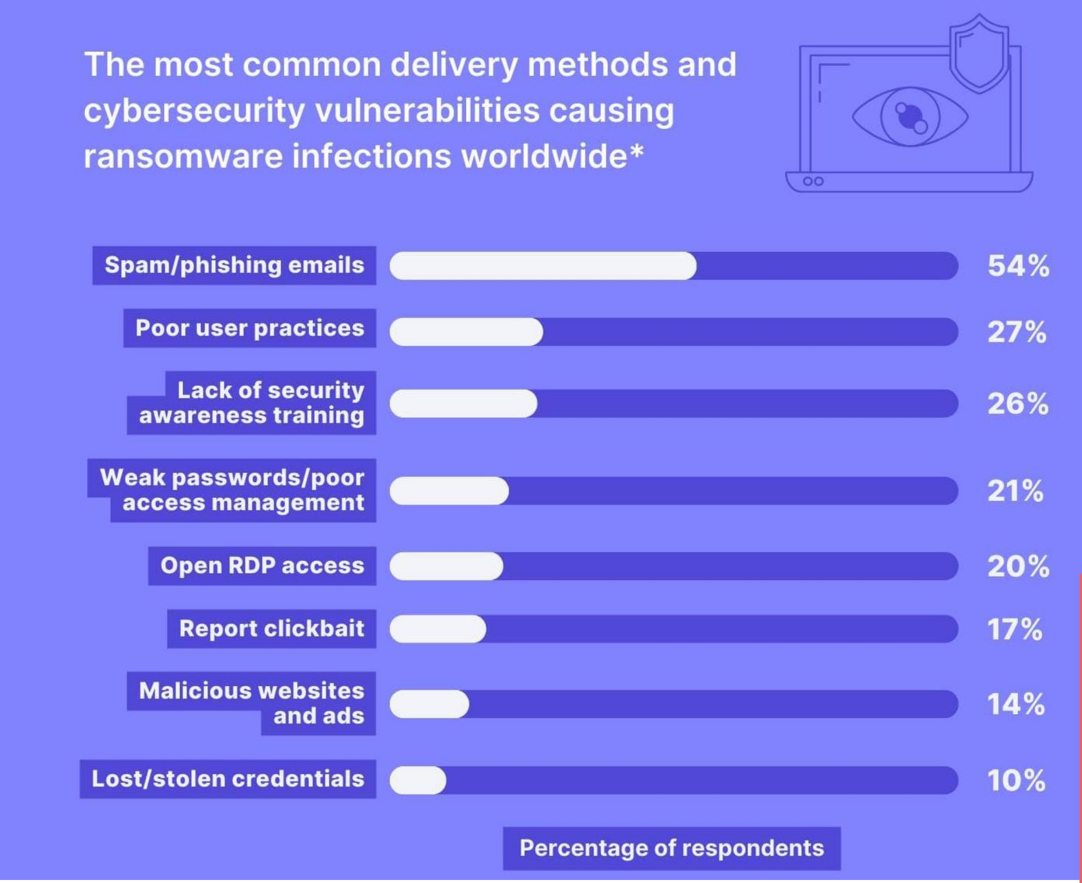
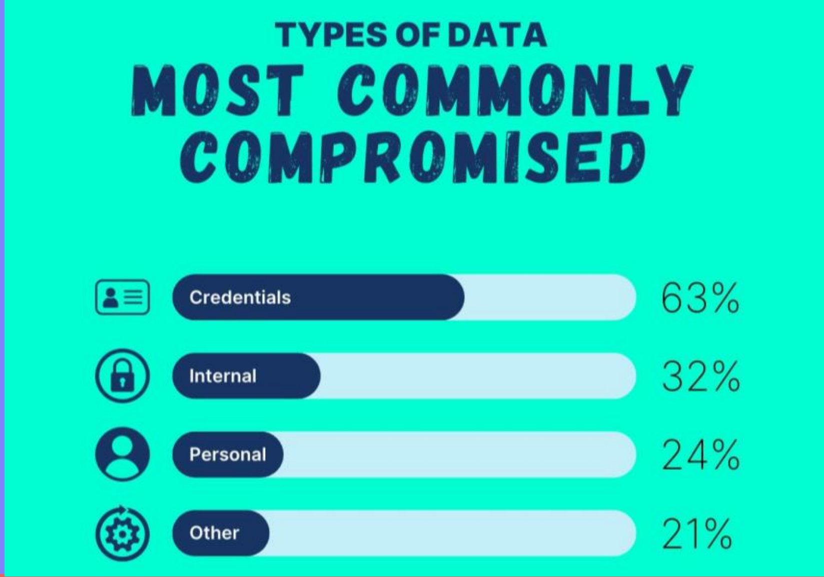
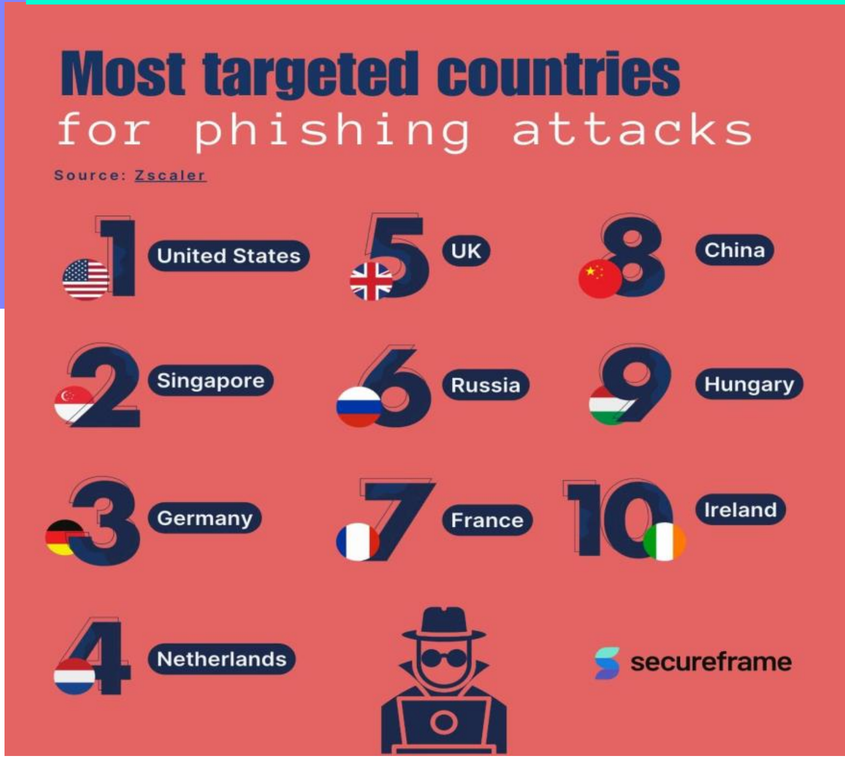
ECCS 3411: Computer Security

