**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

\_\_\_\_\_o0o\_\_\_\_\_



**BÀI TIỂU LUẬN**

**MÔN:**

**PHÂN TÍCH LỖ HỔNG VÀ KIỂM THỬ**

**ĐỀ TÀI:** **SOCIAL ENGINEERING**

**NHÓM: 12**

**Thành phố Hồ Chí Minh, tháng 11 năm 2023**

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**TÊN ĐỀ TÀI:** **SOCIAL ENGINEERING**

|  |  |
| --- | --- |
| **Nhóm: 12**  Trưởng nhóm: Nguyễn Ngọc Hiếu  **Thành viên:**  1. Nguyễn Ngọc Lan Anh  2. Nguyễn Thị Linh Khánh  3. Phan Thị Xuân Yên | **Giảng viên hướng dẫn:**  **Nguyễn Thị Hồng Thảo** |

**Thành phố Hồ Chí Minh, tháng 11 năm 2023**

# LỜI CAM ĐOAN

Nhóm 12 chúng em xin giới thiệu với cô và mọi người đề tài ”Social Engineering”. Trong quá trình thực hiện đề tài này còn có nhiều thiếu sót do kiến thức còn sơ sài nhưng những nội dung trình bày trong quyển báo cáo này là những biểu hiện kết quả của chúng em đạt được dưới sự hướng dẫn của Cô Nguyễn Thị Hồng Thảo.

Chúng em xin cam đoan rằng: Những nội dung trình bày trong quyển báo cáo tiểu luận môn này không phải là bản sao chép từ bất kì tiểu luận nào có trước. Nếu không đúng sự thật, chúng em xin chịu mọi trách nhiệm trước thầy cô.

|  |
| --- |
| TPHCM, tháng 11 năm 2023 |
| Nhóm trưởng |

# LỜI CẢM ƠN

Để hoàn thành bài báo cáo này, chúng em xin chân thành cảm ơn cô Nguyễn Thị Hồng Thảo đã tận tình hướng dẫn cũng như nhận xét, góp ý trong suốt quá trình học tập. Với lòng biết ơn sâu sắc nhất, chúng em xin phép gửi đến cô. Cảm ơn cô đã truyền đạt vốn kiến thức cần có cho chúng em trong suốt quá trình học tập tại trường. Nhờ sự hướng dẫn, chỉ bảo tận tình của cô đã giúp chúng em hoàn thành đề tài một cách tốt nhất.

Chúng em xin gửi lời cảm ơn chân thành đến cô, người đã giúp đỡ và hướng dẫn trong quá trình hoàn thành bài báo cáo này. Vì kiến thức và thời gian hạn hẹp nên bài báo cáo không tránh khỏi những sai sót.

Chúng em mong nhận được sự đóng góp ý kiến từ cô để giúp hoàn thiện kiến thức và bổ sung thêm thông tin cần thiết cho báo cáo của nhóm em.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

[**PHẦN MỞ ĐẦU 1**](#_Toc151293130)

[**NỘI DUNG 2**](#_Toc151293131)

[**I. Social Engineering là gì? 2**](#_Toc151293132)

[**II. Những kiểu tấn công thông dụng 3**](#_Toc151293133)

[**1. Human-based 4**](#_Toc151293134)

[**2. Computer-based 6**](#_Toc151293135)

[**3. Mobile-based 9**](#_Toc151293136)

[**III. Rủi ro gặp phải khi bị tấn công phi kỹ thuật 12**](#_Toc151293137)

[**1. Mất dữ liệu 12**](#_Toc151293138)

[**2. Mất niềm tin xã hội 12**](#_Toc151293139)

[**3. Mất quyền riêng tư 12**](#_Toc151293140)

[**4. Thất thoát tài chính 12**](#_Toc151293141)

[**5. Hoạt động kinh doanh bị ảnh hưởng 13**](#_Toc151293142)

[**IV. Cách thức phòng chống tấn công SE? 13**](#_Toc151293143)

[**1. Các biện pháp dành cho cá nhân 13**](#_Toc151293144)

[**2. Các biện pháp kỹ thuật 14**](#_Toc151293145)

[**Tổng Kết 15**](#_Toc151293146)

[**TÀI LIỆU THAM KHẢO: 15**](#_Toc151293147)

# PHẦN MỞ ĐẦU

1. **Lý do chọn đề tài:**

Theo các chuyên gia lỗ hổng bảo mật lớn nhất, con người Social engineering là cách tấn công nhằm cố gắng thao túng các cá nhân thực hiện các hành động hoặc tiết lộ thông tin bí mật. Social engineering là một kiểu tấn công dựa vào sự tương tác của con người và thường liên quan đến việc thao túng mọi việc bằng cách phá vỡ các quy trình bảo mật thông thường, truy cập vào hệ thống, mạng để đạt được lợi ích tài chính

Bài báo cáo này sẽ giới thiệu tổng quát về các phương pháp và các kỹ thuật tấn công mà hacker sử dụng để xâm nhập và khai thác vào các phiên bản hệ điều hành của windows và giúp ta nắm rõ cách thức Attacker sử dụng và đưa ra giải pháp giúp cho mỗi người dùng được an toàn thông tin.

