhận được thông báo "Bạn đã trúng thưởng 1 tỷ đồng!" hoặc "Xem những bức ảnh bị lộ của người nổi tiếng!", Dopamine được giải phóng, tạo ra cảm giác hưng phấn và thôi thúc hành động để "nhận" phần thưởng hoặc "thỏa mãn" sự tò mò, bất chấp mọi rủi ro về bảo mật.

III.4.2. Cortisol và Adrenaline - Khi stress làm mờ lý trí

- **Bản chất:** Đây là các hormone stress. Khi được giải phóng, chúng gây ra sự tập trung hẹp vào mối đe dọa trực tiếp và làm giảm khả năng tư duy dài hạn.
- **Yếu tố bị khai thác:** Các tình huống đe dọa trực tiếp đến cuộc sống, công việc.
- **Phân tích sâu:** Một cuộc gọi giả mạo từ cảnh sát yêu cầu chuyển tiền gấp để "chứng minh sự vô tội" sẽ làm tăng mức cortisol và adrenaline của nạn nhân. Dưới tác động của stress, nạn nhân sẽ làm theo mọi hướng dẫn, ngay cả khi chúng vô lý, chỉ để thoát khỏi áp lực hiện tại.

III.5. Kết nối giữa các điểm yếu tâm lý và hành vi rủi ro trong môi trường mạng

Các yếu tố tâm lý trên không hoạt động đơn lẻ mà thường kết hợp với nhau tạo thành một "cơn bão" thao túng.

- Vòng lặp khai thác: Sự kết hợp giữa **Thiên kiến xác nhận** (mong đợi email) + **Sự cấp bách** (deadline sát) + **Sự phục tùng quyền lực** (giả danh sếp) + **Thiên kiến lạc quan** (không nghĩ mình bị lừa) tạo thành một kịch bản hoàn hảo để nạn nhân tự nguyện click vào link độc hại.

- Đặc thù môi trường mạng: Môi trường kỹ thuật số thiếu đi các tín hiệu phi ngôn ngữ (ngôn ngữ cơ thể, ánh mắt) khiến các giác quan cảnh báo tự nhiên của con người bị vô hiệu hóa, tạo điều kiện thuận lợi cho việc giả mạo danh tính và thao túng tâm lý.

- **Giả mạo danh tính dễ dàng:** Kẻ tấn công có thể dễ dàng tạo ra một email hoặc website giả mạo hoàn hảo, đánh lừa thị giác và kích hoạt các yếu tố tâm lý liên quan đến sự tin tưởng.

CHƯƠNG IV. ĐỀ XUẤT BIỆN PHÁP GIÁO DỤC NGƯỜI DÙNG

IV.1. Thực trạng nhận thức của người dùng hiện nay

- Trong bối cảnh công nghệ thông tin phát triển mạnh mẽ, Internet và các dịch vụ trực tuyến đã trở thành một phần không thể thiếu trong đời sống hằng ngày của con người. Tuy nhiên, song song với những tiện ích mang lại, các nguy cơ mất an toàn thông tin cũng ngày càng gia tăng, đặc biệt là các hình thức tấn công dựa trên Social Engineering.

- Phần lớn người dùng hiện nay vẫn cho rằng các cuộc tấn công mạng chỉ xảy ra khi hệ thống có lỗ hổng kỹ thuật nghiêm trọng. Trên thực tế, nhiều cuộc tấn công không cần sử dụng kỹ thuật phức tạp mà chỉ khai thác sự thiếu hiểu biết, chủ quan và tâm lý của con người. Social Engineering lợi dụng sự tin tưởng, sợ hãi hoặc mong muốn đạt được lợi ích nhanh chóng của nạn nhân để thực hiện hành vi lừa đảo.

- Nhiều người dùng hiện nay còn tồn tại các hạn chế như:

+ Thiếu kiến thức cơ bản về các hình thức lừa đảo phổ biến trên môi trường mạng.

+ Có tâm lý chủ quan, dễ tin vào các thông tin được cung cấp qua email, tin nhắn hoặc cuộc gọi.

+ Phản xạ theo cảm xúc, đặc biệt trong các tình huống bị đe dọa hoặc thúc ép về thời gian.

- Những yếu tố trên khiến cho số lượng nạn nhân của các cuộc tấn công Social Engineering ngày càng gia tăng, gây ra nhiều thiệt hại về tài chính, thông tin cá nhân và uy tín của tổ chức.

IV.2. Mục tiêu của giáo dục người dùng

- Giáo dục người dùng đóng vai trò quan trọng trong việc giảm thiểu rủi ro từ các cuộc tấn công Social Engineering. Mục tiêu của hoạt động giáo dục không chỉ dừng lại ở việc truyền đạt kiến thức lý thuyết, mà còn hướng tới việc thay đổi nhận thức và hành vi của người dùng trong quá trình sử dụng công nghệ.

