



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐÌNH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Một số dạng kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN

TS. ĐÌNH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập,
Học viện Công nghệ Bưu chính Viễn thông, 2021.

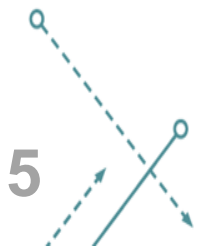
Các nội dung tìm hiểu

- Social Engineering là gì?
- Tại sao Social Engineering lại hiệu quả
- Các giai đoạn trong một cuộc tấn công Social Engineering
- Các mục tiêu phổ biến của Social Engineering
- Các kiểu Social Engineering
- Các chiến thuật xâm nhập phổ biến và chiến lược phòng chống
- Social Engineering với tấn công mạo danh trên mạng xã hội
- Ảnh hưởng của mạng xã hội tới mạng doanh nghiệp
- Ăn cắp ID là gì?
- Thế nào là ăn cắp tính danh?
- Biện pháp đối phó Social Engineering
- Thử nghiệm Social Engineering

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

**Không có bất kỳ bản vá lỗi nào
đối với một con người ngu ngốc**



Social Engineering là gì

- Tấn công vào yếu tố con người - Social Engineering là một nghệ thuật thuyết phục mọi người tiết lộ thông tin bí mật
- Social Engineering phụ thuộc vào những thứ mà mọi người không biết những thông tin về chúng và bất cẩn trong việc bảo vệ nó



Các hành vi dễ bị tấn công

- Sự tin tưởng là nền tảng cơ bản của tấn công Social Engineering
- Sự thiếu hiểu biết về Social Engineering và các hiệu ứng của nó trong đội ngũ nhân viên khiến cho các tổ chức là một mục tiêu dễ dàng
- Social Engineers có thể đe dọa nghiêm trọng đến việc mất mát trong trường hợp không tuân thủ những yêu cầu của tổ chức
- Social Engineers thu hút các mục tiêu tiết lộ thông tin bởi một cái gì đó đầy hứa hẹn
- Các mục tiêu sẽ được hỗ trợ giúp và họ tuân theo những quy định mang tính nghĩa vụ được đưa ra

Những yếu tố làm doanh nghiệp dễ bị tấn công



Việc đào tạo hiểu biết về an toàn thông tin cho nhân viên còn thiếu



Thiếu những chính sách an ninh



Nhiều các đơn vị tổ chức



Dễ dàng truy cập thông tin

Tại sao Social Engineering lại hiệu quả

- Không có một phần mềm hay phần cứng nào có thể chống lại một cuộc tấn công Social Engineering
- Không có một phương pháp chắc chắn nào để đảm bảo an ninh một cách đầy đủ từ các cuộc tấn công Social Engineering
- Chính sách bảo mật mạnh cũng sẽ là liên kết yếu nhất và con người là yếu tố nhạy cảm nhất
- Rất khó để phát hiện ra Social Engineering

Những dấu hiệu của một cuộc tấn công

- Tấn công trên mạng Internet đã trở thành một ngành kinh doanh và Kẻ tấn công liên tục cố gắng để xâm nhập mạng và có các dấu hiệu sau:
 - Không cung cấp số gọi lại
 - Yêu cầu phí chính thức
 - Yêu cầu thẩm quyền và đe dọa nếu như không cung cấp thông tin
 - cho thấy sự vội vàng và vô tình để lại tên
 - Bất ngờ được khen tặng hoặc ca ngợi
 - Thấy khó chịu khi đặt câu hỏi

Các giai đoạn của một cuộc tấn công Social Engineering

- **Nghiên cứu mục tiêu:** Dumpster diving, trang web, nhân sự, lịch trình...
- **Lựa chọn nạn nhân:** Xác định những nhân viên không hài lòng về chính sách trong công ty mục tiêu
- **Phát triển mối quan hệ:** Phát triển mối quan hệ với những nhân viên đã được lựa chọn
- **Khai thác mối quan hệ:** Tập hợp thông tin tài khoản nhạy cảm, thông tin tài chính, và công nghệ hiện tại



Những ảnh hưởng lên tổ chức khi bị tấn công

- Mất sự riêng tư
- Tổn hại uy tín
- Những mất mát về kinh tế
- chính sách khủng bố
- Các vụ kiện và các thủ tục
- Tạm thời hoặc vĩnh viễn đóng cửa

Các phương pháp tấn công



Online

Kết nối Internet cho phép kẻ tấn công tiếp cận nhân viên từ một nguồn internet ẩn danh và thuyết phục họ cung cấp những thông tin thông qua một User đáng tin cậy



Telephone

Yêu cầu thông tin, thông thường bằng cách giả mạo người dùng hợp pháp, mà người đó có thể truy cập tới hệ thống điện thoại hoặc có thể truy cập từ xa vào hệ thống máy tính



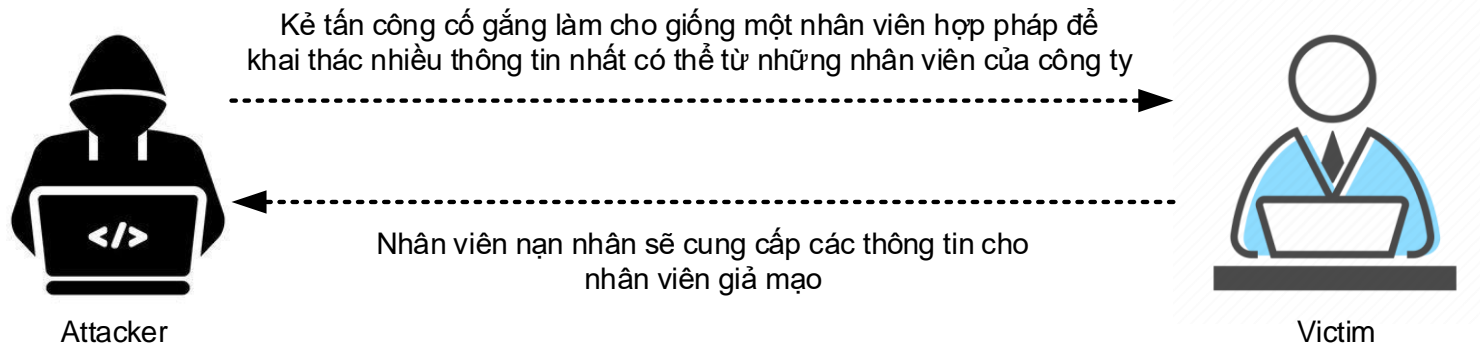
Tiếp cận trực tiếp

Trong việc tiếp cận đối tượng, kẻ tấn công sẽ lấy thông tin bằng cách trực tiếp hỏi đối tượng đó

Những mục tiêu chung của Social Engineering

- Nhân viên tiếp tân và nhân viên hỗ trợ
- Người dùng và khách hàng
- Người bán hàng của doanh nghiệp
- Người quản trị hệ thống
- Giám đốc hỗ trợ kỹ thuật

Những mục tiêu chung của Social Engineering: Nhân viên văn phòng



- Mặc dù có tường lửa tốt nhất, phát hiện xâm nhập, và hệ thống chống virus, thì bạn vẫn bị tấn công bởi những lỗ hổng bảo mật.
- kẻ tấn công có thể cố gắng tấn công Social Engineering lên những nhân viên văn phòng để thu thập những dữ liệu nhạy cảm như:
 - Những chính sách bảo mật
 - Những tài liệu nhạy cảm
 - Cấu trúc mạng văn phòng
 - Những mật khẩu

Mục lục

1. Khái niệm Social Engineering
- 2. Kỹ thuật Social Engineering**
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

Các kiểu Social Engineering

Human-based:

- Tập hợp những thông tin nhạy cảm bằng cách khai thác sự tin tưởng, sợ hãi và sự giúp đỡ

Computer-based:

- Social Engineering được thực hiện bởi sự giúp đỡ của máy tính

Human-based (1)

- **Mạo danh**

- là giả mạo thành một người hay một vật nào đó. Kẻ tấn công giả mạo thành một người dùng chính thống hay người có thẩm quyền.
- Phương pháp này thực hiện trong thực tế hoặc qua một kênh giao tiếp như email, điện thoại ...

Human-based (2)

Giả làm một người sử dụng hợp pháp

- Nhận dạng và yêu cầu thông tin nhạy cảm “Chào ! Đây là John, từ bộ phận X, tôi đã quên password của tôi. Bạn có thể lấy lại nó dùm tôi được chứ ?”

Giả làm một khách hàng quan trọng (VIP)

- “Chào tôi là Kevin, tôi là thư kí giám đốc kinh doanh. Tôi đang làm một dự án cấp bách và bị mất mật khẩu hệ thống của mình. Bạn có thể giúp tôi được chứ?”

Giả làm nhân viên hỗ trợ kỹ thuật

- Nói như một nhân viên hỗ trợ kỹ thuật và yêu cầu ID và mật khẩu cho việc khôi phục dữ liệu “Thưa ngài, tôi là Mathew, nhân viên hỗ trợ kỹ thuật, công ty X, tôi qua chúng tôi có một hệ thống bị sập ở đây do đó chúng tôi đến để kiểm tra có bị mất dữ liệu hay không. Ngài có thể cung cấp cho tôi ID và mật khẩu không?”

Human-based (3)

Ví dụ về việc hỗ trợ kỹ thuật

- “Một người đàn ông gọi đến bàn hỗ trợ của công ty và nói rằng ông ta đã quên mật khẩu của ông ta. Ông ta nói thêm rằng nếu ông ta bỏ lỡ mất dự án quảng cáo lớn trên thì sẽ bị sếp của ông ta đuổi việc. Nhân viên bàn trợ giúp cảm lấy tiếc cho anh ta và nhanh chóng resets lại mật khẩu, vậy là vô tình tạo ra một lỗi vào mạng bên trong của công ty”.