1. **Mục đích nghiên cứu:**

* Tìm hiều được Social Engineering là gì?
* Những kiểu tấn công thông dụng (Human-based, Computer-based, Mobile-based)
* Các rủi ro khi bị tấn công phi kỹ thuật và cách phòng chống nó
* Thực hiện demo qua các công cụ máy ảo và các chương trình hỗ trợ
* Báo cáo kết quả

1. **Phương pháp nghiên cứu :**

* Phương pháp quan sát
* Phương pháp thực nghiệm
* Phương pháp phân tích vấn đề

1. **Công cụ hỗ trợ**

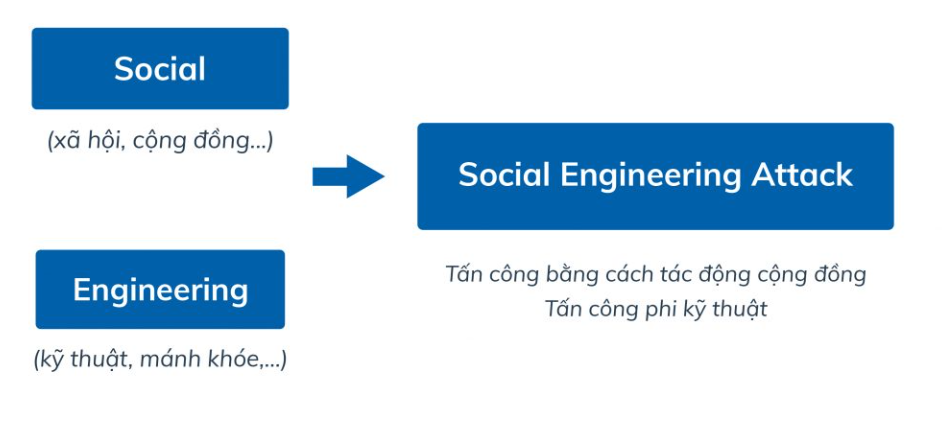
Máy ảo VMWare gồm có Kali làm máy tấn công, Windows 7 là máy nạn nhân.

# NỘI DUNG

# I. Social Engineering là gì?

Social Engineering (hay tấn công phi kỹ thuật) là thuật ngữ phổ biến trong lĩnh vực bảo mật thông tin, mô tả hình thức thao túng hành vi của con người thay vì tập trung khai thác các [lỗ hổng bảo mật](https://cystack.net/blog/lo-hong-bao-mat) của máy móc, thiết bị. Qua đó, kẻ tấn công có thể đạt được các mục đích của mình như xâm nhập vào hệ thống, truy cập thông tin quan trọng,… mà không cần phải thực hiện những kỹ thuật tấn công quá phức tạp.

Social Engineering là kết hợp giữa 2 từ Social (xã hội) và Engineering (kỹ thuật), thể hiện bản chất của kiểu tấn công này: các mánh khóe, kỹ thuật tấn công nhắm vào bản tính xã hội của con người, thứ mà không hề tồn tại trong máy móc. Social Engineering Attack còn được biết đến với cái tên Tấn công phi kỹ thuật.



Bằng cách tác động trực tiếp đến tâm lý con người, xây dựng các mối quan hệ có chủ đích, Social Engineering khai thác các thông tin và dùng những thông tin đó vào mục đích riêng (tống tiền, trộm cắp tài sản, đe dọa, phá hủy cá nhân/ tổ chức,…). Khi áp dụng Social Engineering, tội phạm thường che giấu danh tính và động cơ thực sự bằng một vẻ ngoài đáng tin cậy khiến cho đối phương mất cảnh giác, từ đó dễ dàng xâm nhập các sơ hở. Social Engineering không trực tiếp sử dụng các phương thức kỹ thuật (phá hủy hệ thống, tin tặc) nhưng có thể sẽ dùng các cách thức tinh vi để dẫn đến tấn công bằng kỹ thuật.



Ta có thể hình dung rõ hơn về Social Engineering qua các tình huống quen thuộc như: chó sói đội lốt con cừu để ăn thịt bầy cừu. Một ngày đẹp trời bạn nhận được tin nhắn trúng thưởng kèm theo yêu cầu gửi thêm một khoản tiền thuế/ đảm bảo/ vận chuyển… Hoặc hàng xóm của bạn bị một đối tượng giả danh người thân để chiếm đoạt tài sản. Nhân viên của bạn vô tình tải xuống một phần mềm chứa virus và gây nhiễm độc toàn bộ hệ thống máy tính, ngay sau đó cơ quan bạn bị lộ các thông tin quan trọng như số tài khoản, mật khẩu, đơn hàng…

Có thể thấy rõ rằng Tấn công phi kỹ thuật không giới hạn hình thức, phương thức, nạn nhân và thủ phạm. Bất kỳ ai đều có thể là tội phạm và bất kỳ ai đều có thể là nạn nhân. Chính vì vậy bạn cần phải nâng cao cảnh giác và để ý từ các chi tiết nhỏ nhất.

