Social Engineering

How to Identify and Prevent Social Engineering Cyberattacks – Especially in the Age of COVID-19

faegre drinker

Faegre Drinker Biddle & Reath LLP

Presenters

Bennett B. Borden
Partner and Chief Data Scientist, Faegre Drinker

bennett.borden@faegredrinker.com

+1 202 230 5194

Jason G. Weiss
Counsel, Faegre Drinker

jason.weiss@faegredrinker.com

+ 1 310 203 4062

Art Ehuan
Vice President, The Crypsis Group

Art.Ehuan@crypsisgroup.com

+1 571 331 7763

Stefan Richards
CISO, CorVel

Stefan_Richards@corvel.com

faegre drinker


IDENTIFYING SOCIAL ENGINEERING
ATTACKS

Why Do You Need Cybersecurity?

- Cybersecurity refers, in general terms, to a “body of technology, processes and practices” designed to:
  - Protect Networks
  - Protect Devices
  - Protect Programs
  - **Protect Data** from attack, damage or unauthorized access
- Cybersecurity is the protection of data and systems within networks that are connected to the Internet, including:
  - Information Security
  - Information Technology Disaster Recovery
  - Information Privacy
- In short, Cybersecurity means different things to different people depending on your:
  - Job Title (C-Suite v. IT Manager, etc.)
  - Job Position and Responsibilities
  - What you are required to protect on a computer network

What is Cyber Social Awareness Training?

- The weakest security part of any business are the

EMPLOYEES

- (See Hack, Twitter) in July of 2020 – all initialed through social engineering techniques to infiltrate their network and take over about 130 high profile accounts
- The FBI had a saying they would drum into us almost daily → The only safe network is a network with no users!
- Two very important questions that lead to the genesis of a Social Engineering Attack:
  - How do we identify an effective social engineering attack?
  - How do we defend ourselves, especially in the age of telecommuting and COVID-19?
    - COVID-19 has added a dangerous new twist to Social Engineering attacks since people are working more from home and are less likely to identify these types of attacks when isolated from other staff and IT personnel

What is Social Engineering?

- Social Engineering is the term used for a BROAD range of malicious activities accomplished through simple human interaction and a fair share of "trickery"

- Social Engineering uses "**psychological manipulation**" to basically trick employees into making security mistakes or giving away sensitive information

- No one is immune: Many smart and careful people can fall victim to a social engineering attack without even realizing it until it is too late.
  - Vigilance and common sense are the keys to protection

Foundations of a Social Engineering Attack

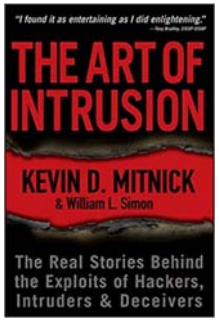
- According to www.terranovasecurity.com, Social Engineering relies on these five basic emotional traits for its success, including:

Social Engineering "MOTIVIATIONS"	How it Affects People that Fall for these Social Engineering Techniques
FEAR	Example: You receive a voice mail that you're under investigation for tax fraud and you must call and pay an immediate fee to the "IRS"
GREED	Example: Someone convinces you that a mere $10.00 investment will pocket you $10,000 or more
CURIOUSITY	Example: Cybercriminals convince you that some event you see on the news affects you and they have evidence that they send you for review and it is in fact Malware
HELPFULNESS	Example: Playing on the basic desire of humans to trust and help one another – collecting charity and donations for a false cause
URGENCY	Example: You receive a fake or spoofed email from a vendor you use indicating that they need to confirm your credit card information ASAP

How Does Social Engineering Work?