LECTURE 3

SOCIAL ENGINEERING







Most Imitated Brands in phishing attacks: Microsoft, WeTransfer, DHL, Google, eFax, DocuSign, Facebook, Amazon. OneDrive, Paypal..

Source: social-engineering-statistics

Social Engineering

Scenario: A person gets a call from the attacker on the pretext of an IRS investigation. The attacker requests the target's social security number to confirm the target's identity. The attacker then uses this information to apply for a loan.

An attacker may use social engineering to convince a target to:

- Click a malicious link
- Pay for nonexistent goods
- Share personal information

Definition: "Tricking" or manipulating people into revealing information or performing actions that may compromise a system's security.

https://www.youtube.com/watch?v=mwQpuDDjL-Q

The Psychology of Social Engineering – Why It Works

Principles of Influence:

1. **Authority –** A target believes the attacker is in a position of power over the target.
2. **Familiarity -** A target believes the attacker is a known individual or associated with a known organization.
3. **Intimidation -** A target believes the attacker can inflict harm.
4. **Trust** - A target believes the attacker is trustworthy because the attacker has built a connection with the target.
5. **Consensus** - A target believes the attacker's suggested action has been done by others.
6. **Scarcity** - A target believes the attacker's suggested action has limited availability.
7. **Urgency** - A target believes the attacker's suggested action has a time constraint.