- Cụ thể, giáo dục người dùng nhằm đạt được các mục tiêu sau:

+ Giúp người dùng hiểu rõ bản chất của Social Engineering và các thủ đoạn thường được kẻ tấn công sử dụng.

+ Hình thành tư duy cảnh giác và nghi ngờ hợp lý khi tiếp nhận thông tin từ các nguồn không rõ ràng.

+ Rèn luyện kỹ năng tự bảo vệ và xử lý tình huống một cách bình tĩnh, chính xác.

+ Xây dựng thói quen sử dụng công nghệ an toàn, góp phần bảo vệ thông tin cá nhân và tổ chức trong dài hạn.

IV.3. Các biện pháp giáo dục người dùng

IV.3.1. Đào tạo kiến thức nền tảng về Social Engineering

- Một trong những biện pháp quan trọng nhất là cung cấp cho người dùng kiến thức nền tảng về Social Engineering. Người dùng cần được giới thiệu khái niệm Social Engineering, các hình thức tấn công phổ biến như phishing, vishing, baiting và cách thức hoạt động của chúng.

- Việc phân tích các tình huống lừa đảo thực tế giúp người dùng nhận thức rõ hơn về mức độ nguy hiểm của các cuộc tấn công này. Thông qua các ví dụ cụ thể, người dùng sẽ dễ dàng nhận ra rằng Social Engineering không phải là vấn đề xa lạ, mà có thể xảy ra bất cứ lúc nào trong cuộc sống hằng ngày.

IV.3.2. Giáo dục kỹ năng nhận diện và xử lý tình huống

- Bên cạnh kiến thức lý thuyết, người dùng cần được trang bị kỹ năng nhận diện các dấu hiệu bất thường trong quá trình giao tiếp trực tuyến. Điều này bao gồm việc kiểm tra nguồn gửi email, nội dung tin nhắn, giọng điệu trong các cuộc gọi và yêu cầu cung cấp thông tin cá nhân.

- Ngoài ra, giáo dục người dùng cách giữ bình tĩnh và không đưa ra quyết định vội vàng là yếu tố then chốt. Trong nhiều trường hợp, chỉ cần dừng lại để xác minh thông tin qua kênh chính thức cũng có thể giúp người dùng tránh được rủi ro đáng tiếc.

IV.3.3. Tăng cường học tập thông qua mô phỏng và thực hành

- Việc học thông qua mô phỏng các tình huống lừa đảo giúp người dùng có cơ hội trải nghiệm và rèn luyện kỹ năng trong môi trường an toàn. Các buổi học có thể sử dụng email giả lập hoặc kịch bản cuộc gọi mẫu để người dùng phân tích và đưa ra phương án xử lý.

- Phương pháp này không chỉ giúp người dùng ghi nhớ kiến thức lâu hơn mà còn nâng cao khả năng phản xạ khi gặp các tình huống tương tự trong thực tế.

IV.3.4. Hình thành thói quen sử dụng công nghệ an toàn

- Giáo dục người dùng cần hướng tới việc hình thành các thói quen sử dụng công nghệ an toàn. Điều này bao gồm việc sử dụng xác thực hai yếu tố, tạo mật khẩu mạnh và không sử dụng chung mật khẩu cho nhiều dịch vụ.

-Bên cạnh đó, người dùng cần được cảnh báo về nguy cơ khi cài đặt phần mềm không rõ nguồn gốc hoặc truy cập vào các đường link đáng ngờ. Khi các thói quen an toàn được duy trì thường xuyên, mức độ rủi ro sẽ giảm đi đáng kể.

IV.3.5. Giáo dục theo nhóm đối tượng cụ thể

- Mỗi nhóm người dùng có đặc điểm và nguy cơ khác nhau, do đó nội dung giáo dục cần được điều chỉnh cho phù hợp. Sinh viên thường dễ trở thành nạn nhân của các hình thức lừa đảo liên quan đến học bổng, việc làm và chuyển tiền. Người cao tuổi thường dễ bị lừa qua các cuộc gọi giả danh cơ quan chức năng. Trong khi đó, nhân viên văn phòng cần đặc biệt cảnh giác với các email giả mạo lãnh đạo hoặc bộ phận IT.

- Việc phân loại đối tượng giúp nâng cao hiệu quả của hoạt động giáo dục và giảm thiểu rủi ro phát sinh.