Ví dụ về việc giả mạo cơ quan hỗ trợ (1)

- “Chào, tôi là John Brown. Tôi đang ở cùng với kiểm soát viên ngài Arthur Sanderson. Chúng tôi đã làm việc với công ty về một cuộc kiểm tra bất ngờ đối với bạn nhằm khắc phục các thảm họa xảy ra từ bạn.
- Bộ phận của bạn có 10 phút để chỉ cho tôi biết làm cách nào bạn khôi phục một website sau khi bị tai nạn

Human-based (4)

Ví dụ về việc giả mạo cơ quan hỗ trợ (2)

- “Chào, dịch vụ chuyển phát nhanh Airon phải không? Chúng tôi nhận được cuộc gọi rằng phòng máy tính bị quá nóng và cần được kiểm tra hệ thống HVAC của bạn”
- Sử dụng hệ thống mang tên HVAC (hệ thống sưởi, thông gió và điều hòa nhiệt độ) có thể thêm độ tin cậy đủ để giả mạo một kẻ xâm nhập cho phép anh ta hoặc cô ta để đạt được quyền truy cập vào tài nguyên mục tiêu.

Human-based (5)

Eavesdropping

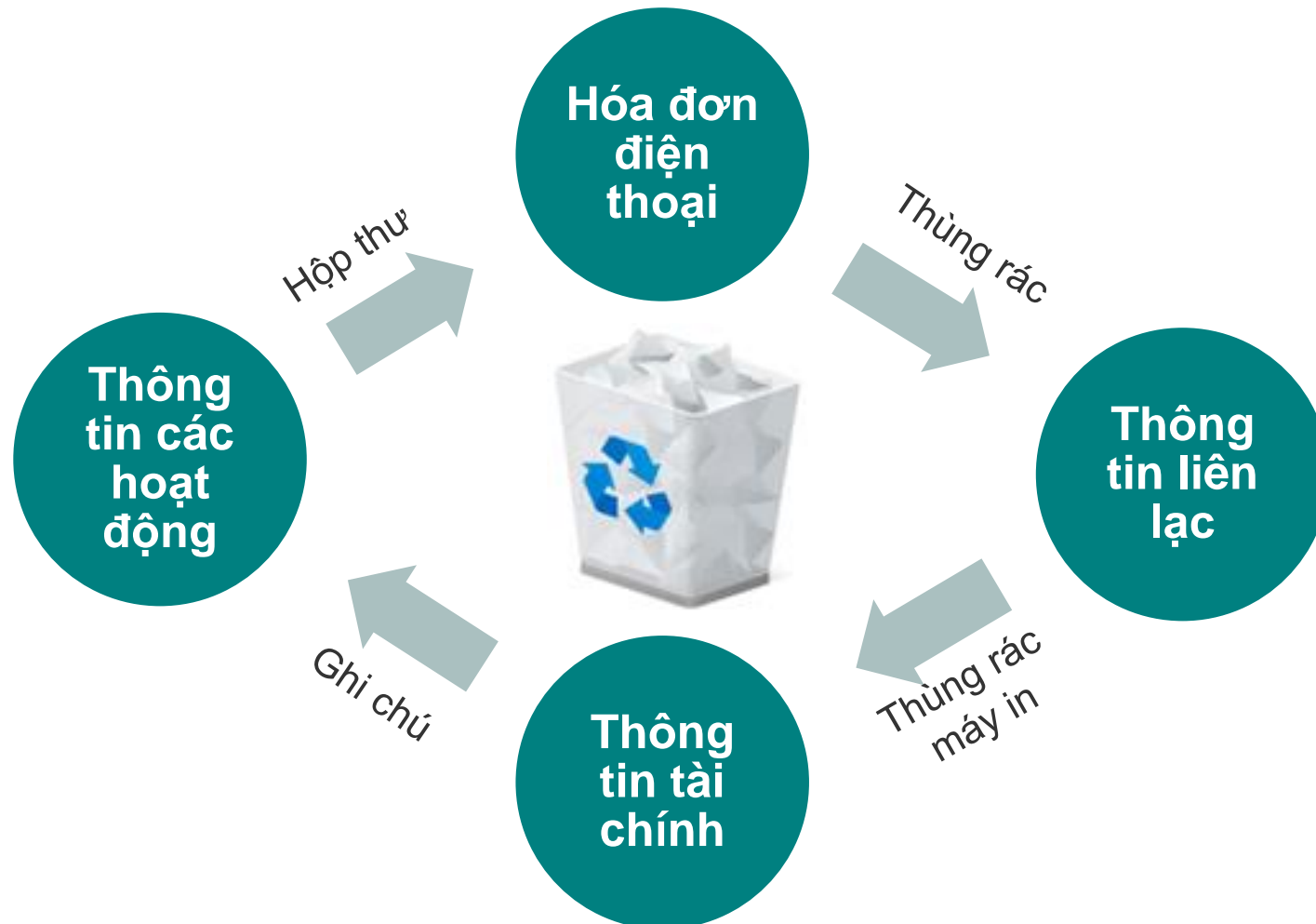
- Nghe lén hoặc nghe trái phép các cuộc hội thoại hoặc đọc tin nhắn
- Chặn lại bất kỳ các hình thức như âm thanh, video hoặc văn bản.
- Eavesdropping cũng sử dụng với những kênh truyền thông khác như đường dây điện thoại, email, tin nhắn tức thời ...

Shoulder Surfing

- Shoulder Surfing là một quy trình mà kẻ tấn công sử dụng để tìm ra mật khẩu, số chứng minh nhân dân, số tài khoản ...
- Kẻ tấn công đứng đằng sau nhìn qua vai của nạn nhân hoặc thậm chí quan sát từ một khoảng cách xa bằng cách sử dụng ống nhòm, để có được thông tin.

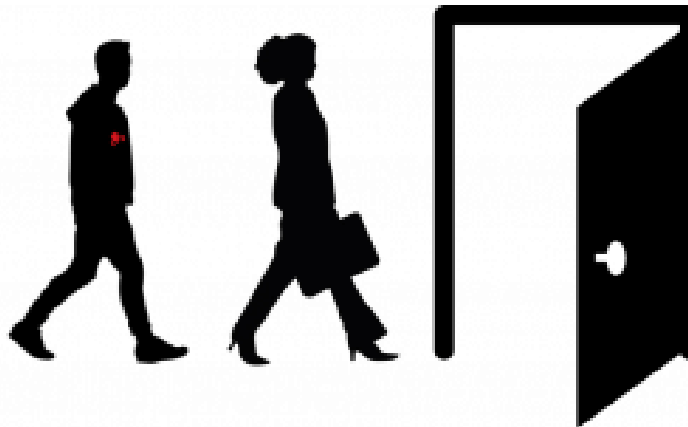
Human-based (6)

Dumpster Diving: là tìm kiếm kho báu của người khác trong thùng rác



Human-based (7)

- **Piggybacking** và **Tailgating** là hai kỹ thuật khá giống nhau.
 - **Piggyback** là phương pháp mà trong đó người không có thẩm quyền chờ một người có thẩm quyền để lấy quyền truy cập vào khu vực giới hạn. VD: Tôi quên thẻ ID ở nhà. Vui lòng hãy cho tôi đi cùng. Một người có thẩm quyền cho phép truy cập cho một người trái phép bằng cách cho cách cửa luôn được mở
 - **Tailgating** là kỹ thuật trong đó người không có thẩm quyền lấy quyền truy cập vào khu vực giới hạn bằng cách theo người có thẩm quyền. VD: sử dụng ID giả và theo sát người dùng khi đi qua điểm kiểm tra



Human-based (8)



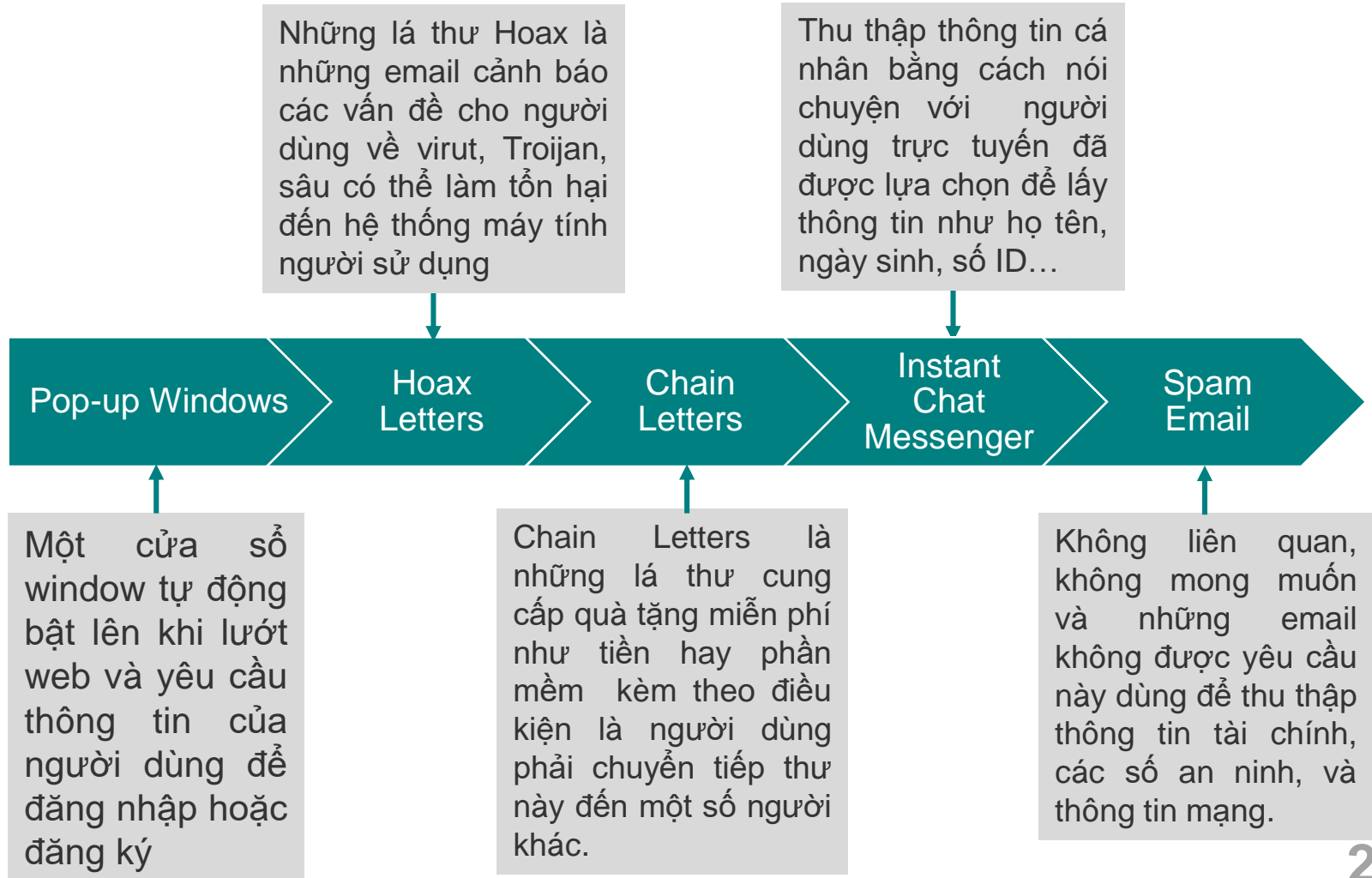
Human-based (9)