# II. Những kiểu tấn công thông dụng

Social Engineering được chia làm ba hình thức chính :

* Human-based: Human-based Social Engineering dựa trên dựa trên mối quan hệ giữa người và người để khai thác, thu thập thông tin như gọi điện thoại hỏi các nhân viên bộ phận hỗ trợ người dùng để thử tìm các thông tin nhạy cảm.
* Computer-based: Computer-based Social Engineering sử dụng các chương trình máy tính hay những trang web để dẫn dụ người dùng nhập vào các thông tin bí mật là tài khoản và mật khẩu truy cập. Dạng tấn công này thường được gọi là phishing.
* Mobile-based: Những kẻ tấn công sử dụng các ứng dụng để thực hiện cuộc tấn công SE và lấy thông tin nhạy cảm dựa trên thiết bị di động.

## **Human-based**

* Impersonation: Những trường hợp điển hình cho dạng tấn công này là giả dạng nhân viên hay là cộng tác viên để truy cập vật lý vào những thông tìn được bảo vệ. Như giả dạng làm nhân viên bảo trì hệ thống để đột nhập phòng máy chủ trái phép. Bên cạnh đó hacker còn giả làm một nhân vật quan trọng hay nhân vật thứ ba nào đó để gọi điện thoại cho bộ phận hỗ trợ, những quản trị hệ thống yêu cầu cung cấp các tài khoản quản trị như hình minh họa. Tình huống tấn công này đã được hacker Kevin Mitnick cùng cộng sự trình diễn tại đại hội Blackhat, trong tình huống này anh ta đã dùng phần mềm giả giọng nói và cả số điện thoại của một nhân vật quản trị cao cấp yêu cầu quản trị mạng nhắc mật khẩu email do bị quên password, và kết quả là hoàn toàn thành công.
* Impersonation - Vishing (Voice hoặc VoIP phishing): là một kỹ thuật mạo danh, trong đó attacker lừa các cá nhân tiết lộ thông tin cá nhân và tài chính bằng công nghệ giọng nói như hệ thống điện thoại, VoIP,…

Ví dụ: Lạm dụng sự hữu ích quá mức của bộ phận trợ giúp: Attacker gọi đến bộ phận trợ giúp của công ty và giả vờ là người có thẩm quyền hoặc có liên quan để lấy thông tin nhạy cảm.

Ủy quyền của bên thứ ba: Attacker lấy được tên của nhân viên được ủy quyền của tổ chức mục tiêu, người có quyền truy cập vào thông tin mà attacker muốn, sau đó attacker thực hiện cuộc gọi đến tổ chức mục tiêu nơi lưu trữ thông tin và nói rằng nhân viên này đã yêu cầu cung cấp thông tin đó.

Hỗ trợ kỹ thuật: Attacker giả làm nhân viên hỗ trợ kỹ thuật của các nhà cung cấp hoặc nhà thầu phần mềm của tổ chức mục tiêu. Attacker có thể yêu cầu ID người dùng và mật khẩu để khắc phục sự cố trong tổ chức.

* Eavesdropping: Nghe trái phép các cuộc hội thoại hoặc đoạn tin nhắn. Đánh chặn âm thanh, video hoặc giao tiếp bằng văn bản.
* Shoulder surfing*:* Dạng tấn công này hacker sẽ xem lén thông tin mật khẩu chúng ta nhập vào màn hình như tên tài khoản, xem lén kí tự bàn phím hay lắng nghe các âm thanh phát ra khi người dùng gõ vào để đoán xem đó là những kí tự gì. Vì lý do này mà nhiều doanh nghiệp cho thiết kế các trạm làm việc sao cho vẫn bảo đảm tính thận thiện nhưng ngăn ngừa người này có thể nhìn thấy màn hình của người khác.
* Dumpster diving*:* Cũng có những tình huống các hacker giả dạng làm những người quét dọn vệ sinh, hay những đồng nghiệp lục lọi hồ sơ của nhau để tìm kiếm các bị mật công nghệ, nhưng thông tin riêng tư và hình thức này được gọi là Dumpster diving. Vì vậy, các doanh nghiệp thường trang bị các máy hủy giấy để ngăn ngừa các thông tin bí mật hay các ý tưởng quan trọng bị lộ từ các mãnh giấy bỏ. Hoặc chính sách của các công ty này yêu cầu nhân viên khi rời khỏi bàn làm việc phải đặt màn hình chế độ Screen Saver, và lật úp mặt các tài liệu mang tính riêng tư của mình.
* Reverse Social Engineering: Phương pháp nâng cao hơn trong kỹ thuật Social Engineering là Reverse Social Engineering (Social Engineering ngược). Trong kỹ thuật này, hacker trở thành người cung cấp thông tin. Điều đó không có gì là ngạc nhiên, khi hacker bây giờ chính là nhân viên phòng help desk.
* Piggybacking: Thường xảy ra với những người có thẩm quyền trong tổ chức như giám đốc, attacker sẽ lừa họ để xâm nhập vào hệ thống công ty. Attacker có thể giả làm nhân viên sửa máy tính, người thân hay nhân viên văn phòng để gắn các thiết bị theo dõi hay trực tiếp tấn công vào hệ thống dữ liệu để lấy cắp thông tin.
* Tailgating:Đôi khi được gọi là piggybacking, là khi một hacker xâm nhập vào một tòa nhà được bảo vệ bằng cách theo dõi ai đó có thẻ ra vào tòa nhà đó. Cuộc tấn công này giả định người có quyền bước vào tòa nhà đó sẽ giữ cửa mở cho người đứng sau họ (giả sử họ được phép làm điều này ở đó).
* Diversion theft: Là một kỹ thuật trong đó kẻ tấn công nhắm mục tiêu vào các chuyên gia giao hàng hoặc công ty vận tải. Kỹ thuật này còn được gọi là "Round The Corner Game" hoặc "Cornet Game". Mục tiêu chính của kỹ thuật này là lừa người chịu trách nhiệm thực hiện giao hàng thực sự giao hàng đến sai địa điểm, do đó làm gián đoạn giao dịch. Ví dụ: nếu nạn nhân là tài xế xe van đang giao một gói hàng thì người đó sẽ bị thuyết phục lái xe đến một địa điểm khác ngoài địa điểm giao hàng thực tế. Do đó, việc người lái xe van phải thực hiện một loạt thủ thuật kỹ thuật xã hội sẽ giúp vụ trộm thành công. Hành vi trộm cắp chuyển hướng cũng có thể được thực hiện bởi các kẻ lừa đảo xã hội trên Internet; nạn nhân có thể bị thuyết phục gửi các tập tin nhạy cảm hoặc bí mật cho một số người không liên quan nhưng không có ý định nhận chúng.
* Honey trap: Đây là một cuộc tấn công trong đó các social engineering giả vờ là một người “hấp dẫn” để tương tác với một người trực tuyến hoặc giả mạo một mối quan hệ trực tuyến và thu thập thông tin nhạy cảm thông qua mối quan hệ đó.
* Baiting: Baiting là một phương pháp kỹ thuật xã hội khác gây rắc rối cho nhiều người dùng thiếu chú ý. Nó liên quan đến việc sử dụng mồi để dụ nạn nhân dựa trên sự tham lam hoặc tò mò của họ. Chẳng hạn, những kẻ lừa đảo có thể tạo ra một trang web cung cấp một cái gì đó miễn phí, như các tệp nhạc, video hoặc sách.
* Quid pro quo: Yêu cầu người khác cung cấp thông tin hoặc truy cập vào một hệ thống nhất định bằng cách cung cấp một dịch vụ hoặc lợi ích trong cùng một lúc.
* Elicitation: Hình thức khơi gợi câu chuyện, gãi bẫy để đối tượng không nhận ra rằng mình đang vô tình cung cấp thông tin. Các kỹ thuật như tâng bốc, giả khờ, đóng vai nhà cố vấn, …