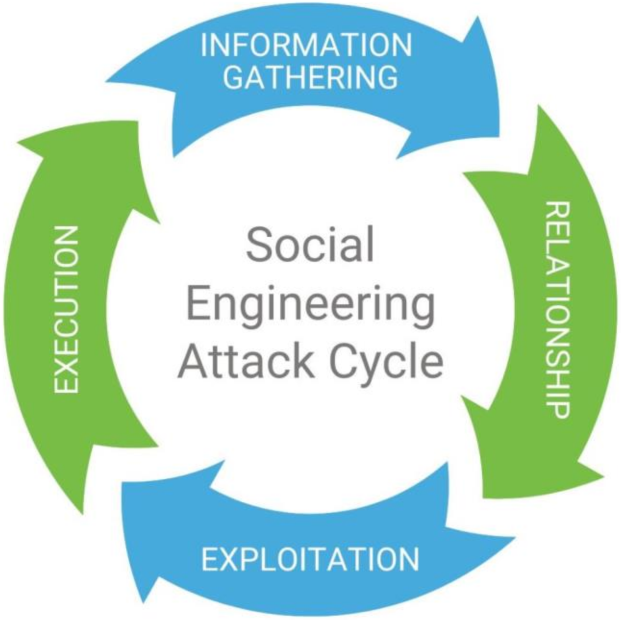
Social Engineering Lifecycle

Preparing the ground for the attack:

- Identifying the victim(s)
- Gathering background information
- Selecting attack models

Closing the interaction,
Ideally without arising any suspicion:

- Removing all traces of malware
- Covering tracks
- Bringing the charade to a natural end



Deceiving the victims to get a foothold:

- Engaging the target
- Spinning a story
- Taking control of the interaction

Obtaining the information over a period of time:

- Expanding the foothold
- Executing the attack
- Disrupting the business and/or siphoning data

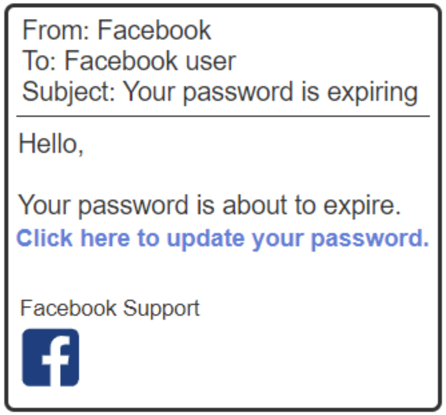
SE Attacks

- Phishing
- Baiting
- Pretexting
- Quid Pro Quo
- Tailgating/Piggybacking
- Shoulder Surfing

SE Attack Classification

Stealing a target's Facebook password

Social-based



From: Facebook
To: Facebook user
Subject: Your password is expiring

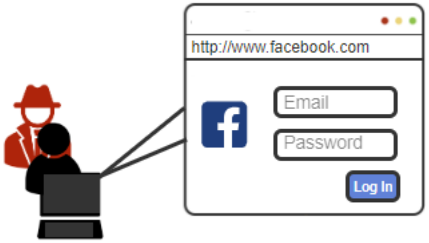
Hello,

Your password is about to expire.
Click here to update your password.

Facebook Support

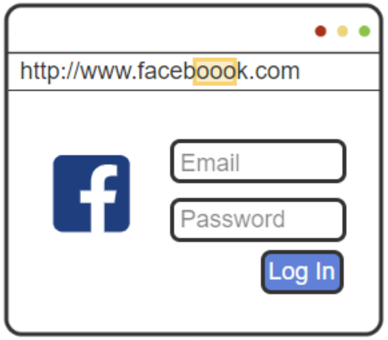
A target receives an email stating that the Facebook password is expiring.

Physical-based



The attacker watches the target enter the target's Facebook password.