Human-based (9)

- Mạo danh
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Piggybacking
- Tailgating

Computer-based



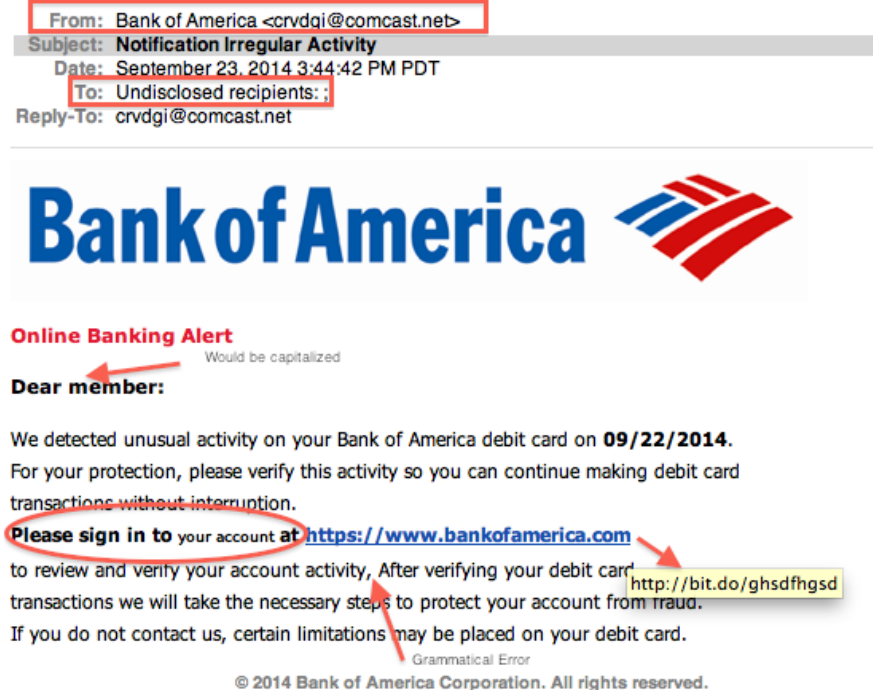
Computer-based: Pop-Ups

- Cửa sổ pop-ups lừa đảo bật lên khi click chuột vào một liên kết sẽ chuyển hướng chúng đến các trang web giả mạo yêu cầu thông tin cá nhân hoặc tải chương trình độc hại như Keyloggers, Trojan, hoặc phần mềm gián điệp

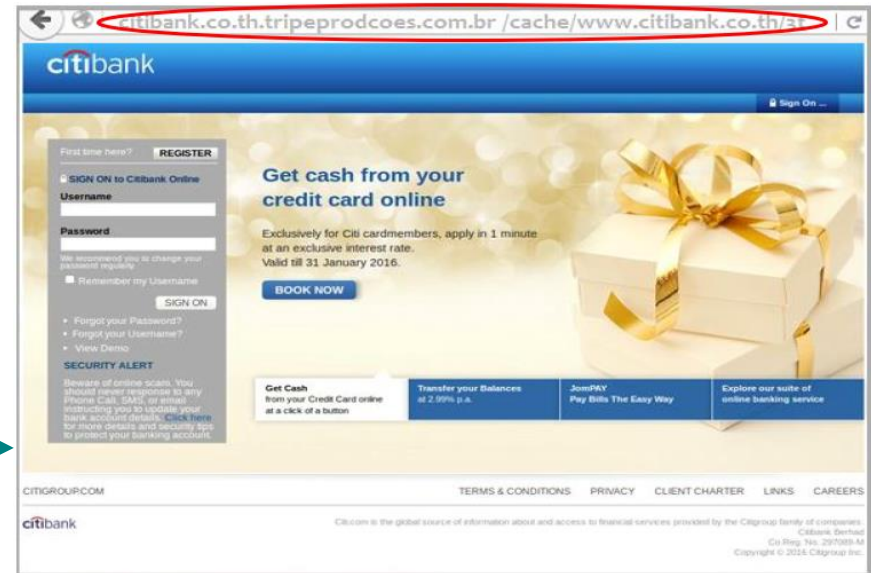
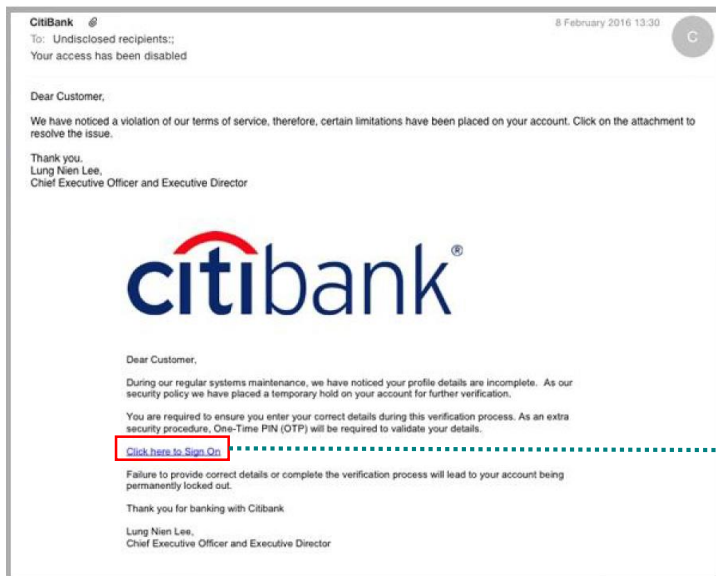


Computer-based: Phishing

- Một email giả bất hợp pháp tự nhận là đến từ một web hợp pháp và cố gắng để có được thông tin cá nhân hoặc tài khoản người dùng.
- Các email Phishing hoặc các Pop-Up chuyển hướng người dùng tới những trang web giả mạo bắt trước trang web đáng tin cậy và yêu cầu họ gửi thông tin các nhân của họ



Computer-based: Phishing



Social Engineering sử dụng SMS

- Tracy nhận được một tin nhắn SMS, mạo nhận từ bộ phận bảo mật tại ngân hàng XIM. Trong đó nói có việc khẩn cấp và Tracy nên gọi ngay một cuộc điện thoại ngay lập tức, cô lo lắng và đã gọi để kiểm tra tài khoản của mình.
- Cô đã gọi cho số đó và nghĩ đó là số điện thoại của dịch vụ khách hàng của ngân hàng XIM. Kẻ tấn công thông báo cuộc gọi đang được ghi âm đồng thời yêu cầu cô cung cấp thẻ tín dụng hoặc số thẻ ghi nợ
- Không có gì ngạc nhiên, Tracy đã tiết lộ những thông tin nhạy cảm do tin nhắn giả mạo trên gây ra



Tấn công Insider

Spying

- Nếu đối thủ cạnh tranh muốn gây ra thiệt hại cho một tổ chức, ăn cắp các bí mật quan trọng, hoặc tiêu diệt, họ chỉ cần tìm ra một công việc mà tổ chức này đang cần và cho người của mình tham gia, vượt qua vòng phỏng vấn, và họ đã có người của họ trong tổ chức đó.