## **Computer-based**

* Pop-up Windows: Các cửa sổ pop-up hiện lên trong thiết bị của nạn nhân. Nếu vô tình click vào pop-up đó thì nó sẽ dẫn đến 1 website khác của hacker yêu cầu người dùng đăng nhập đầy đủ thông tin hoặc tải phần mềm chứa mã độc về máy.
* Hoax Letters: Là một thông báo cảnh báo người nhận về mối đe dọa vi-rút máy tính không tồn tại. Nó dựa vào kỹ thuật xã hội để mở rộng phạm vi tiếp cận của nó. Thông thường, trò lừa đảo không gây ra bất kỳ thiệt hại vật chất hoặc mất mát thông tin nào; nhưng chúng làm giảm năng suất và sử dụng tài nguyên mạng có giá trị của tổ chức.
* Chain Letters: Là một tin nhắn cung cấp quà tặng miễn phí, chẳng hạn như tiền và phần mềm, với điều kiện người dùng chuyển tiếp email đến một số lượng người nhận được xác định trước. Các cách tiếp cận phổ biến được sử dụng trong các bức thư dây chuyền là những câu chuyện thuyết phục về mặt cảm xúc, kế hoạch kim tự tháp "làm giàu nhanh chóng", niềm tin tâm linh và những lời đe dọa mê tín về vận rủi đối với người nhận mà họ "phá vỡ sợi dây chuyền" và không truyền đạt được thông điệp hoặc đơn giản là từ chối chuyển tiếp. đọc nội dung của nó. Chuỗi thư cũng dựa vào kỹ thuật xã hội để lan truyền.
* Scareware: Người dùng bị tấn công bằng báo động giả và các mối đe dọa không có thật. Họ bị đánh lừa khi nghĩ rằng hệ thống của họ bị nhiễm phần mềm độc hại. Scareware còn được gọi là phần mềm lừa gạt, phầm mềm scan giả mạo, phần mềm gian lận.

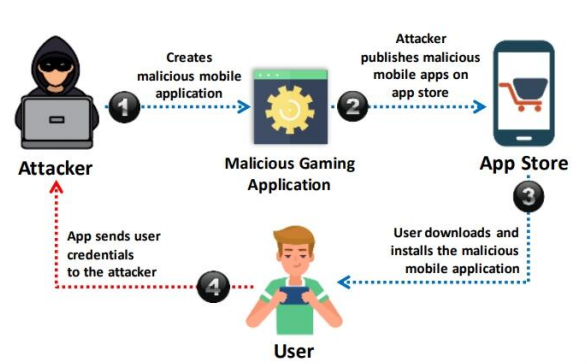
Ví dụ: Khi lướt web thị hiển thị thông báo máy bạn bị nhiễm virus và đề xuất bạn cài đặt phần mềm diệt virus, khi click vào đường dẫn đề xuất hoặc cài đặt phần mềm được đề xuất thì nó sẽ hướng bạn tới trang web độc hại, nơi máy của bạn bị nhiễm.