IV.3.6. Xây dựng môi trường khuyến khích báo cáo sự cố

- Một môi trường an toàn cần khuyến khích người dùng chủ động báo cáo các hành vi đáng ngờ. Việc không đổ lỗi hay chỉ trích nạn nhân giúp người dùng cảm thấy yên tâm hơn khi chia sẻ sự cố.

- Thông qua việc ghi nhận và xử lý kịp thời các báo cáo, tổ chức có thể phát hiện sớm các mối nguy và ngăn chặn thiệt hại lan rộng.

IV.3.7. Đánh giá, cải tiến và cập nhật thường xuyên

- Hoạt động giáo dục người dùng cần được đánh giá và cập nhật định kỳ để phù hợp với sự thay đổi của các hình thức tấn công. Việc tổ chức khảo sát nhận thức, kiểm tra kiến thức và cập nhật nội dung đào tạo giúp đảm bảo hiệu quả lâu dài của chương trình giáo dục an toàn thông tin.

IV.4. Kết luận

Social Engineering là hình thức tấn công khai thác trực tiếp yếu tố con người, do đó giáo dục người dùng được xem là biện pháp phòng chống hiệu quả và bền vững nhất. Khi người dùng được trang bị đầy đủ kiến thức, kỹ năng và thói quen an toàn, nguy cơ bị tấn công sẽ giảm đáng kể, góp phần xây dựng một môi trường số an toàn và lành mạnh hơn.

KẾT LUẬN

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, Internet và các nền tảng trực tuyến đã trở thành môi trường hoạt động thiết yếu trong mọi lĩnh vực của đời sống. Tuy nhiên, song hành với sự tiện lợi là sự gia tăng nhanh chóng của các hình thức tấn công mạng, đặc biệt là **các chiêu thức lừa đảo khai thác yếu tố con người (social engineering)** như **phishing, baiting** và **vishing**. Đây là những phương thức không đòi hỏi kỹ thuật cao nhưng lại gây thiệt hại nghiêm trọng, bởi chúng đánh trực tiếp vào tâm lý, cảm xúc và lòng tin của người dùng.

Qua việc tìm hiểu và phân tích các ví dụ thực tế tại Việt Nam, có thể nhận thấy rằng người dùng Internet trong nước vẫn còn hạn chế về nhận thức và kỹ năng nhận diện rủi ro trực tuyến. Nhiều vụ việc lừa đảo diễn ra chỉ vì sự chủ quan hoặc thiếu cảnh giác trước những tình huống tưởng như vô hại. Điều đó cho thấy **yếu tố con người chính là mắt xích yếu nhất trong chuỗi an toàn thông tin**.

Để giảm thiểu các nguy cơ từ tấn công xã hội, **giáo dục và nâng cao nhận thức an toàn thông tin** cần được xem là biện pháp cốt lõi, lâu dài và bền vững. Việc trang bị cho người dùng kiến thức cơ bản về an ninh mạng, kỹ năng phản ứng khi gặp tình huống nghi ngờ, cùng với việc hình thành thói quen sử dụng Internet an toàn sẽ góp phần quan trọng trong việc xây dựng "lá chắn nhận thức" – tuyến phòng thủ đầu tiên và hiệu quả nhất trước các mối đe dọa phi kỹ thuật.

Nhìn chung, bảo mật thông tin không chỉ là trách nhiệm của cơ quan quản lý hay chuyên gia kỹ thuật, mà còn là **ý thức và hành động của từng cá nhân**. Khi người dùng hiểu rõ rủi ro, hành xử cẩn trọng và có khả năng nhận diện lừa đảo, xã hội số sẽ trở nên an toàn và đáng tin cậy hơn.

TÀI LIỆU THAM KHẢO

1. Bộ Thông tin và Truyền thông. (2024). *Báo cáo hiện trạng an toàn thông tin tại Việt Nam*. Hà Nội: NXB Thông tin và Truyền thông.
2. Cục An toàn thông tin. (2024). *Cảnh báo về các hình thức lừa đảo trực tuyến phổ biến*. Truy cập từ: https://ais.gov.vn
3. VietNamNet. (2023, 15/6). *Lừa đảo mạo danh nhân viên ngân hàng: Người dùng mất tiền chỉ sau một cuộc gọi*.
4. Kaspersky. (2023). *Phishing, Baiting, and Vishing: The Evolution of Social Engineering Attacks*.
5. OWASP Foundation. (2023). *Social Engineering Attack Techniques and Defense Mechanisms*.
6. BleepingComputer. (2024). *Deepfake voice scams rise as criminals exploit AI technology*.
7. Trung tâm Giám sát An toàn không gian mạng quốc gia (NCSC). (2025). *Khuyến nghị nâng cao nhận thức người dùng trước tấn công lừa đảo qua mạng*. Bộ Thông tin và Truyền thông.