Revenge

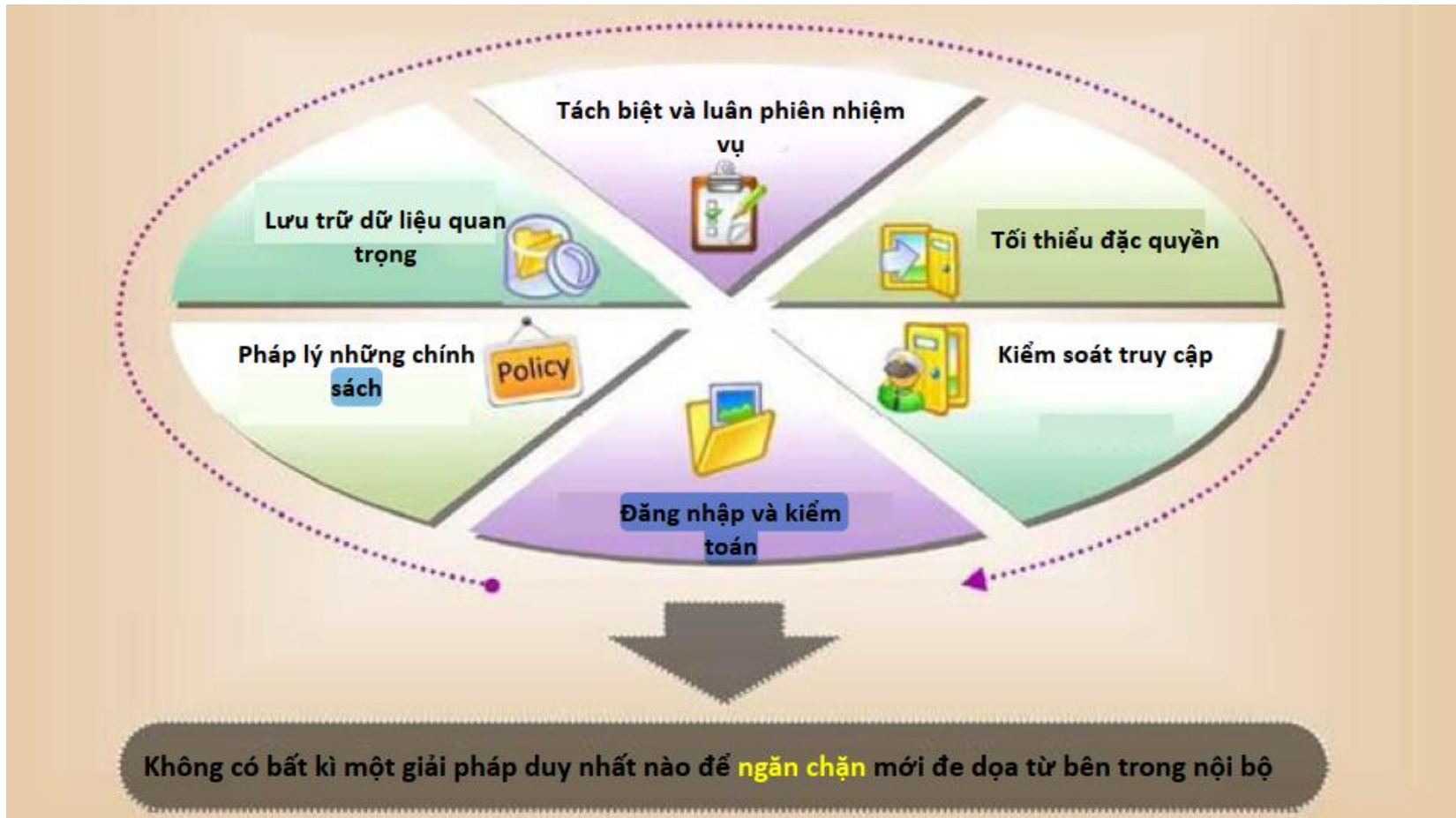
- việc trả thù chỉ cần có người bất mãn để trả thù và công ty đó sẽ bị tổn hại.
 - 60 % các cuộc tấn công xảy ra phía sau tường lửa
 - Một cuộc tấn công bên trong sẽ dễ dàng khởi động
 - Phòng chống là rất khó khăn
 - Những kẻ tấn công bên trong có thể dễ dàng thành công

Nhân viên bất mãn

- Hầu hết các trường hợp lạm dụng nội bộ có thể được khởi nguồn từ một cá nhân sống nội tâm, không có khả năng đối phó với căng thẳng hay xung đột, và cảm thấy thất vọng với công việc của mình, chính trị trong văn phòng và sự thiếu tôn trọng ...
- Những nhân viên bất mãn có thể cung cấp những bí mật công ty và sở hữu trí tuệ có ích cho đối thủ cạnh tranh



Ngăn chặn mối đe dọa bên trong nội bộ



Các chiến thuật xâm nhập phổ biến và chiến lược phòng chống

Lĩnh vực rủi ro	Chiến thuật của kẻ tấn công	Chiến lược phòng chống
Điện thoại (bàn trợ giúp) 	Mạo danh hoặc thuyết phục	Đào tạo nhân viên bàn trợ giúp không được tiết lộ mật khẩu cũng như các thông tin khác thông qua đường điện thoại
Lối ra vào 	Không được phép truy cập vật lý	Quản lý thẻ an ninh chặt chẽ, đào tạo nhân viên, và nhân viên an ninh
Văn phòng 	Shoulder surfing	Không nên gõ bất kỳ mật khẩu nào khi có bất kỳ người nào đang có mặt tại đó (nếu phải làm, thì nên nào việc đó rất nhanh). Gán một mã PIN cho mỗi nhân viên bàn hỗ trợ giúp đỡ
Điện thoại(bàn trợ giúp) 	Mạo danh các cuộc gọi trợ giúp	Hộ tống tất cả các khách
Văn phòng 	Lang thang qua các phòng tìm kiếm các phòng đang mở	Khóa và theo dõi Mail Room
Mail room 	Chèn các bản ghi nhớ giả mạo	Giữ phòng điện thoại riêng, phòng server, vv. Đều được khóa và kiểm kê cập nhật thiết bị
Phòng máy / phòng điện thoại riêng 	Cố gắng truy cập, loại bỏ thiết bị, hoặc đính kèm một số giao thức để lấy dữ liệu mật	Kiểm soát các cuộc gọi ở nước ngoài và các cuộc gọi đường dài, dấu viết cuộc gọi, và từ chối chuyển cuộc gọi
Điện thoại và hệ thống PBX 	Ăn cắp số điện thoại để truy cập	

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
- 3. Mạo danh trên mạng xã hội**
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập



Social Engineering thông qua mạo danh trên các mạng xã hội

- Mạo danh có nghĩa là bắt chước hoặc sao chép các hành vi hoặc hành động của người khác
- Mã độc hại được sử dụng để thu thập thông tin bí mật từ các trang mạng xã hội và tạo ra các tài khoản với những tên khác nhau
- Kẻ tấn công sử dụng những hồ sơ khác nhau để tạo ra các mạng lớn những người bạn và triết xuất thông tin để sử dụng tấn công Social Engineering
- Kẻ tấn công cũng có thể sử dụng thông tin thu thập được để tiến hành các hình thức tấn công Social Engineering khác

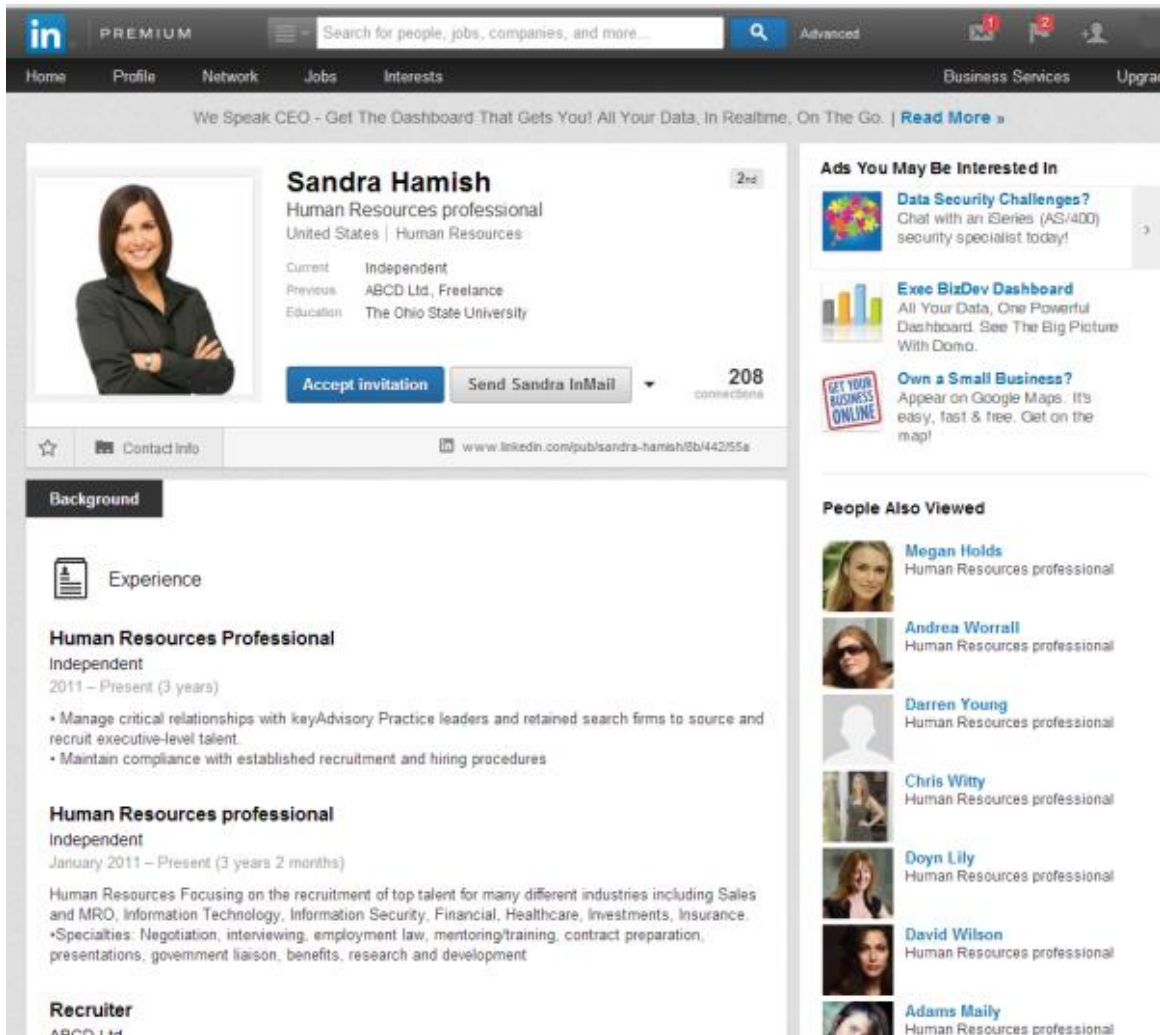
Chi tiết về tổ chức

Chi tiết nghề nghiệp

Địa chỉ liên lạc và kết nối

Chi tiết cá nhân

Social Engineering example: LinkedIn Profile



Sandra Hamish
Human Resources professional
United States | Human Resources

Current: Independent
Previous: ABCD Ltd., Freelance
Education: The Ohio State University

Accept invitation Send Sandra InMail 208 connections

Background

Experience

Human Resources Professional
Independent
2011 – Present (3 years)

- Manage critical relationships with key Advisory Practice leaders and retained search firms to source and recruit executive-level talent.
- Maintain compliance with established recruitment and hiring procedures

Human Resources professional
Independent
January 2011 – Present (3 years 2 months)

Human Resources Focusing on the recruitment of top talent for many different industries including Sales and MRO, Information Technology, Information Security, Financial, Healthcare, Investments, Insurance.