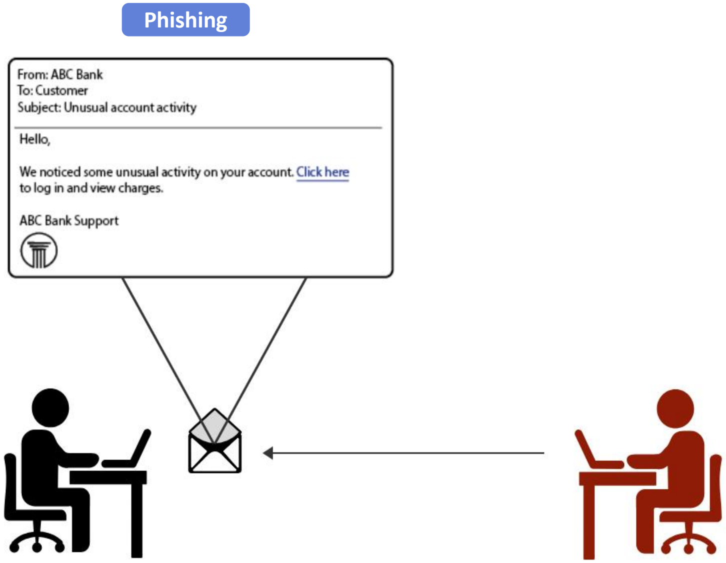
Technical-based



The attacker sets up an illegitimate website at http://www.facebooook.com to steal the password of users who accidentally add an extra "o" in Facebook.

From zyBooks – Introduction to Computer Security with CompTIA Security+

Phishing



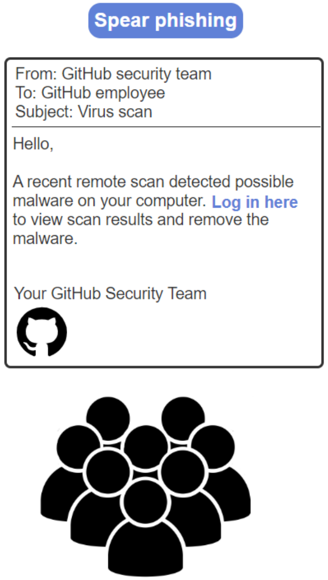
Phishing

From: ABC Bank
To: Customer
Subject: Unusual account activity

Hello,

We noticed some unusual activity on your account. Click here to log in and view charges.

ABC Bank Support



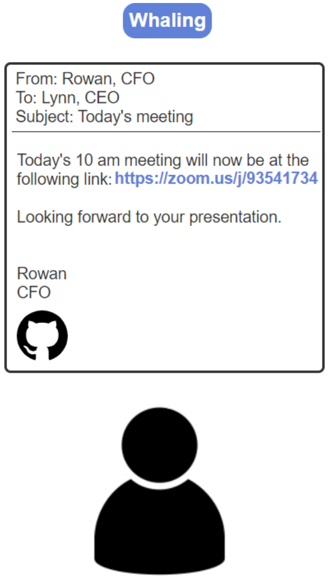
Spear phishing

From: GitHub security team
To: GitHub employee
Subject: Virus scan

Hello,

A recent remote scan detected possible malware on your computer. Log in here to view scan results and remove the malware.

Your GitHub Security Team



Whaling

From: Rowan, CFO
To: Lynn, CEO
Subject: Today's meeting

Today's 10 am meeting will now be at the following link: https://zoom.us/j/93541734

Looking forward to your presentation.

Rowan
CFO

"fishes" for confidential information by sending a fraudulent message to a target.

- **Vishing** – phishing via phone
- **Smishing** – phishing via text messages (SMS)

phishing attack aimed at a specific group or individual.

phishing attack aimed at a high-value individual like a CEO.