- Social Engineering is a multi-faceted attack and includes:
  - The perpetrator first investigates the intended victim and gathers necessary background information, such as potential points of entry and weak security protocol needed to proceed with the attack
  - The attacker then moves to gain the victim's trust and provides a stimuli for subsequent action that breaks established security practices, such as revealing sensitive information and granting access to critical resources (www.imperva.com)

- Social Engineering is simply the most efficient, cost-effective and capable tool used by cyber-criminals in so many different types of crimes
  - The original master of social engineering was one of the most famous hackers our generation, Kevin Mitnick. They have literally written books about him and how he used social engineering to effectuate his attacks.



faegre drinker

Additional Common Social Engineering Attacks

Attack Type	What Happens in the Attack
1) Phishing	Targeting people through social media ruse
2) Spear Phishing	Targeting specific group of people
3) Whaling	Targeting business executives
4) Watering Hole	Injecting malicious script in public websites
5) Pretexting	Faking your identity
6) Tailgating	Piggy backing into a restricted site
7) Dumpster Diving	Going through garbage bins for sensitive info
8) Quid Pro Quo	Hacker offers service in benefit for an exchange
9) Business Email Compromises (BEC)	Faking fraudulent wire transfers - BEC has become the single largest damages claim today for Cyber Insurance - There are multiple types of BEC claims that have cost consumers well over one billion dollars ($1,000,000,000)

Some Additional Common Social Engineering Attacks

Attack Type	What Happens in the Attack
10) Smishing	Smishing is the fraudulent practice of sending text messages to trick people to reveal personal information
11) Vishing	Vishing is the fraudulent practice of making phone calls or leaving voice messages to trick people into revealing personal information
12) Baiting	Baiting attacks use a false promise to pique a victim's greed or curiosity
13) Scareware	Scareware involves victims being bombarded with false alarms and fictitious threats
14) Malware	Victims are tricked into believing that malware is installed on their computer and, if they pay, the malware will be removed
15) Doxxing	When someone threatens to publish private or identifying information about you on the internet, typically with malicious intent
16) Catfishing	When someone uses a stolen online identity for the purpose of creating a fake or deceptive relationship
17) Gaslighting	When someone tries to manipulate you into questioning your own sanity as a means to trick you into providing something of value
18) SIM Swapping	SIM swap is when someone convinces your cell phone carrier to switch your phone number over to a SIM card they own

Common Social Engineering Attacks

- Cyber Social Engineering attacks can lead to many different problems for many businesses, financial institutions and the population as a whole
  - Disruptionware
  - Ransomware
  - Cyber Wipers
  - Malware
  - Business Email Compromise
  - Economic Espionage
  - Data Sniffers
  - Keyboard Stroke Monitors
  - Back Doors Into Your Network
  - Theft Of Business Email
  - Theft Of Intellectual Property
  - Theft Of Employee PII

faegre drinker

Consequences for Poor Employee Training

- There can be numerous consequences for poor social awareness employee training, including but not limited to:
  - External breach of internal business networks
  - Loss of business or customer data
  - Introduction of ransomware, malware or other cyberattack techniques into your network
  - New Consumer “Private Right of Action” for lost data damages under the GDPR and/or the CCPA
  - Permanent loss of intellectual property
  - Public embarrassment and loss of business trust in the community
  - Bad publicity in the media
  - Loss of customers - both current and future
  - Regulatory fines by the government
  - Extensive costs to remediate breaches and repair networks to re-establish customer trust