•Specialties: Negotiation, interviewing, employment law, mentoring/training, contract preparation, presentations, government liaison, benefits, research and development

Recruiter
ABCD LTD

Ads You May Be Interested In

- Data Security Challenges?**
Chat with an iSeries (AS/400) security specialist today!
- Exec BizDev Dashboard**
All Your Data, One Powerful Dashboard. See The Big Picture With Domo.
- Own a Small Business?**
Appear on Google Maps. It's easy, fast & free. Get on the map!

People Also Viewed

- Megan Holds**
Human Resources professional
- Andrea Worrall**
Human Resources professional
- Darren Young**
Human Resources professional
- Chris Witty**
Human Resources professional
- Doyn Lily**
Human Resources professional
- David Wilson**
Human Resources professional
- Adams Maily**
Human Resources professional

Social Engineering on Facebook

- Kẻ tấn công tạo ra một nhóm người sử dụng giả mạo trên facebook là “nhân viên” của công ty
- Sử dụng identity giả, kẻ tấn công sau đó sẽ tiến tới “làm bạn”, hoặc mời, nhóm nhân viên giả mạo, nhóm nhân viên giả mạo này giả mạo là nhân viên của công ty
- Khi người sử dụng tham gia vào nhóm và họ sẽ cung cấp những thông tin về họ như ngày sinh, trường lớp, nguồn gốc, việc làm vợ chồng, tên ...
- Bằng cách sử dụng những chi tiết của một nhân viên bất kỳ nào đó, kẻ tấn công có thể truy cập vào tòa nhà công ty.



Social Engineering on Twitter

The screenshot shows the 'john_attacker's settings' page on Twitter, specifically the 'Mobile' tab. The page is framed by a blue ribbon with double arrows. The navigation bar at the top includes links for Home, Profile, Find People, Settings, Help, and Sign out. The settings tabs are Account, Password, Mobile (selected), Notices, Profile, Design, and Connections.

Use Twitter with Text Messaging!
Twitter is more fun when used through your mobile phone. Set yours up! It's easy!

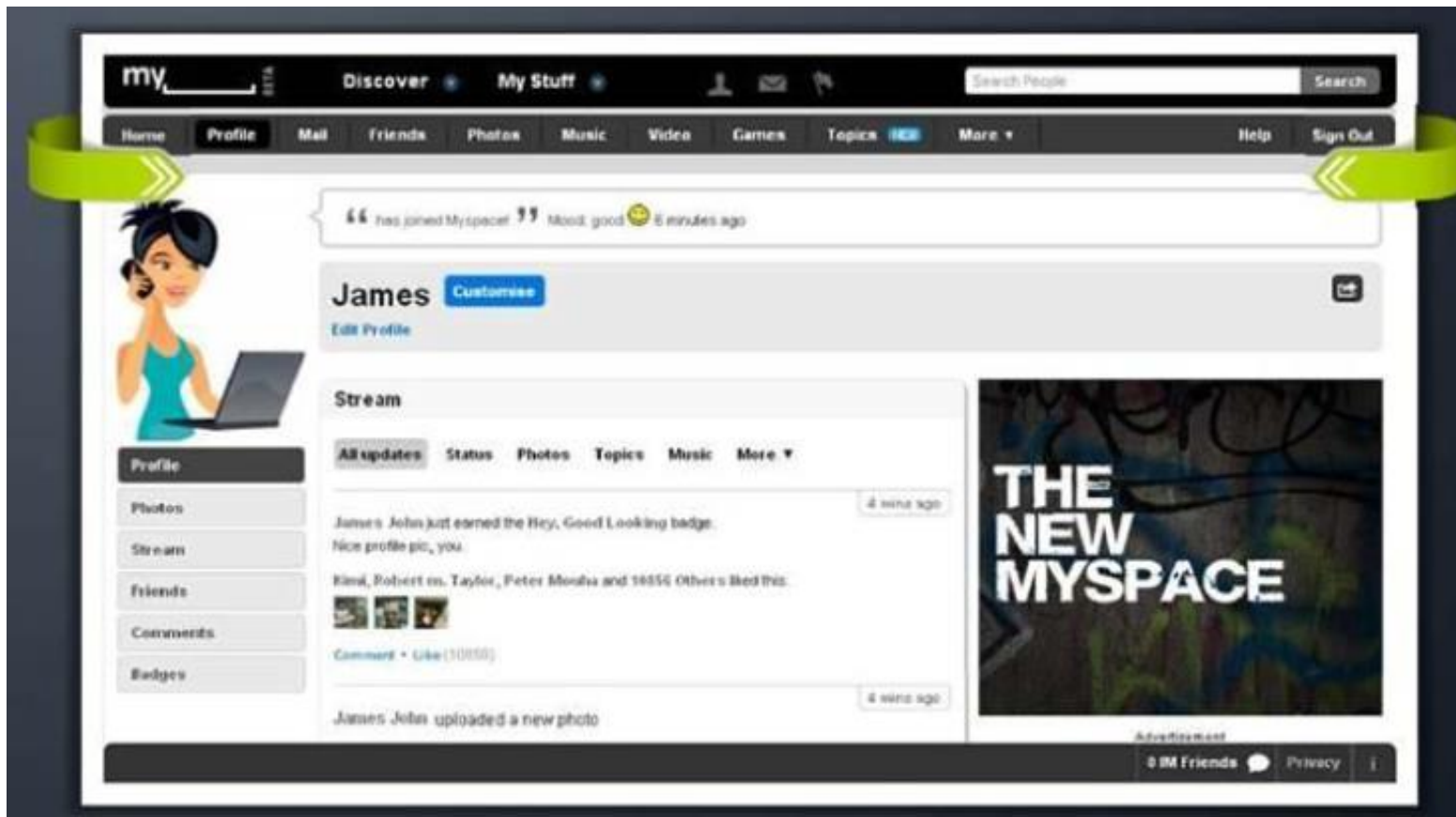
Twitter does not charge for this service. Standard message and data rates may apply.

- 1. Choose your country/region**
United States (dropdown menu)
- 2. Enter your mobile phone number**
+1 [redacted] [redacted]
☒ Let others find me by my phone number
- 3. Verify your phone**
Start

Text Messaging on Twitter
Setting up your phone allows you to:
Send tweets with text messaging on your phone.
Receive texts for DMs and the tweets from users you want to be notified about.
Clicking the phone icon on a users profile page or your followers page sets Tweet notifications for that user.
OFF ON

Twitter commands
Do more than Tweet! Send these commands to Twitter:
FOLLOW *username*
Start following a user
UNFOLLOW *username*
Stop following a user

Social Engineering on MySpace



Rủi ro của mạng xã hội với các mạng công ty

Ăn cắp dữ liệu

- Một trang web mạng xã hội là một cơ sở dữ liệu khổng lồ được truy cập bởi nhiều cá nhân, tăng nguy cơ khai thác thông tin

Không cố ý làm rò rỉ thông tin

- Trong trường hợp không có chính sách mạnh mẽ, nhân viên có thể vô tình gửi dữ liệu nhạy cảm về công ty của họ lên trên mạng xã hội

Tấn công mục tiêu

- Các thông tin trên các trang web sử dụng để thăm dò sơ bộ trong một cuộc tấn công mục tiêu

Lỗi hỏng hệ thống mạng

- Tất cả các trang mạng xã hội có thể dễ sai sót và lỗi và lộ có thể dẫn đến lỗi hỏng trong mạng của công ty

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
- 4. Ăn cắp danh tính**
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập



Số liệu thống kê tình trạng ăn cắp danh tính



Ăn cắp danh tính

Mất cắp
thông tin cá
nhân

Ăn cắp danh tính xảy ra khi một người nào đó bị ăn cắp tên của bạn và các thông tin cá nhân khác cho các mục đích gian lận