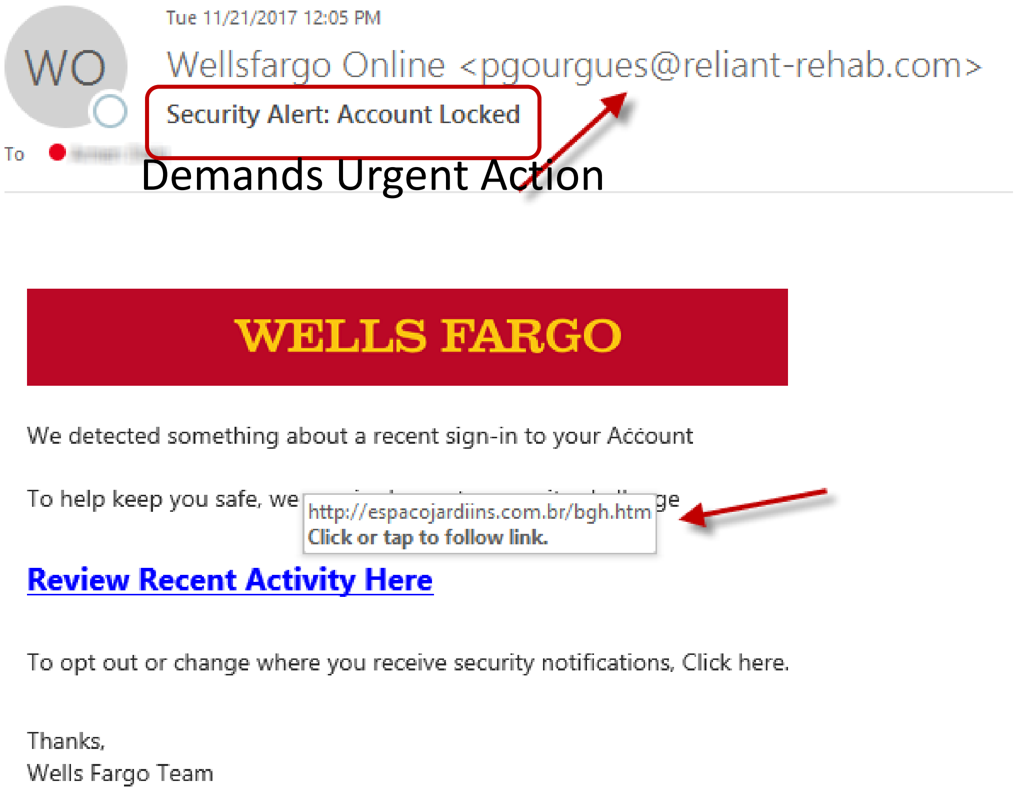
From zyBooks – Introduction to Computer Security with CompTIA Security+

Phishing Emails

Phishing Emails are:

- Emails with a very professional look and presentation. These emails may include spoofed email addresses of legitimate companies or seemingly innocent pitches such as the sale of Mother's Day flowers.
- Emails that are very short and to the point, often citing a bogus invoice, blocked payment, delivery, or fax.
- Emails that are meant to engineer click-behavior by intimidation, such as an email made to look like it is from the FBI, a bank authority, or the IRS.

Phishing Email



Tue 11/21/2017 12:05 PM

Wellsfargo Online <pgourgues@reliant-rehab.com>

Security Alert: Account Locked

To [redacted]