Technical Defenses to Social Engineering Attacks

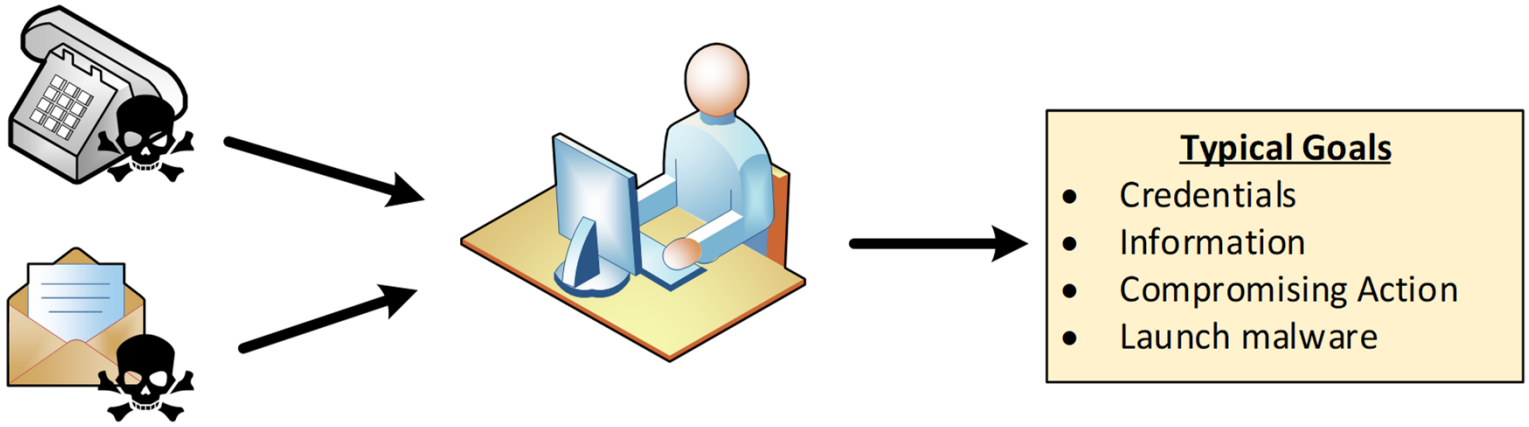
- Most companies have very astute IT departments to keep their hardware and their networks safe….
  - There is not time here to discuss all the intricacies of technical IT defense, so I want to discuss the REALLY IMPORTANT way to defend your data….
- Which leads to the most critical question of the day:
  - What is the **WEAKEST** part of any organization's data security plan?
  - Does the company have a current and up to date Incident Response Plan to react quickly?
- What has the IT department done to "harden" its network from both
  - External Attack?
  - Internal Infiltration?


TECHNICAL
SOCIAL ENGINEERING DEFENSES

Things Social Engineering Attackers Know

- **A LOT** of company information is out there, more than you might think
- **A LOT** of personal information is out there, more than you might think
- Security is very vulnerable at **connection points**
- Security is very vulnerable in **exception processes**
- It's easy to send (a lot of) email **as anyone**
- It's easy to call someone appearing to come from **any number**
- In bigger companies, most people don't know each other, but everyone wants to help
- Social engineering approaches: **go big or go targeted**
- Most people **avoid advanced security** because "it's hard"

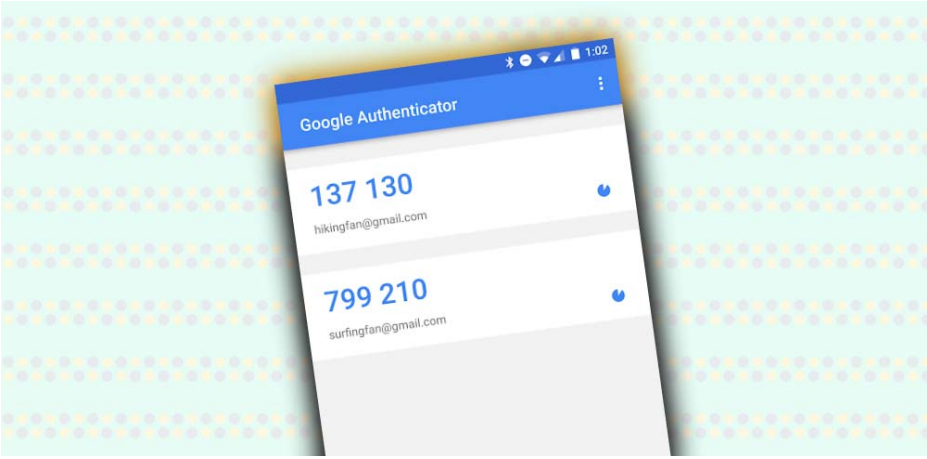
Social Engineering Attack Overview



faegre drinker

Technical Defenses – Multi-Factor Authentication (MFA)