Bằng những
phương
pháp đơn
giản

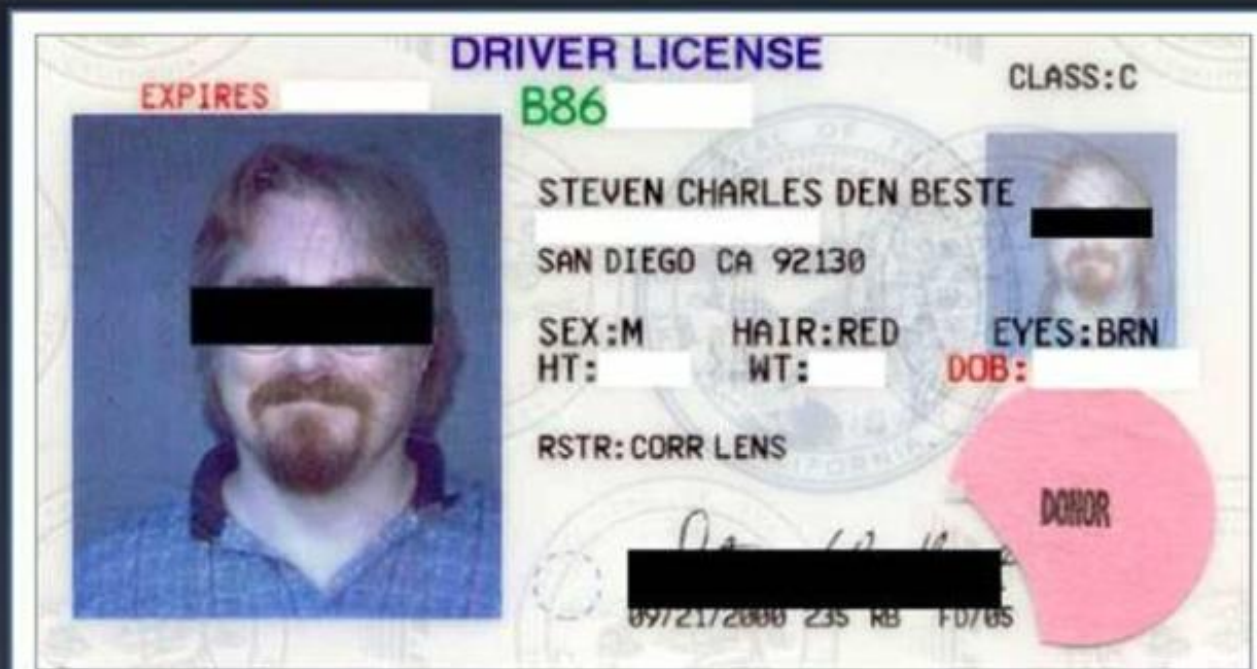
Không gian ảo đã làm cho việc ăn cắp Identity dễ dàng hơn để sử dụng thông tin cho các mục đích gian lận

Bị mất những
con số an
ninh xã hội

Ở một số nước sẽ rất nguy hiểm nếu mà kẻ mạo danh có được thông tin cá nhân, như số an ninh xã hội hoặc bằng lái xe

Làm thế nào để ăn cắp danh tính

Identity gốc – **Steven Charles**
Địa chỉ: **San Diego CA 92130**



Bước 1

Kẻ tấn công ăn cắp hóa đơn điện thoại, hóa đơn nước hoặc hóa đơn điện của Steven sử dụng Dumpster Diving, Sotolen Email, hoặc ăn trộm tại chỗ.

[illegible]

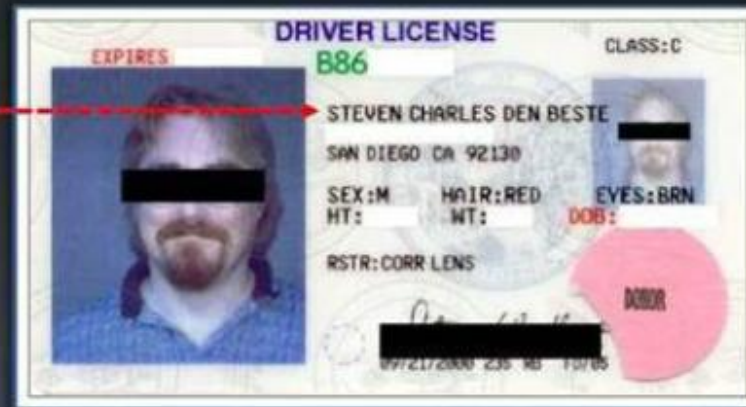
Bước 2



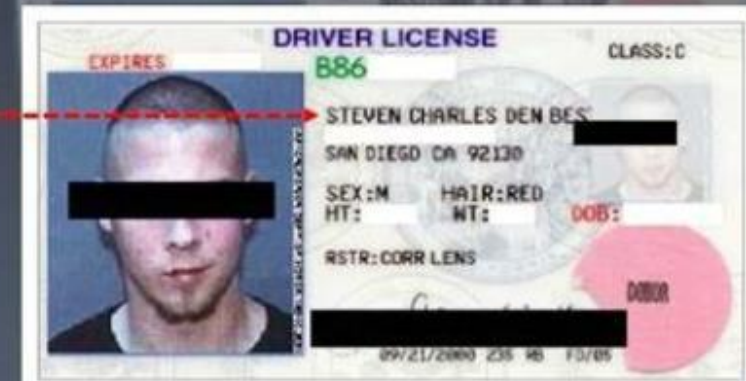
- Kẻ mạo danh (A) đến sở giao thông và nói rằng bị mất bằng lái xe
- Họ sẽ yêu cầu A cho bằng chứng xác nhận nhân thân như hóa đơn nước và hóa đơn điện
- A cho họ xem những hóa đơn đã lấy cấp
- A thông báo đã di chuyển từ địa điểm ban đầu nào (vd ở 1 bang khác)
- Nhân viên các bộ phận sẽ yêu cầu A hoàn thành hai việc cho việc thay đổi bằng lái xe và việc thứ hai cho sự thay đổi trên địa chỉ
- A sẽ cần một hình ảnh để cấp giấy phép lái xe
- Giấy phép lái xe thay thế của A sẽ được cấp với địa chỉ mới của nhà A
- Bây giờ A đã sẵn sàng với một danh tính mới.

So sánh

Ban đầu



Tên tương tự : Steven Charles
Ăn cắp Identity



Bước 3

- A đi đến một ngân hàng trong đó đã có tài khoản của Steven Charles và cho họ biết A muốn mở một thẻ tín dụng mới
- A nói với ngân hàng là không nhớ số tài khoản và yêu cầu họ tìm nó bằng cách sử dụng địa chỉ và tên Steven
- Ngân hàng sẽ yêu cầu id của A: A cho họ thấy số id trên bằng lái xe, và nếu như họ chấp nhận, thẻ tín dụng của Steven sẽ được phát hành và sẵn sàng được sử dụng bởi A
- → A có thể sẵn sàng đi shopping rồi:
 - Thực hiện mua những mặt hàng giá trị với hàng ngàn đô la
 - Vay tiền mua xe
 - Làm một hộ chiếu mới
 - Mở mới một tài khoản ngân hàng
 - Đóng các dịch vụ tiện ích của A

Kết quả



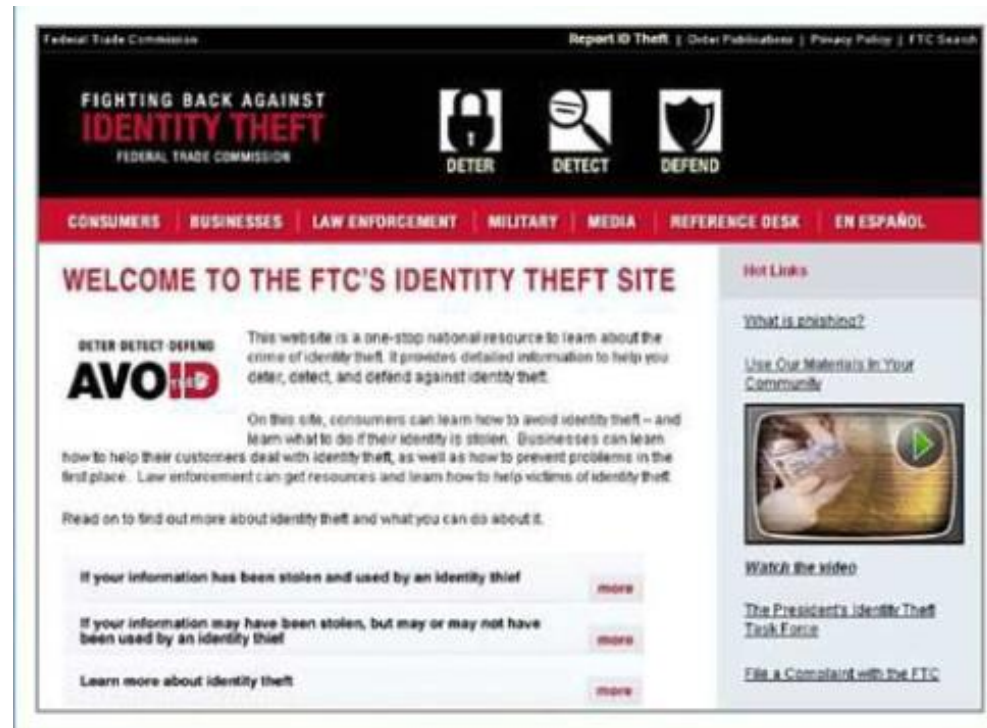
**Kẻ nào đó đã lấy cắp
số chứng minh của
tôi !**





Lấy cắp danh tính – vấn đề nghiêm trọng

- Lấy cắp danh tính là một vấn đề nghiêm trọng
- Số lượng và các hành vi vi phạm đã tăng lên
- Đảm bảo thông tin cá nhân tại nơi làm việc và tại nhà; kiểm tra các báo cáo thẻ tín dụng chỉ là một trong những cách để giảm thiểu nguy cơ mất cắp danh tính



Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
- 5. Biện pháp đối phó với Social Engineering**
6. Thử nghiệm xâm nhập

Biện Pháp Đối Phó với Social Engineering: Chính Sách

- Những chính sách và thủ tục tốt sẽ không hiệu quả nếu như chúng không được giảng dạy và trang bị cho các nhân viên của công ty.
- Sau khi được đào tạo, nhân viên phải ký một tuyên bố thừa nhận rằng họ hiểu các chính sách