Demands Urgent Action

WELLS FARGO

We detected something about a recent sign-in to your Account

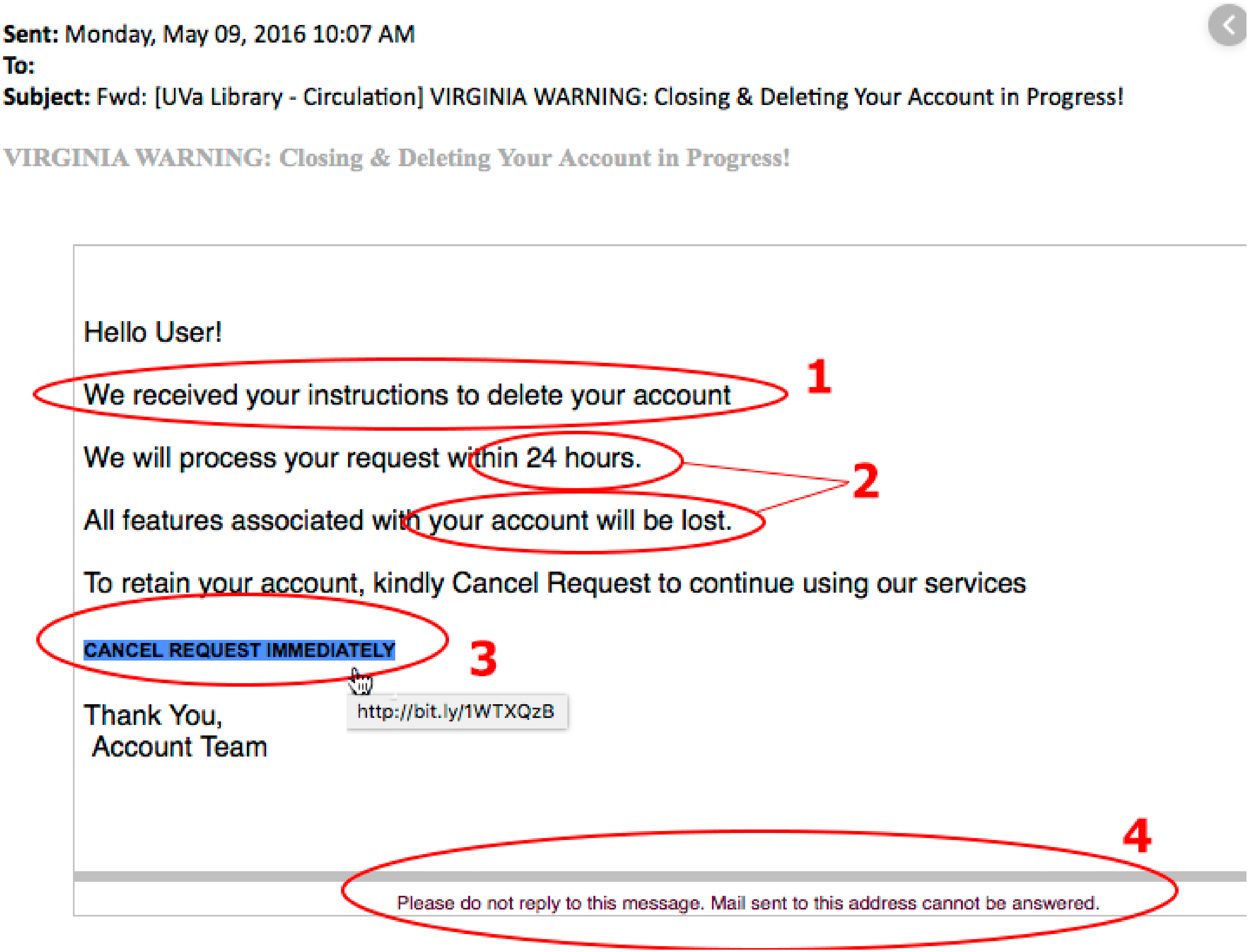
To help keep you safe, we ge

http://espacojardiins.com.br/bgh.htm
Click or tap to follow link.

Review Recent Activity Here

To opt out or change where you receive security notifications, Click here.

Thanks,
Wells Fargo Team



Sent: Monday, May 09, 2016 10:07 AM
To:
Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

We will process your request within 24 hours.

All features associated with your account will be lost.

To retain your account, kindly Cancel Request to continue using our services

CANCEL REQUEST IMMEDIATELY

http://bit.ly/1WTXQzB

Thank You,
Account Team

Please do not reply to this message. Mail sent to this address cannot be answered.

Pretexting: The Art of Deception

How it Works?

- Research
- Pretext Creation
- Engagement
- Manipulation

Examples

- IT Support Scam
- Bank Employee
- Vendor Request
- Emergency Situation

Plays On

- Human Psychology
- Detailed Scenarios
- Information Gathering

Physical-Based SE Attacks

Dumpster diving

searching through the trash for useful information.