* Instant chat messenger: Attacker trò chuyện với người dùng trực tuyến thông qua trình tin nhắn trò chuyện tức thời và cố gắng thu thập thông tin cá nhân của họ như ngày sinh, biệt danh,… Sau đó sử dụng thông tin thu thập được để bẻ khóa tài khoản người dùng.
* Spam Email: Là các email không liên quan, không mong muốn và không được yêu cầu được thiết kế để thu thập thông tin tài chính như số an sinh xã hội và thông tin mạng. Những kẻ tấn công gửi tin nhắn rác đến mục tiêu để thu thập thông tin nhạy cảm, chẳng hạn như chi tiết ngân hàng. Những kẻ tấn công cũng có thể gửi tệp đính kèm email có chứa các chương trình độc hại ẩn như virus và trojan. Attacker cố gắng ẩn phần mở rộng tệp bằng cách đặt cho tệp đính kèm một tên tệp dài.
* Phishing: Có các loại phishing như Spear phishing, Whaling, Pharming, Spimming, Angler phishing, Catfishing Attack, Deepfake Attack
* Spear phishing: Một cuộc tấn công lừa đảo được nhắm mục tiêu nhằm vào các cá nhân cụ thể trong một kẻ tấn công tổ chức gửi lời đánh lừa một bài viết với chuyên gia kỹ thuật xã hội, với một người cụ thể, hoặc một nhóm nhỏ người. Những kẻ tấn công gửi lời lừa đảo để gửi tin nhắn với chuyên gia xã hội, nội dung xã hội trực tiếp tại một người cụ thể, hoặc một nhóm nhỏ.
* Whaling: Một kẻ tấn công nhắm mục tiêu các giám đốc điều hành cao như CEO, CFO, chính trị gia, và những người nổi tiếng có quyền truy cập đầy đủ vào thông tin bí mật và có giá trị cao. Kẻ tấn công đánh lừa nạn nhân cho thấy thông tin quan trọng và công ty thông tin thông qua thông tin email hoặc giả mạo trang web.
* Pharming: Người tấn công chuyển hướng lưu lượng truy cập web sang trang web gian lận bằng cách cài đặt một chương trình hoặc máy tính cá nhân độc hại trên máy tính cá nhân. Còn được gọi là "Phishing without a Lure", và được thực hiện bằng cách sử dụng ngộ độc bộ nhớ cache DNS hoặc tập tin lưu trữ.
* Spimming: Một biến thể của spam khai thác nền tảng tin nhắn tức thời để lam tràn qua mạng. Kẻ tấn công sử dụng các chương trình để thu thập ID tin nhắn tức thời và phát tán thư rác.
* Angler phishing: Những kẻ tấn công tạo một tài khoản mạng xã hội giả mạo mạo danh tài khoản bộ phận trợ giúp của tổ chức và kết nối với những khách hàng bất mãn bằng cách đăng liên kết dịch vụ giả mạo. Khi nạn nhân nhấp vào liên kết, phần mềm độc hại được cài đặt trên hệ thống của họ hoặc họ được chuyển hướng đến một trang web khác yêu cầu họ cung cấp thông tin chi tiết.
* Catfishing Attack: Những kẻ tấn công tạo ra các phương tiện truyền sai của một cá nhân mục tiêu sử dụng các công nghệ tiên tiến như ML hoặc AI. Những kẻ tấn công thực hiện các câu trả lời bằng cách sử dụng mẫu âm thanh và video đã ghi lại trước đây của người nhắm mục tiêu và sau đó kiểm tra các clip đó. Những kẻ tấn công lừa người dùng trực tuyến tin rằng họ đang nghe các đoạn phim gốc, thường yêu cầu đóng góp.
* Deepfake Attack: Những kẻ tấn công nhắm mục tiêu một người trên nền tảng truyền thông xã hội và thực hiện trộm danh tính để tạo tài khoản phương tiện truyền thông xã hội giả mạo. Sau đó, kẻ tấn công sử dụng tài khoản giả mạo để giao tiếp với người dùng khác qua các hộp trò chuyện để thực hiện màu đúc cho lợi nhuận tiền tệ.

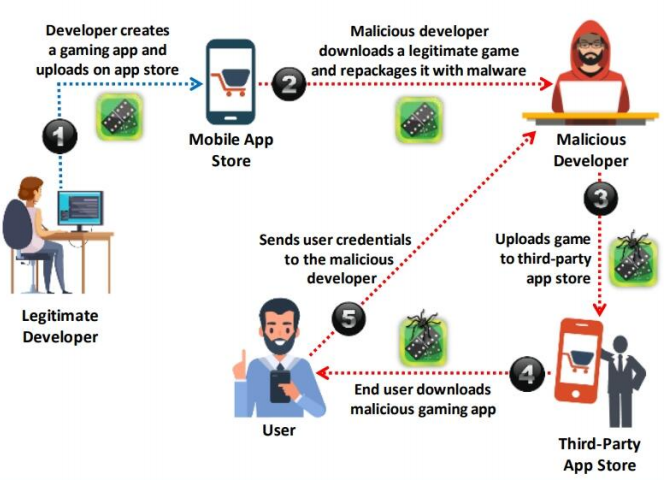
## **Mobile-based**

Những kẻ tấn công sử dụng các ứng dụng để thực hiện cuộc tấn công SE dựa trên thiết bị di động. Chúng lừa người dùng bằng cách bắt chước các ứng dụng phổ biến và tạo ra các ứng dụng di động độc hại với các tính năng hấp dẫn rồi gửi đến các cửa hàng ứng dụng lớn có cùng tên. Nếu người dùng vô tình tải xuống các phầm mềm độc hại này thì sẽ tạo điều kiện cho phần mềm độc hại lây nhiễm vào thiết bị của họ.