Các chính sách về mật khẩu

- Thay đổi mật khẩu định kỳ
- Tránh mật khẩu đoán được
- Tài khoản cần được năng chặn sau khi cố gắng đăng nhập thất bại
- Mật khẩu phải có độ dài và tính phức tạp
- Giữ bí mật mật khẩu

Các chính sách an ninh vật lý

- Phát thẻ id, đồng phục
- Hộ tống những khách mời
- Hạn chế các khu vực truy cập
- Tiêu hủy, băm nhỏ những tài liệu không còn sử dụng
- Tuyển dụng nhân viên an ninh

Biện Pháp Đối Phó với Social Engineering

Đào tạo

- Một chương trình đào tạo hiệu quả nên bao gồm tất cả những chính sách bảo mật và phương pháp để nâng cao nhận thức về Social Engineering

Nguyên tắc hoạt động

- Đảm bảo an ninh thông tin nhạy cảm và ủy quyền sử dụng tài nguyên

Biện Pháp Đối Phó với Social Engineering

phân loại thông tin

- Phân loại các thông tin tối mật, độc quyền, sử dụng nội bộ, sử dụng công cộng

đặc quyền truy cập

- cần phải có quản trị viên, người sử dụng các tài khoản phải được ủy quyền thích hợp

Kiểm tra nhân viên và sử lý đình chỉ đúng đắn

- Trong nội bộ các tiềm tàng về hình sự và nhân viên bị thôi việc rất dễ dàng cho việc mua thông tin

tần xuất phản hồi thích hợp

- cần có những phản ứng thích hợp cho những trường hợp cố gắng sử dụng Social Engineering

Biện Pháp Đối Phó với Social Engineering

Xác thực hai yếu tố

- Thay vì mật khẩu cố định, sử dụng xác thực hai yếu tố cho những dịch vụ mạng có nguy cơ cao như VPN và Modem Pool

Phòng thủ Anti-Virus/Anti-Phishing

- sử dụng nhiều lớp để phòng chống virus như người dùng đầu cuối và mail gateway để giảm thiểu các cuộc tấn công Social Engineering

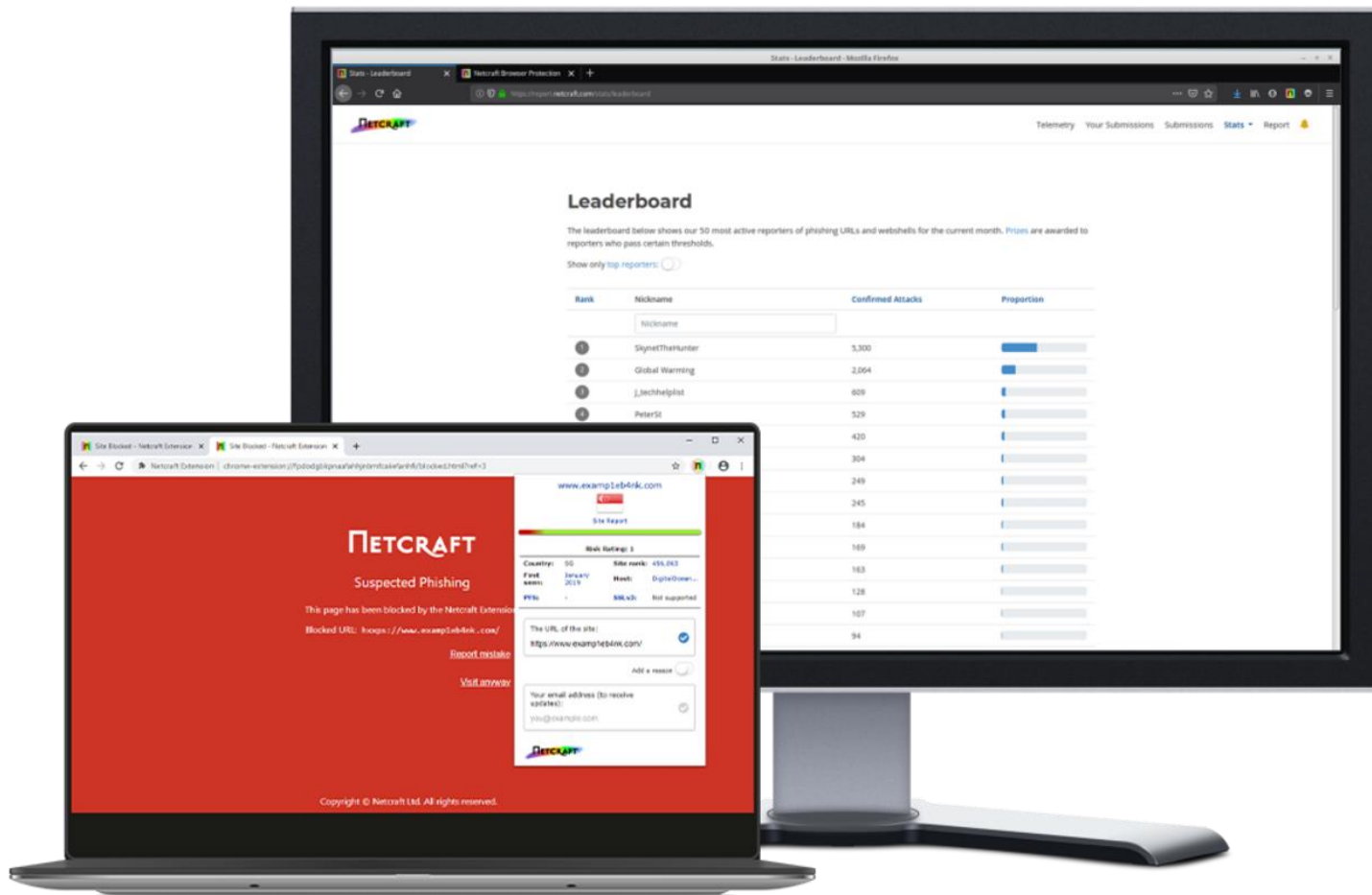
Thay đổi công tác quản lý

- việc thay đổi quy trình quản lý tài liệu sẽ bảo mật hơn


Làm thế nào để phát hiện các Email giả mạo

- Nó bao gồm các liên kết dẫn đến các trang web giả mạo yêu cầu nhập thông tin cá nhân khi click
- Email lừa đảo có vẻ đến từ một ngân hàng, tổ chức tài chính, công ty hoặc một mạng xã hội
- Giống như đến từ một người trong danh sách địa chỉ email
- Chỉ đạo để gọi một cuộc điện thoại để cung cấp số tài khoản số điện thoại cá nhân, mật khẩu hoặc các thông tin bí mật
- Bao gồm logo của các viên chức và các thông tin khác được lấy trực tiếp từ các trang web hợp pháp thuyết phục nạn nhân tiết lộ chi tiết cá nhân của mình

Thanh công cụ chống lừa đảo: Netcraft



Thanh công cụ chống lừa đảo: PhishTank


Out of the Net, into the Tank.

[Home](#)
[Add A Phish](#)
[Verify A Phish](#)
[Phish Search](#)
[Stats](#)
[FAQ](#)
[Developers](#)
[Mailing Lists](#)
[My Account](#)

[Register](#)
[Forgot P](#)

Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
8035246	https://ebisaplus.herokuapp.com/des/index.php	voldemor
8035245	https://amerikoolernet.w3spaces.com/	JackSparrow2016
8035244	https://att-101776.weeblysite.com/	prodigvabuse
8035243	https://att-103094.weeblysite.com/	prodigvabuse
8035242	http://att-103094.weeblysite.com/	prodigvabuse
8035241	https://bt-login-page-103284.weeblysite.com/	verifrom
8035240	http://bt-login-page-103284.weeblysite.com/	verifrom
8035239	https://sim-update.eu/verification/login.php	verifrom
8035238	https://sfresim.net/	verifrom
8035237	https://sfr-esim-desactivation.com/	verifrom
8035236	http://www.thefishfinder.com/mass/	r3gersec
8035235	https://youthful-golick.178-170-13-195.plesk.page/...	verifrom
8035233	https://virtual5.com.mx/mass/	r3gersec
8035232	http://positivistthings.org.uk/	Amarena98
8035231	https://funny-nobel.178-170-13-195.plesk.page/ad/w...	verifrom

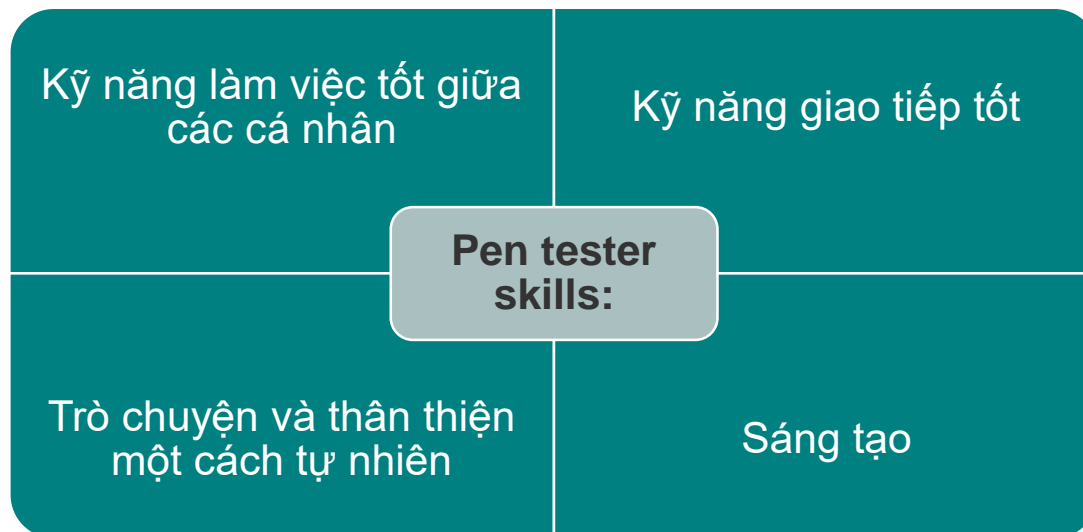
[See more suspected phishes...](#)