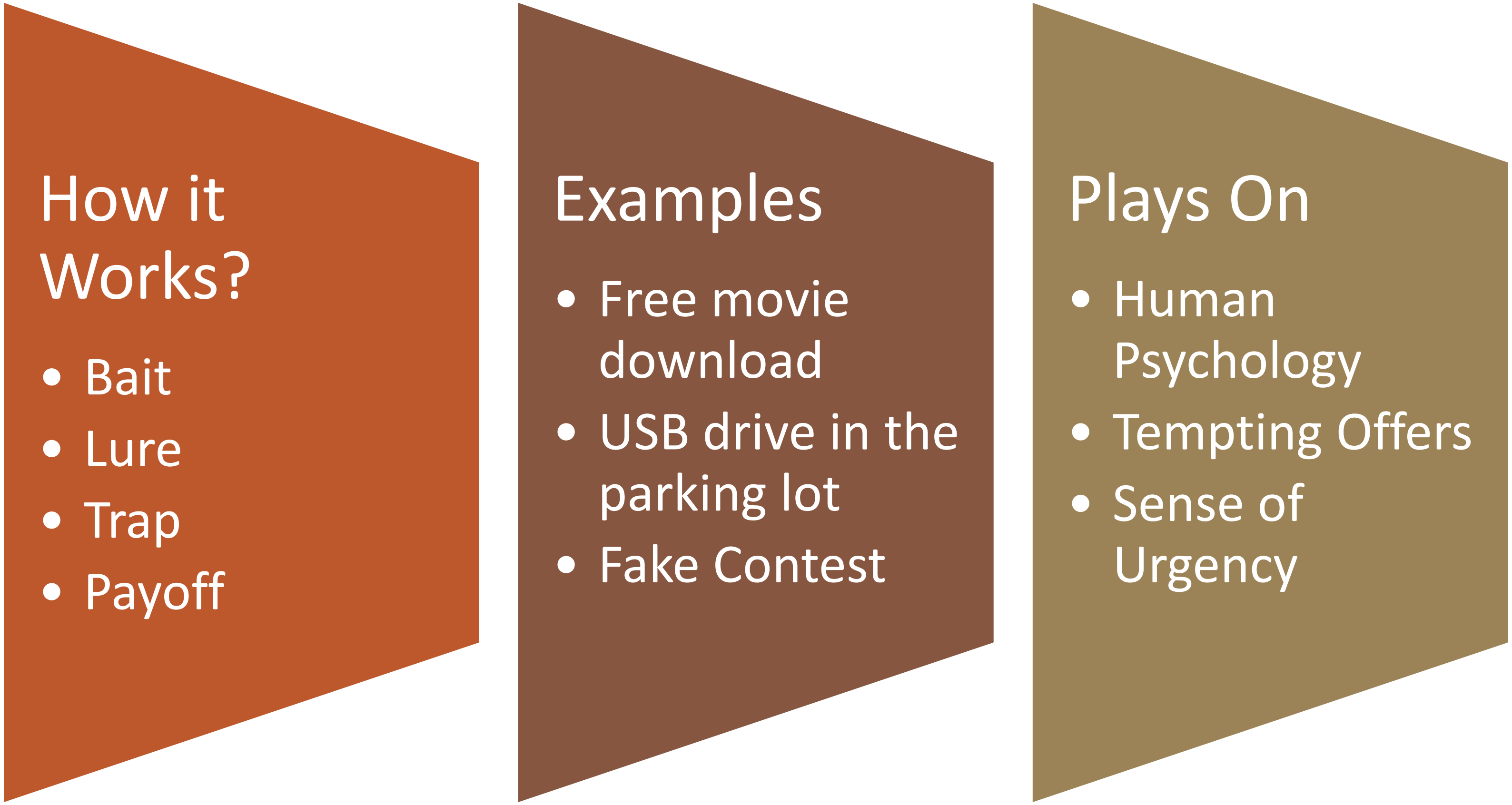
Shoulder surfing

using direct observation techniques, such as looking over someone's shoulder, to get information.

Tailgating

Following an unaware user to gain access to an area without authorization.

Baiting



How it Works?

- Bait
- Lure
- Trap
- Payoff

Examples

- Free movie download
- USB drive in the parking lot
- Fake Contest

Plays On

- Human Psychology
- Tempting Offers
- Sense of Urgency

Quid Pro Attack

How it Works?