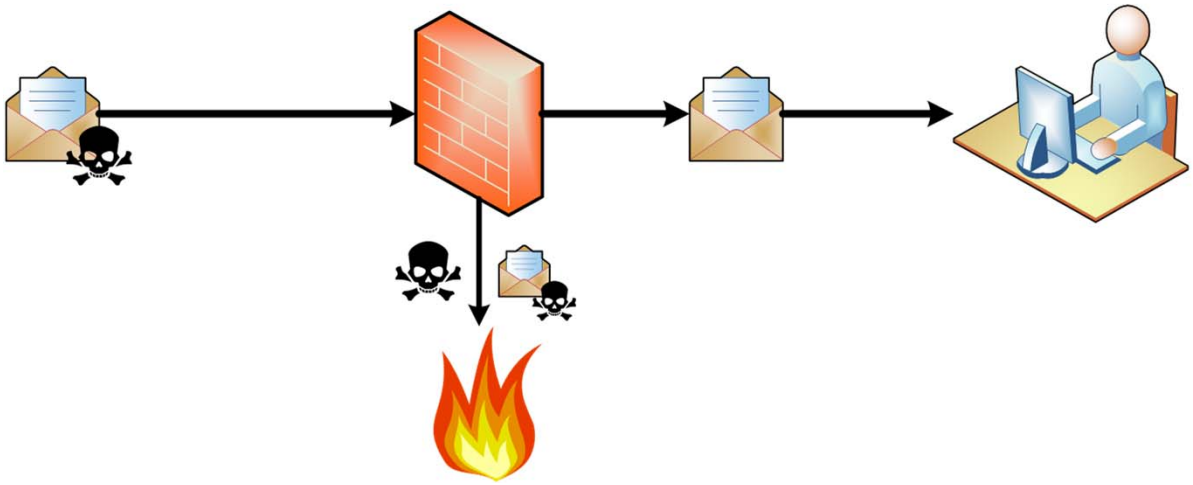
- Generally, passwords are not good enough
  - If you have to use: **<u>length is the most important factor</u>**
- MFA = the most effective mitigation
- MFA can't be given away in clever social engineering
- MFA Tips:
  - Avoid text (SMS) or email
  - **Best option:** authentication apps (e.g. Google Authenticator)
  - Consider the recovery process:
    - *Social Engineers can probably answer **<u>your</u>** security questions*



faegre drinker

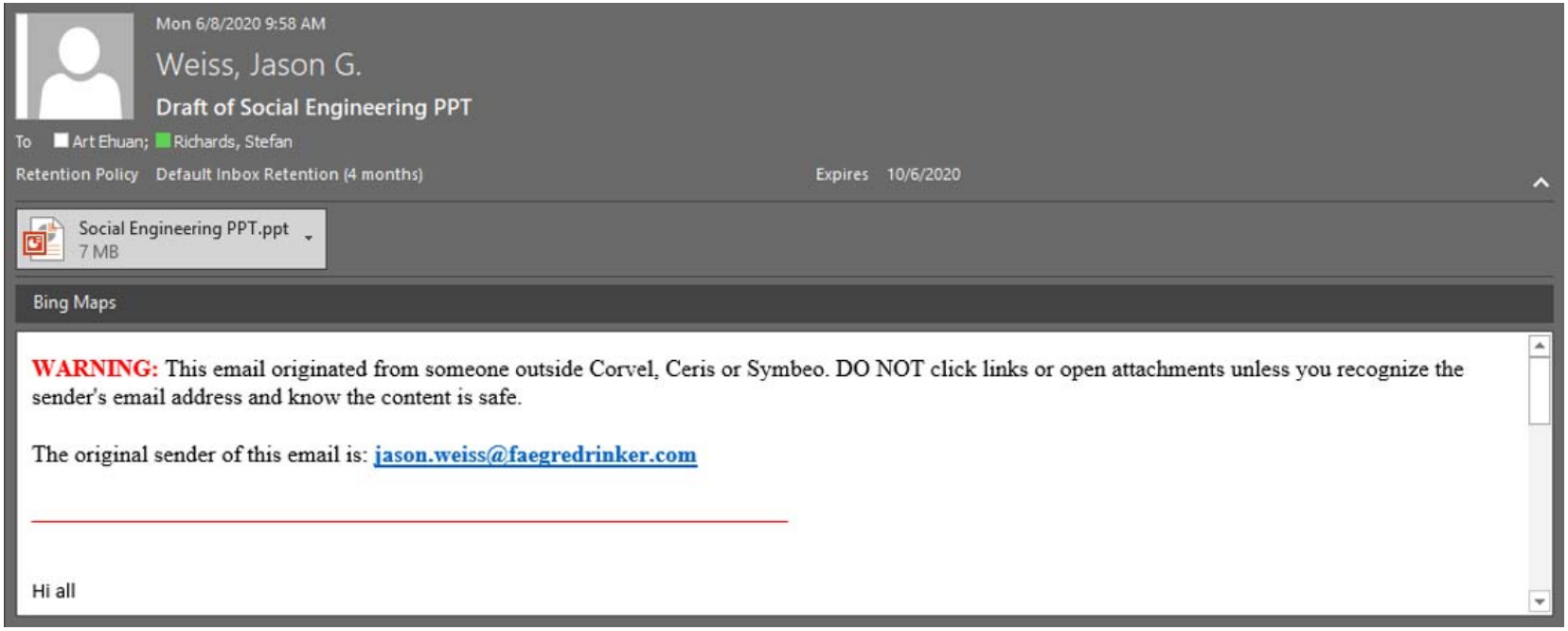
Technical Defenses – Inbound Filtering (Email Gateways)

