CNA

Identify and Reduce Social Engineering Attacks

Construction Industry

MCAA
Mechanical Contractors Association of America
MSCA PCA NCPWB MCAA JRGF

Legal Disclaimer

One or more of the CNA companies provide the products and/or services described. The information is intended to present a general overview for illustrative purposes only. It is not intended to constitute a binding contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.

Foundational Series

This course is a part of the Risk Control foundational series.

Introduction

The median number of
days that attackers stay dormant within a network before detection

Cybercrime global damage costs to hit $6 trillion annually by 2021

Cyber black market “more profitable than drug trade”

Symantec data reveals that one out of every 39 construction industry email users gets targeted by phishing.

Source: swimlane.com, darkreading.com, telegraph.co.uk, securitymagazine.com, cnbc.com, ENR.com

Objectives

- Identify clues used in Social Engineering email attacks
- Identify clues used in Social Engineering phone and text scams
- Identify risk mitigation controls to address

Current Cybersecurity Landscape

CNA

Social Engineering / Phishing

“Psychological manipulation of people into performing actions or divulging confidential information”

- **Baiting with “free” stuff**
- **Exploiting human nature’s desire to help**

CNA

What is Phishing Attack?

- A form of social engineering.
- Use email or malicious websites to solicit personal information by posing as a trustworthy organization.
- May also appear to come from other types of organizations, such as charities or business clients.
- Attackers often take advantage of current events and certain times of the year, such as:
- Natural disasters
- Epidemics and health scares
- Economic concerns
- Major political elections
- Holidays

Identify a Phishing Attack

- Asks you to verify account or order information through a link in the email. Asks you to call a phone number.
- Requests account and/or order information.
- Contains unsolicited attachments including images, files and documents.
- Uses an IP address (string of numbers) in the header or body of the email communications, e.g. http://123.456.789.123/aicpa
- Asks for personal information, including your username and password, Social Security Number, Tax ID number, financial records, bank account numbers, debit or credit card numbers or security codes, etc.
- May ask you to copy and paste website URLs into your browser.
- May misspell your personal information, such as your name.
- Appears to be from an official organization.
- Tone conveys a sense of urgency.

Business Email Compromise

Cyber-Enabled Financial Fraud on the Rise Globally

Step 1: Identify a Target	Step 2: Grooming	Step 3: Exchange of Info	Step 4: Wire Transfer
			
Organized crime groups target businesses, using online information to develop a profile on the company and its executives.	Spear phishing emails or calls target company officials. Perpetrators persuade, pressure, manipulate and exploit.	Victim is convinced they are conducting a legitimate transaction. The unwitting victim is then provided wiring instructions.	Upon transfer, the funds are steered to a bank account controlled by the Organized crime group .

Business Email Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

CNA

Source: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Ransomware

Type of malware that restricts access to the infected computer system and demands that the user pay a ransom to remove the restriction. Some forms of ransomware encrypts files which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.

Phone/text Scams

CNA

Identify a Phone/Text Attack

- Direct approach: an aggressor may directly ask a target individual to complete a task
- Important user: by pretending to be a senior manager of an organization with an important deadline, the aggressor could pressure the employee
- Helpless user: an aggressor may pretend to be a user who requires assistance
- Technical support personnel
- Sense of urgency
- The caller or text offers free prizes, coupons, unbelievable deals, health cures

The caller or text may note

- Notice of suspicious activity on your account
- Claim there's a problem with your payment information
- Send you a fake invoice
- Send fake package status or delivery notice with a link to click on

Mitigation Controls

Controls for Phishing Attacks

- Be especially cautious and suspicious in unsolicited emails.
- Even if the sender looks legitimate use care before clicking on links or attachments. When in doubt utilize “out of band verification”, call the sender using a known good phone number to verify the email authenticity.
- Phishing scams may include misspellings in names or websites.
- The URL listed may use a different extension. Example .net instead of the known .com
- Phishing scams ask for personal information as some type of verification.
- Beware a tone that coveys a sense of urgency.

Controls for a Phone/Text Attack

- Beware a tone of urgency
- If the caller states they are a senior manager you should still seek verification.
- Do not provide sensitive details by phone/text.
- Government agencies and financial institutions will never call you to ask for sensitive information.
- Don’t click on an unsolicited link in a text.
- Beware of readily replying STOP to an unsolicited text
- Report suspicious messages to your carrier.
- Use your cell phone’s blocking tool.
- File a complaint with FCC
- Don’t readily believe your caller ID
- Never agree to pay up front for any prize or gift.
- Simply hang-up on robo calls
- Sign up for free scam alerts from the FTC at ftc.gov/scams.

The Construction Industry

Construction Industry

Construction
General Contractors, trades, management

Types of Attacks
Phishing, Spearphishing, Wire transfers, Ransomware, Hack of IoT, Vehicle telematics,

Key considerations
Employee use policies training, monitoring and access privilege management, MFA,

Incident response plan – integrated into business continuity/DR plan, including tested data backup and recovery

Data encryption – desktops, laptops, portable devices and removable media

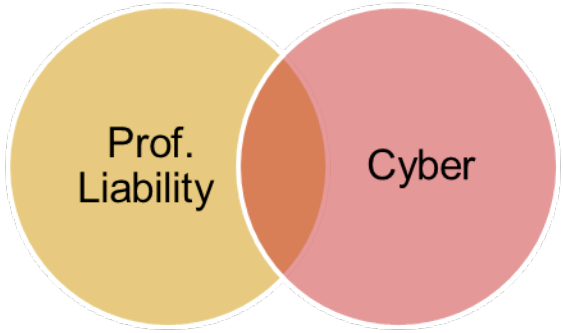
Vendor and Third Party – Legal review of representations about cyber security practices.

Data Breach
Network Interruption
Reputational Harm

Data Breach
- PHI
- PII
- Payment info
- Proprietary plans and designs

Network Interruption
- Business Interruption, Professional Liability

Improper Data Collection/Use
- Regulations– HIPPA, CCPA, sensitive business records



CNA

Best In Class Controls

- Full disk encryption on all laptops, desktops, mobile devices, and external storage
- Segmentation of network
- Controls extending to embedded devices
- Careful with unsupported operating systems
- Documented and tested DR/BC and Incident Response plans
- Formal Data Retention Policy – including secure deletion of data
- Multi-Factor authentication
- Physical Security
- Robust Cloud/Vendor management system
- Security awareness training
- Understanding the additional controls necessary for PCI and HIPAA
- Conducting annual penetration tests, and remediating issues
- Mobile Device Management (MDM) for smartphones, tablets, and BYOD (bring you own device)
- Password Management – Policies/Enforcement

CNA

As applicable.

Course Summary

Congratulations on completing this class!

Now that you've reached the end, you should be able to:

1. Identify clues in recognizing Social Engineering email attacks
2. Identify clues used in Social Engineering phone and text scams
3. Implement risk mitigation controls to address an attack

CNA

Thank You!

Upcoming MCAA COVID-19 Contingency Plan Webinars:

Webinar #16: **Calculating Impacts: How to Apply the Measured Mile Method**
Tuesday, May 26

Webinar #17: **Legal Issues Concerning COVID-19 Employee Screening**
Thursday, May 28

Webinar #18: **Learn How to Influence Your Workers to Willingly COMPLY with COVID-19 Protections**
Thursday, June 4

Webinar #19: **Virtual Communication Skills**
Thursday, June 11

REGISTER TODAY AT: MCAA.ORG/EVENTS/