- Offer
- Building Trust
- The Request
- The Exchange

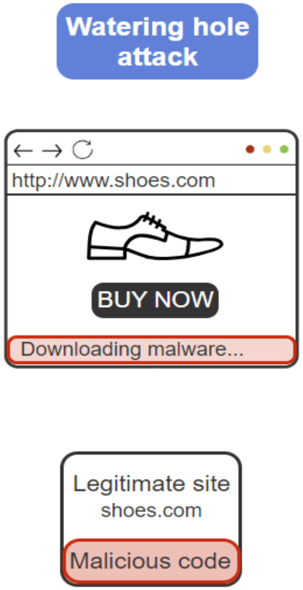
Examples

- Tech Support Scam
- Survey Scam
- IT Help Desk Scam

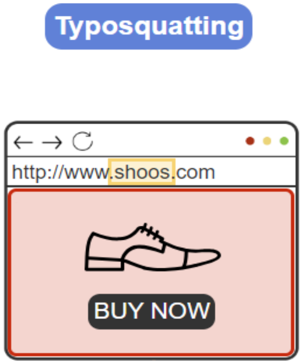
Plays On

- Reciprocity
- Trust
- Apparent Legitimacy

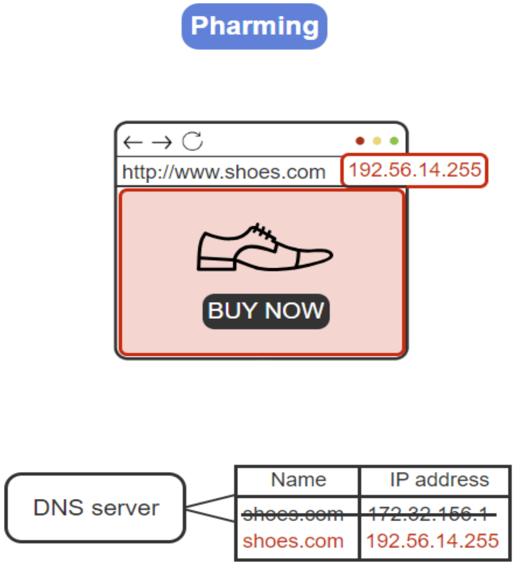
Technical-Based SE Attacks



compromises a legitimate site so that a user's computer is infected with malware when the user visits the site.



creates a fraudulent site at shoe.com to attack users who forget the second 's' in shoes.com.



Name	IP address
~~shoes.com~~	~~172.32.156.1~~
shoes.com	192.56.14.255

changes the DNS entry for shoes.com to a fraudulent site's IP address.

How to Protect Yourself?

- **Be skeptical**: Question unsolicited requests for information.
- **Verify identities**: Contact organizations directly to confirm requests.
- **Don't click on suspicious links**: Be cautious of emails, messages, and websites.
- **Use strong passwords**: And don't reuse them.
- **Enable two-factor authentication**: Add an extra layer of security.
- **Be aware of your surroundings**: Protect your passwords and sensitive information.
- **Trust your instincts**: If something feels wrong, it probably is.

Scenario:

You get a **call** from the “Help Desk.” The person calling explains that there is a problem with your computer. They ask for your Username and Password to access your machine to be able to investigate and remediate the problem.

Think (Critically) About It:

Principles of Influence Used:

Emotional Triggers Used:

Scenario:

You get a **call** from the “Help Desk.” The person calling explains that there is a problem with your computer. They ask for your Username and Password to access your machine to be able to investigate and remediate the problem.

Think (Critically) About It:

Providing your login credentials to the Caller is a liability. A password is your authentication, and as soon as even one other person knows it, it can no longer prove your identity. Any activity done on your machine, with your password, is traced back to you. Do you really want to be responsible for the actions of another?

Principles of Influence Used: Reciprocity and Authority

Emotional Triggers Used: Fear, Trust

Source: Social Engineering Education

The Ethical Dilemma

- Is social engineering ever justifiable (e.g., penetration testing)?
- The importance of informed consent.
- The potential harm of social engineering attacks.