- Stops or ‘cleans’ trouble emails before they reach you
- Leverages reputation and collective threat intelligence
- Learns from other users that flag dangerous email
- Authenticating senders – DMARC



faegre drinker

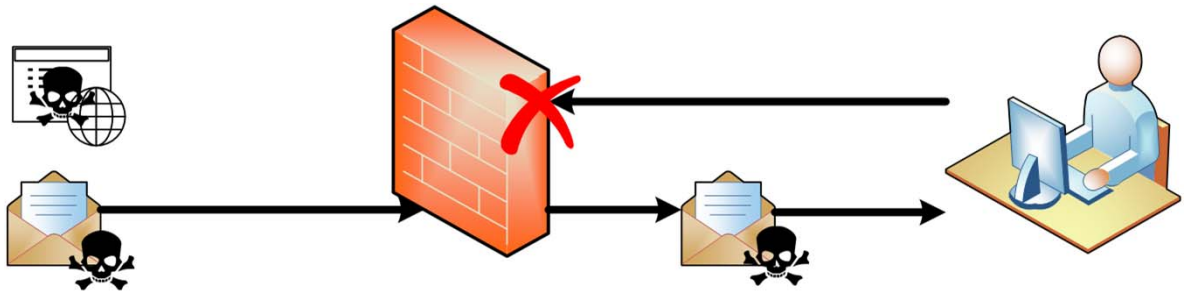
Technical Defenses – Email Banners



faegre drinker

Technical Defenses – Outbound Filtering (Firewalls, Proxies)

- Block that click!
- Stops traffic to Internet “bad neighborhoods”
- Looks for and stops malware call home (Command and Control)
- Watches outbound traffic for likely exfiltration
- Leverages reputation and collective threat intelligence



faegre drinker

Technical Defenses – Automated Phish Tests

- Automate for scale
- Test multiple times per year
- Tune to current threats
- Test all employees, especially risky departments
- Automatically refer to training on click
- Collect metrics to inform continued awareness efforts

[redacted], Carol

From: Finance <finance@financeteam.com>
Sent: Thursday, February 27, 2020 9:01 AM
To: [redacted], Carol
Subject: Quartely Bonus

WARNING: This email originated from someone outside Corvel, Ceris or Symbeo. DO NOT click links or open attachments unless you recognize the sender's email address and know the content is safe.

The original sender of this email is: **bounces+6841375-0cd9-carol[redacted]=symbeo.com@mails.phishbait.us**

Congratulations!

Thank you for being an amazing employee! Carol

This past quarter was a great one, so we thought everyone deserved a bonus. Thank you to everyone for their hard work and dedication to our growth!