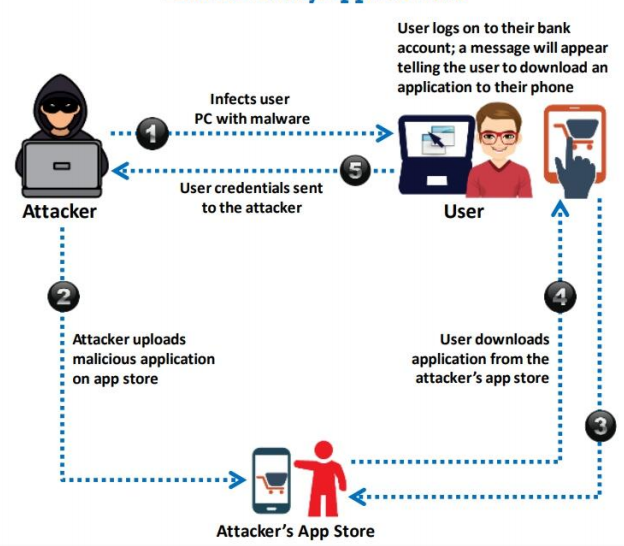
* Publishing malicious apps: Attacker tạo ra các ứng dụng độc hại có tính năng hấp dẫn và có tên giống với các ứng dụng phổ biến rồi xuất bản trên các cửa hàng ứng dụng lớn. Những người vô tình tải xuống các ứng dụng này sẽ bị nhiễm phần mềm độc hại gửi thông tin đăng nhập cho attacker.



* Repackaging legitimate apps: Attacker tải xuống phần mềm hợp pháp và đóng gói chúng lại bằng phần mềm độc hại và xuất bản phần mềm đó trên cửa hàng ứng dụng. Người dùng cuối cùng nếu tải phải phần mềm này sẽ gửi thông tin xác thực người dùng đến attacker.



* Using fake security apps: Attacker cho lây nhiễm phần mềm độc hại vào PC của nạn nhân, người dùng đăng nhập tài khoản ngân hàng sẽ xuất hiện thông báo yêu cầu tải ứng dụng về điện thoại nạn nhân. Attacker tải lên phần mềm độc hại trên kho ứng dụng, và người dùng khi tải phần mềm từ kho ứng dụng này thì thông tin đăng nhập sẽ bị gửi cho attacker.



* *SmiShing (SMS phishing):* Hoạt động bằng cách gửi tin nhắn văn bản đánh cắp thông tin cá nhân hoặc lừa đảo người nhận thực hiện các hành động không mong muốn. Tin nhắn Smishing thường được thiết kế để gây sự lạc quan hoặc sợ hãi trong người nhận, thúc đẩy họ tiết lộ thông tin nhạy cảm hoặc truy cập vào các liên kết độc hại.



*Các phương pháp Smishing phổ biến:*

* Tin nhắn Smishing: Tin nhắn Smishing thường được gửi từ một số điện thoại giả mạo hoặc thông qua các dịch vụ SMS đáng ngờ. Nội dung tin nhắn thường yêu cầu người nhận truy cập vào một liên kết hoặc cung cấp thông tin cá nhân như số thẻ tín dụng.
* *Cuộc gọi Smishing:* Cuộc gọi Smishing thường được thực hiện bằng cách sử dụng các số điện thoại giả mạo hoặc số không rõ nguồn gốc. Kẻ tấn công sẽ giả vờ là ngân hàng, tổ chức hay dịch vụ nổi tiếng và yêu cầu người nghe cung cấp thông tin cá nhân hoặc tiến hành các giao dịch tài chính bất thường.
* *Email Smishing*: Email Smishing là hình thức Smishing được thực hiện thông qua email. Kẻ tấn công gửi email giả mạo từ một nguồn không đáng tin cậy, thường là một tổ chức hay công ty nổi tiếng. Email thường yêu cầu người nhận cung cấp thông tin cá nhân hoặc tiến hành các hành động không an toàn.

# Rủi ro gặp phải khi bị tấn công phi kỹ thuật

## **Mất dữ liệu**

Các thông tin về hợp đồng kinh tế, hợp đồng vay vốn, chiến lược kinh doanh, marketing, thậm chí là bảng lương… đều là những thông tin hết sức nhạy cảm và có thể ảnh hưởng đến toàn bộ công ty. Đơn giản hơn, các dữ liệu về công việc bạn mất bao nhiêu công sức để soạn có thể bị lấy cắp và xóa hết…

## **Mất niềm tin xã hội**

Khi bị tấn công phi kỹ thuật, thông tin nội bộ của một tổ chức bị lộ ra ngoài có thể gây hoang mang dư luận. Doanh nghiệp (ngân hàng, bảo hiểm,…) nắm các thông tin cá nhân quan trọng của khách hàng, khi doanh nghiệp bị tấn công có thể dẫn đến thông tin cá nhân khách hàng bị lộ, khách hàng sẽ không con niềm tin đối với doanh nghiệp. Hoặc bạn là một cá nhân, bạn có thể bị lộ những hình ảnh nhạy cảm, riêng tư, gây mất hình tượng,..