Biện pháp đối phó việc đánh cắp Identity

- ✓ Bảo đảm hoặc xé nhỏ tất cả các tài liệu có chứa thông tin cá nhân
- ✓ Luôn giữ cho hòm thư được an toàn, làm sạch chúng một cách nhanh chóng
- ✓ Đảm bảo rằng tên của mình không xuất hiện trong các danh sách của người tiếp thị
- ✓ Nghi ngờ và xác minh lại tất cả những yêu cầu cho dữ liệu cá nhân
- ✓ Xem xét các báo cáo thẻ tín dụng/ ghi nợ của mình một cách thường xuyên
- ✓ Không bao giờ để thẻ tín dụng/ ghi nợ của mình ngoài tầm nhìn
- ✓ Bảo vệ thông tin cá nhân của mình khi được công bố công khai
- ✓ Không bao giờ đưa ra bất cứ thông tin cá nhân nào trên điện thoại
- ✓ Không hiển thị số tài khoản hoặc số liên lạc trừ khi bắt buộc

Kiểm thử Social Engineering

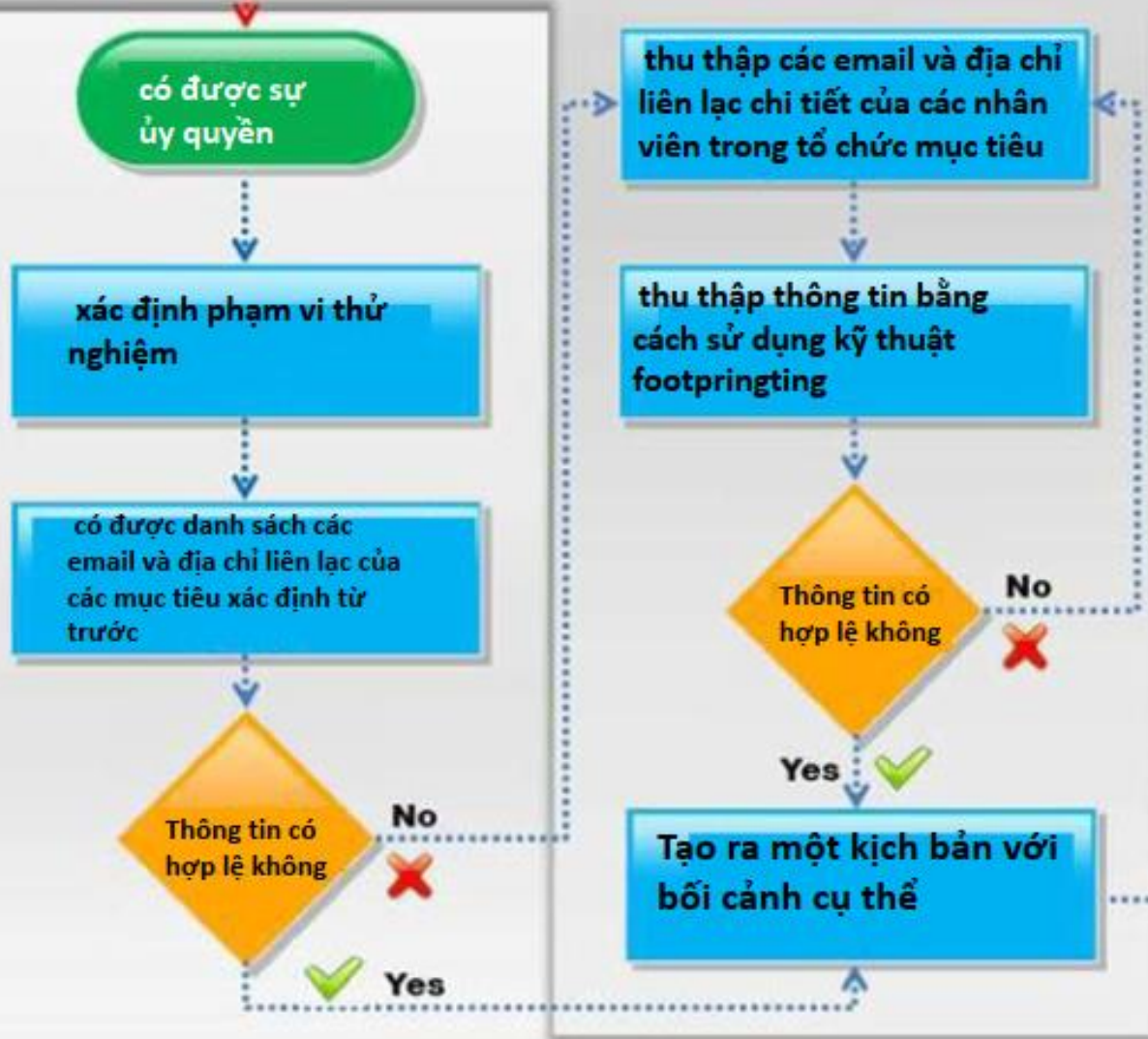
- Mục tiêu của kiểm thử Social Engineering là để kiểm tra của yếu tố con người trong một chuỗi bảo mật trong tổ chức
- Kiểm thử Social Engineering thường được sử dụng để nâng cao trình độ nhận thức bảo mật giữa các nhân viên
- Người kiểm thử phải cẩn thận và chuyên nghiệp khi thử nghiệm Social Engineering vì nó có liên quan đến vấn đề pháp lý vi phạm quyền riêng tư và có thể dẫn đến các tình huống lúng túng





START

Thử nghiệm Social Engineering



- Có được **sự ủy quyền** quản lý rõ ràng và chi tiết sẽ giúp cho **việc xác định phạm vi** kiểm tra, chẳng hạn như danh sách các danh sách các phòng ban, nhân viên cần phải được kiểm tra, hoặc mức độ xâm nhập vật lý
- Thu **thập địa chỉ email và chi tiết liên lạc** của tổ chức mục tiêu và nguồn nhân lực (nếu không được cung cấp) bằng cách sử dụng cá kỹ thuật như **Dumpster diving**, đoán email, USENET và các trang web tìm kiếm, công cụ bẫy email như Email Extractor
- Cố gắng triết xuất thông tin càng nhiều càng tốt về các mục tiêu đã xác định bằng cách sử dụng kỹ thuật footprinting
- Tạo ra một kịch bản dựa trên những thông tin thu thập được xem xét kết quả tích cực và tiêu cực của một cố gắng



Thử nghiệm Social Engineering: **Sử Dụng Emails**



- Email nhân viên yêu cầu **thông tin cá nhân** như tên người dùng mật khẩu bằng cách cải trang quản trị mạng, hỗ trợ kỹ thuật, hoặc bất kỳ ai từ các bộ phận khác nhau lấy lý do là có một trường hợp khẩn cấp
- Gửi email tới các mục tiêu có đính kèm file độc hại và theo dõi phản ứng của họ với file đính kèm đó bằng cách sử dụng công cụ như ReadNotify
- Gửi một email lừa đảo tới các mục tiêu như thể từ một ngân hàng và yêu cầu thông tin nhạy cảm từ họ (bạn cần phải có sự cho phép cần thiết cho việc này)

Thử nghiệm Social Engineering: **Sử Dụng Điện Thoại**

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như một đồng nghiệp và yêu cầu thông tin nhạy cảm

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như một user quan trọng

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như nhân viên hỗ trợ kỹ thuật và yêu cầu họ thông tin nhạy cảm

Đề cập đến một người quan trọng trong tổ chức và cố gắng thu thập dữ liệu

Gọi đến mục tiêu và cung cấp cho họ những phần thưởng thay thế cho thông tin cá nhân của họ

Đe dọa mục tiêu với những hậu quả nghiêm trọng (vd như tài khoản sẽ bị vô hiệu hóa) để có được thông tin

Sử dụng kỹ thuật Reverse Social Engineering sao cho các mục tiêu mang lại lại thông tin



Thử nghiệm Social Engineering: In Person

kết bạn với nhân viên trong quán ăn tự phục vụ và cố gắng để lấy thông tin

cố gắng vào trụ sở giả như một kiểm toán viên bên ngoài

cố gắng vào trụ sở giả như một nhân viên kỹ thuật

cố gắng vào cổng sau đeo một thẻ ID giả hoặc piggyback

cố gắng nghe trộm trên hệ thống, nhìn trộm và những người sử dụng

tất cả các tài liệu tìm thấy nằm trong một báo cáo

Thành công của bất kỳ kỹ thuật Social Engineering đều phụ thuộc vào một người thử nghiệm bằng cách nào **nó đưa ra một kịch bản thử nghiệm và kỹ năng giao tiếp của mình**

Có vô số kỹ thuật Social Engineering dựa trên những thông tin có sẵn và phạm vi thử nghiệm. **Luôn luôn xem xét các bước thử nghiệm có vấn đề pháp lý không**



Tổng kết

- Social Engineering là nghệ thuật thuyết phục mọi người tiết lộ thông tin
- Social Engineering liên quan đến việc thu thập thông tin nhạy cảm hoặc các đặc quyền truy cập không phù hợp với người ngoài
- Kỹ thuật Computer-based đề cập đến việc sử dụng các phần mềm máy tính để lấy thông tin mong muốn
- Phòng thủ thành công phụ thuộc vào chính sách tốt và việc thi hành các chính sách đó có nghiêm túc và liên tục hay không

Quotes

“Nếu bạn nghĩ rằng công nghệ có thể giải quyết các vấn đề bảo mật, thì tức là bạn không hiểu gì về các vấn đề bảo mật của bạn và công nghệ là gì!”

Bruce Schneier,
Security Technologist
and Author