CorVel Management

Click Here [u6841375.ct.sendgrid.net]To Claim Your Bonus

faegre drinker

Technical Defenses – Cyber Hygiene

- Use currently supported software only
- Patch early and often
- Remove unneeded software and services
- Don’t run as administrator
- Implement and test regular backups
- Regularly scan and test your security posture
- Consider advanced anti-malware protection

faegre drinker

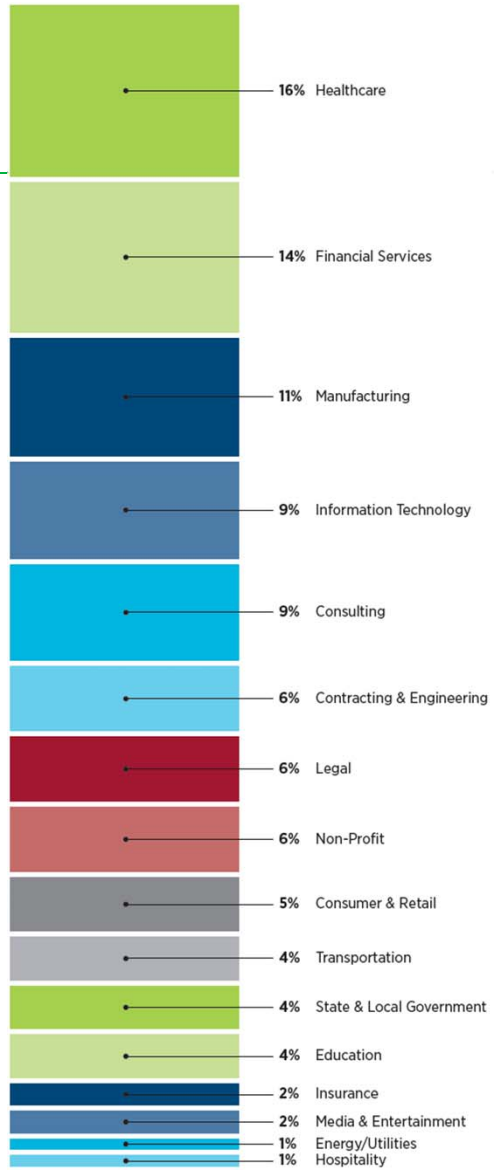

SOCIAL AWARENESS
SOCIAL ENGINEERING DEFENSES

Social Engineering Statistics 2019 – 2020 Industries

1. **Healthcare** (16%)

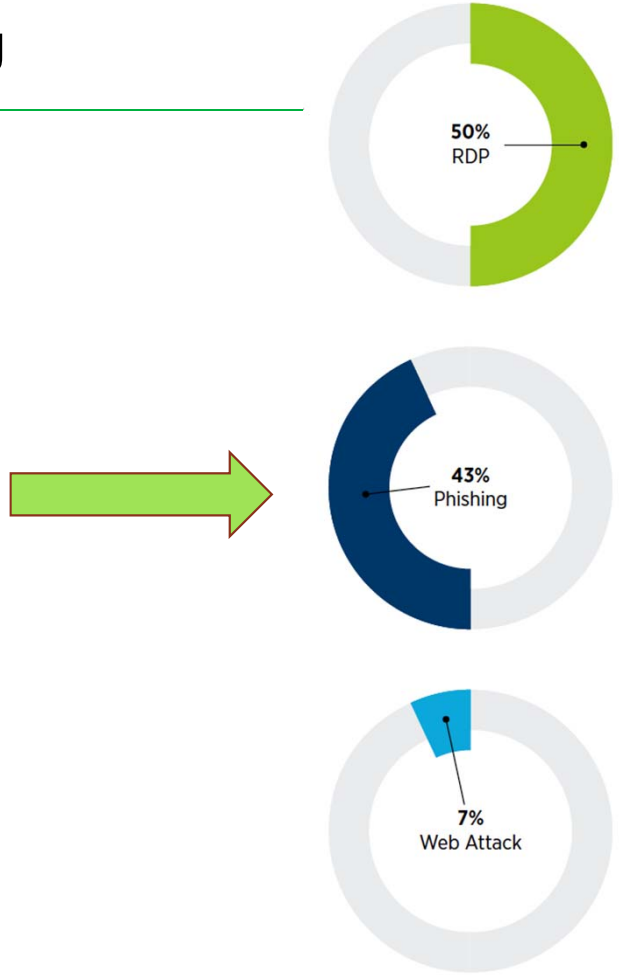
2. **Financial Services** (14%)

The top target industries disproportionately attract threat actors due to storing, transmitting, and processing high volumes of monetizable sensitive information.