## **Mất quyền riêng tư**

Bị lấy thông tin các nhân như địa chỉ, số điện thoại, thói quen sinh hoạt,… dẫn tới nhiều hệ lụy phiền toái. Nhiều người phàn nàn vì họ liên tục nhận được các cuộc gọi điện thoại “mời chào” cho vay tín dụng, bảo hiểm,… Thậm chí một vài người bị theo dõi và tấn công.s

## **Thất thoát tài chính**

Theo IBM, vi phạm gây ra bởi các trục trặc hệ thống và do lỗi của con người khiến các doanh nghiệp thiệt hại lần lượt là 3,5 triệu USD và 3,24 triệu USD.Bên cạnh đó, các tài khoản ngân hàng còn có thể bị rút tiền trực tiếp,…. Các đơn hàng/ tiền có thể bị cố tình gửi nhầm sang địa chỉ mà tội phạm mạng xác định từ trước.

## **Hoạt động kinh doanh bị ảnh hưởng**

* Nếu bị tấn công mạnh vào máy chủ website hoặc máy chủ hệ thống mạng, hệ thống rất có thể bị đánh sập. Vì thế mà website của công ty, tổ chức có thể bị treo (tạm ngừng hoạt động dịch vụ). Hiện nay các hệ thống y tế hiện đại cập nhập dữ liệu trên mạng internet, có thể bị tấn công khiến cho hồ sơ sức khỏe của hàng triệu bệnh nhân có thể bị mất hoặc sai sót, khiến cho quá trình điều trị có thể bị ảnh hưởng…

# Cách thức phòng chống tấn công SE?

Chính vì sự đa dạng về phương thức, đối tượng, nạn nhân nên tất cả mọi người đều cần phải cảnh giác với tội phạm Social Engineering, đặc biệt là các cá nhân, tổ chức nắm giữ khối lượng tài chính, thông tin lớn. Dưới đây là một vài lời khuyên của các chuyên gia công nghệ về các cách nâng cao bảo mật:

## ***Các biện pháp dành cho cá nhân***

* Cập nhập trang bị các thông tin cần thiết về an ninh.
* Luôn xác nhận liên lạc với người thân, tránh trao đổi thông tin/ tài sản với người lạ.
* Tránh sử dụng nhiều tài khoản cùng một mật khẩu và ngược lại
* Hạn chế đăng thông tin/ đặc điểm nhận dạng/ lịch trình/ sinh hoạt cá nhân lên mạng xã hội.
* Nên sử dụng tách biệt các tài khoản cá nhân và công việc riêng biệt.
* Giữ bình tĩnh và kéo dài thời gian đề phòng kẻ xấu đánh vào tâm lý làm trước khi nghĩ để lừa đảo.
* Không sử dụng các ứng dụng đòi quyền truy cập cá nhân và không rõ nguồn gốc.
* Nói không với mọi email yêu cầu xác minh tài chính, mật khẩu,..

***Những mẹo cần nhớ:***

* Chậm lại: Người gửi spam muốn bạn hành động trước và suy nghĩ sau. Nếu thông điệp truyền tải tạo một cảm giác cấp bách hoặc sử dụng chiến thuật gây áp lực cao thì hãy cảnh giác. Đừng bao giờ để cho sự khẩn cấp chúng tạo ra ảnh hưởng đến sự đánh giá của bạn.
* Nghiên cứu kỹ càng: Hãy nghi ngờ bất kỳ tin nhắn nào bạn nhận được. Nếu email có vẻ như là từ một công ty bạn đang sử dụng dịch vụ, hãy tìm hiểu theo cách của riêng bạn. Sử dụng công cụ tìm kiếm để truy cập trang web của công ty hoặc thư mục điện thoại để tìm số điện thoại của họ rồi xác thực thông tin.
* Đừng để một liên kết kiểm soát nơi bạn đến: Giữ quyền kiểm soát bằng cách tự tìm kiếm trang web thông qua việc sử dụng công cụ tìm kiếm để đảm bảo bạn đến đúng trang web mình cần. Di chuột qua các liên kết trong email sẽ hiển thị URL thực tế ở phía dưới, nhưng lưu ý là những giả mạo tinh vi vẫn có thể đánh lừa bạn.
* Việc hack email đang diễn ra tràn lan: Tin tặc, kẻ gửi spam và những kẻ sử dụng social engineering chiếm quyền kiểm soát tài khoản email của mọi người (và các tài khoản liên lạc khác) đã trở nên ngày càng nguy hiểm hơn. Khi chúng kiểm soát tài khoản email, chúng sẽ đánh cắp danh bạ của người đó. Ngay cả khi người gửi dường như là người bạn biết, nếu bạn không mong đợi một email có liên kết hoặc file đính kèm, hãy kiểm tra với bạn bè trước khi mở liên kết hoặc tải xuống.
* Cẩn thận với các mục tải xuống: Nếu bạn không biết người gửi là ai và vì sao họ lại gửi file đính kèm cho bạn, việc tải xuống bất kỳ điều gì là một sai lầm nghiêm trọng.
* Địa chỉ email nước ngoài là giả mạo: Nếu bạn bỗng dưng nhận được email từ công ty xổ số hoặc rút thăm trúng thưởng ở nước ngoài, tiền từ một người họ hàng không xác định hoặc yêu cầu chuyển tiền từ nước ngoài thì chắc chắn đó là lừa đảo.