Social Engineering Statistics 2019 – 2020 Phishing

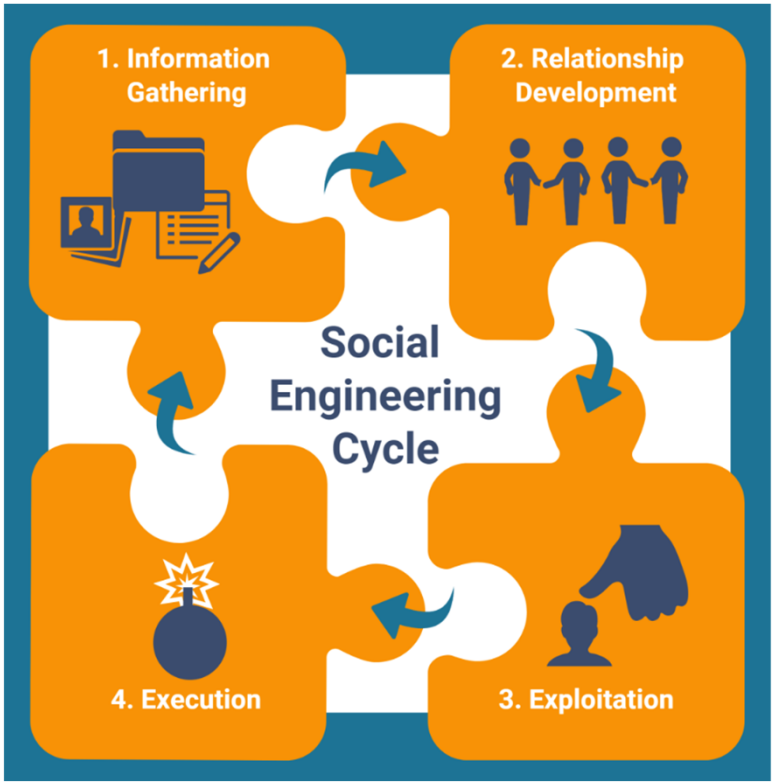
- Initial Attack Vectors for Ransomware
  - RDP Attack
  - Phishing (Social Engineering)
  - Web Attack



faegre drinker

Social Engineering Prevention (Awareness)

- Create a “security awareness” culture in the organization
  - Management should regularly conduct awareness campaigns on importance of protecting data from social engineering attacks
  - Post visual reminders (posters, etc.) throughout office space
  - Send regular email reminders on vigilance against social engineer attacks
  - Publicly reward staff who embody good security awareness



https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

faegre drinker

Social Engineering Prevention (Awareness)

- Management should regularly conduct awareness campaigns on importance of protecting data from social engineering attacks
  - Management vocalization on criticality of protecting data during staff meetings on a scheduled basis
  - Support and promote richer cyber training programs, and emphasize security in company communications
  - Management should identify opportunities for measuring performance of staff in protecting data

https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

faegre drinker

Social Engineering Prevention (Awareness)

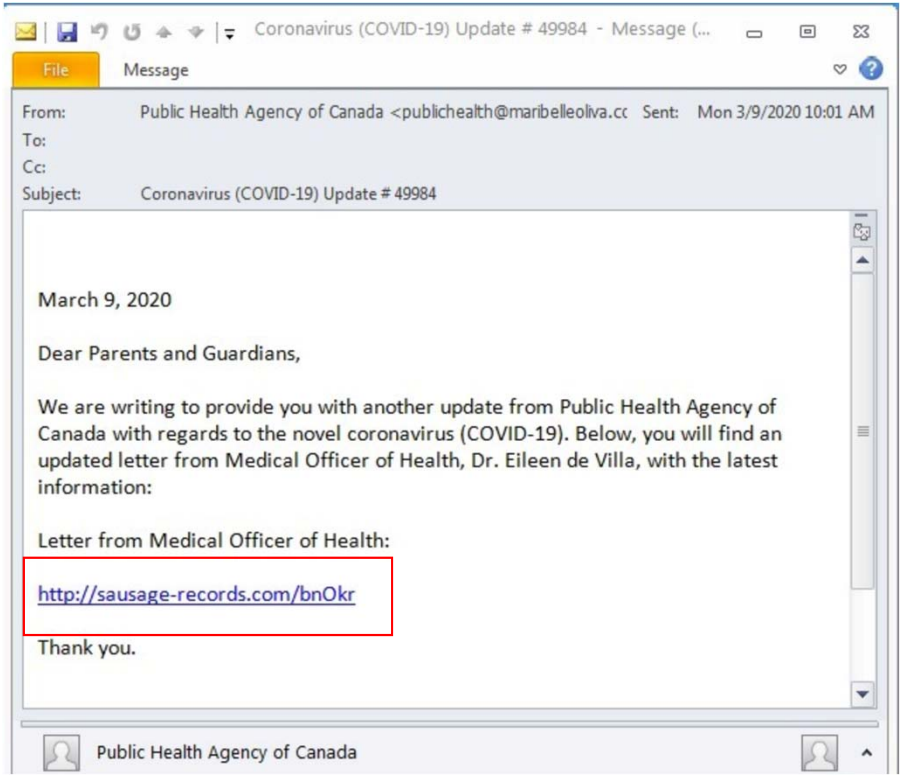
- Post visual reminders (posters, etc.) throughout office space
  - Internal media campaigns provide a reminder of the importance of employee awareness
  - Post reminders in offices, cubicles, shared space (kitchen, conference rooms, etc.)
  - Tailor web-based modules customized to individual groups pertinent to their roles and how they may be specifically targeted so employees can better spot and avoid tactics that may be used against them.

https://www.biola.edu/information-technology/information-security/dont-be-manipulated-by-social-engineering

faegre drinker

Social Engineering Prevention (Awareness)

- Send regular email reminders on vigilance against social engineer attacks
  - Send management and HR email coordinated campaigns to staff to maintain awareness
  - Develop comprehensive training that includes, and goes beyond, phishing and spear phishing; include other social engineering concerns that involve physical security, industry best practices against device loss, insider threat indicators, etc.

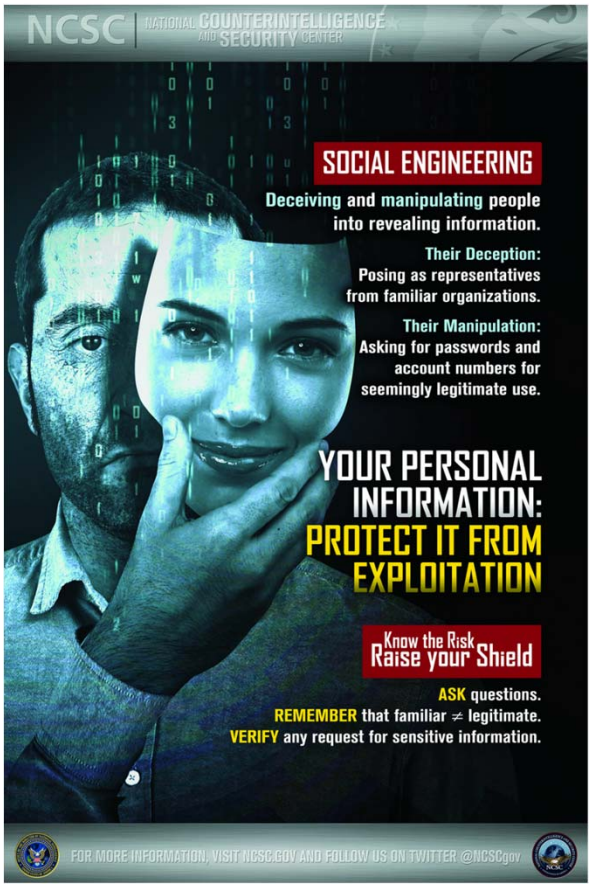


https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

faegre drinker

Social Engineering Prevention (Awareness)

- Publicly reward staff who embody good security awareness
  - Provide incentives (gift certificates, etc.) for staff who identify a social engineering attack and notify management
  - Identify staff who have been vigilant against social engineering attacks and highlight their examples during all-hands/staff meetings



https://www.dni.gov/files/NCSC/documents/campaign/Poster_Social-Engineering_6April2017_FINAL.jpg

faegre drinker


QUESTIONS