## ***Các biện pháp kỹ thuật***

* Trang bị camera an ninh.
* Cập nhập hệ thống quản lý nghiêm ngặt.
* Phân chia tài khoản, quyền hạn và trách nhiệm rõ ràng đối với các tài khoản mạng xã hội, website, hệ thống.
* Hệ thống đăng nhập nhiều lớp.
* Cập nhật trình duyệt web mới nhất, tránh sử dụng plug-in hoặc add-on không cần thiết.
* Sử dụng phần mềm chặn pop-up (quảng cáo tự động).
* Phần mềm diệt virus uy tín, nếu các doanh nghiệp hoặc tổ chức có thông tin bảo mật nên dùng các phần mềm trả phí.
* Cảnh báo trang web nguy hiểm.
* Cập nhập tự động để vá các lỗ hổng an ninh.
* Duyệt web chế độ ẩn danh.
* Thường xuyên cập nhập tin tức công nghệ, bảo mật…
* Đặt bộ lọc Spam ở mức cao nhất (đối với email).

# 

# TỔNG KẾT

Qua chương này chúng ta đã nắm một số khái niệm quan trọng như dạng tấn công Social engineering ứng dụng các kỹ năng xã hội, dùng mối quan hệ con người để thu thập tin cần thiết phục vụ cho những cuộc tấn công phía sau. Việc các cuộc tấn công social engineering có thể thành công là do đánh vào điểm yếu của con người. Các bước thực hiện một cuộc tấn công Social engineering gồm: Thu thập thông tin, chọn mục tiêu, tấn công. Ngoài ra, các bạn . đã tìm hiểu những vấn đề Insider Attack, Indentify Theft, Online Scam, Phising… Và cuối cùng là để phòng chống lại kiểu tấn công này, chúng ta cần phải đào tạo, huấn luyện người dùng để nâng cao nhận thức về an toàn thông tin cho họ.

# 

# TÀI LIỆU THAM KHẢO:

[1]. Miller, R. C., & Easttom, C. (2022). Certified Ethical Hacker : CEH v12 Study Guide : Exam 312-501. EC-Council. (Module 9)

[2]. CyStack. (2023, March 8). Social engineering: The art of deception. CyStack. Retrieved from <https://cystack.net/blog/social-engineering>

[3]. Quantrimang. (2023-08-10). Social Engineering là gì? Làm sao để phòng tránh Social Engineering?. Retrieved from <https://quantrimang.com/cong-nghe/social-engineering-la-gi-lam-sao-de-phong-tranh-social-engineering-154125>

[4]. Locker.io. (2023, August 10). Social engineering là gì? Cách phòng tránh social engineering. Retrieved from <https://locker.io/vi/blog/social-engineering-la-gi-cach-phong-tranh-social-engineering>

[5]. Binance Academy. (2023, August 10). What is social engineering? Retrieved from <https://academy.binance.com/vi/articles/what-is-social-engineering>

[6]. Lam, N. H. (2023, August 10). Tản mạn về social engineering. Retrieved from <https://www.linkedin.com/pulse/t%E1%BA%A5n-c%C3%B4ng-social-engineering-l%C3%A0-g%C3%AC-ngoc-hoa-lam>

PHỤ LỤC

**BẢNG PHÂN CÔNG CÔNG VIỆC CỦA NHÓM**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và Tên - MSSV | Nội dung công việc | Nhận Xét |
| 1 | Nguyễn Thị Linh Khánh -2033211669 | Làm word, tìm nội dung, thuyết trình | 90% |
| 2 | Phan Thị Xuân Yên - 2033216613 | Làm ppt, tìm nội dung, thuyết trình | 100% |
| 3 | Nguyễn Ngọc Lan Anh - 2033210445 | Làm word, tìm nội dung, thuyết trình, viết report demo | 100% |
| 4 | Nguyễn Ngọc Hiếu - 2033210461 | Tìm nội dung, quay video demo, demo | 100% |

BIÊN BẢN LÀM VIỆC NHÓM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thời gian** | **Địa điểm** | **Thành viên** | **Nội dung** | **Ghi chú** |
| 3/4/2021  8h | Group zalo | A  B  C | PCCV |  |
| 3/4/2021  15h | Lớp học OL | A  B  C | Lập dàn ý |  |
| 6/4/2021 | … | A  B  C (vắng) |  |  |
| ….. | …. | …. | ….. |  |

Nhóm trưởng

(ký và ghi rõ họ tên, sdt)

5, TIÊU CHÍ ĐÁNH GIÁ

|  |  |  |
| --- | --- | --- |
| Tiêu chí đánh giá  (trọng số) | | Thang điểm |
| Cấu trúc  (10%) | | 1 |
| Nội dung  (80%) | Các nội dung thành phần  (40%) | 4 |
| Lập luận  (20%) | 2 |
| Kết luận/kết quả  (20%) | 2 |
| Hình thức trình bày  (10%) | | 1 |
| Tổng | | 10 |