Phishing Email Exercise:

Introduction:

The objective of this assignment is to help students understand how phishing attacks work and how to prevent them. Phishing is a type of cyber-attack where an attacker attempts to trick people into revealing sensitive information such as login credentials, credit card numbers, or personal details. This is typically done through a deceptive email or message that appears to be from a trustworthy source, such as a bank, social media platform, or government agency. Phishing attacks can also contain links to malicious websites that can infect your computer system/network with other malware such as ransomware. The manufacturing industry was heavily targeted by spear phishing attacks. Therefore, it's crucial for workers to learn to recognize and report phishing incidents.

The Scenario:

In this exercise, you will be performing a phishing attack on a fictional company, Mindful Manufacturing. Cybercriminals will use information that is open to the public, commonly called Open-Source Intelligence (OSINT), to create convincing phishing emails that trick victims into divulging sensitive information or taking actions that could compromise their security. Utilize the OSINT below to create your phishing attack:

Background: Mindful Manufacturing is a leading provider of manufacturing/machining services. They specialize in the design and production of precision parts for the automotive and aerospace industries. With such a strong reputation for quality and innovation, Mindful Manufacturing has become a prime target for cybercriminals to steal valuable data and intellectual property. As workers in the machining industry, it is your responsibility to be aware of these kinds of attacks.

Employee Information:

- John Smith **CEO**: Oversees the overall management and strategic direction of the company. Sets goals, develops business plans, and manages the financial performance.
- Sarah Johnson **Production Manager**: Manages the day-to-day operation of the production floor, including scheduling, production planning, and quality control.
- Tyrese Ortiz **Sales Manager**: Leads the sales team, develops sales strategies, and manages customer relationships.
- Erin Donaldson **Machine Operator**: Operates CNC machines and other machining equipment to produce precision parts.
- Jayson Caldwell **Machine Technician**: Conducts preventative maintenance on equipment, repairs equipment as needed, and ensures that all machines are functioning properly.
- Ben Lee **Administrative Assistant**: Provides administrative support to the management team, including scheduling, meetings, maintaining files, and responding to customer information inquires.

The Phishing:

Here are some methods that cyber attackers use to create successful phishing attacks. Use these techniques to create your own phishing attack, specific to Mindful Manufacturing.

Authority:

- Pretending to be a high-ranking official, such as a CEO or department chair, and requesting an urgent action, like a money transfer or gift card purchase, can make the recipient feel obligated to comply.
- Falsely claiming to be from a court or law enforcement agency and stating there's a warrant for the recipient's arrest can create a sense of urgency and fear.

Likability:

- Creating a sense of familiarity or likeability can make people more inclined to help or comply with requests.
- Using a crying baby in the background of a call or asking for a password reset for an employee on maternity leave can create an emotional appeal and make them more likely to help.

Urgency and Scarcity:

- Creating a sense of urgency by implying that time is limited, or that there are limited quantities of something, can make people act quickly without thinking things through.
- Falsely claiming that an account will be closed or that a deal will expire soon can create a sense of urgency.

Commitment and Consistency:

- People value consistency and are more likely to comply with requests if they have previously committed to something similar.
- Pretending to be a follow-up to a previous conversation or email can create a sense of consistency and make the recipient more likely to comply.

Social Proof:

- People are more likely to act if they see others doing the same thing.
- Implying that an action is normal, appropriate, or of status, and that many others are already doing it, can create a sense of social proof and make the recipient more likely to comply.

Reciprocity:

- People feel obliged to help someone who has helped them in the past.
- Pretending to offer a reward or benefit in exchange for information or actions can create a sense of reciprocity and make the recipient more likely to comply.

Prevention Strategies:

Now that you have learned about the various methods used to conduct phishing attacks and have even created your own, it's time to shift our focus to identifying these attacks. By being able to recognize the signs of a phishing attempt, you can better protect yourself and your organization from potential cyber threats. Let's explore some useful strategies for detecting phishing attacks.

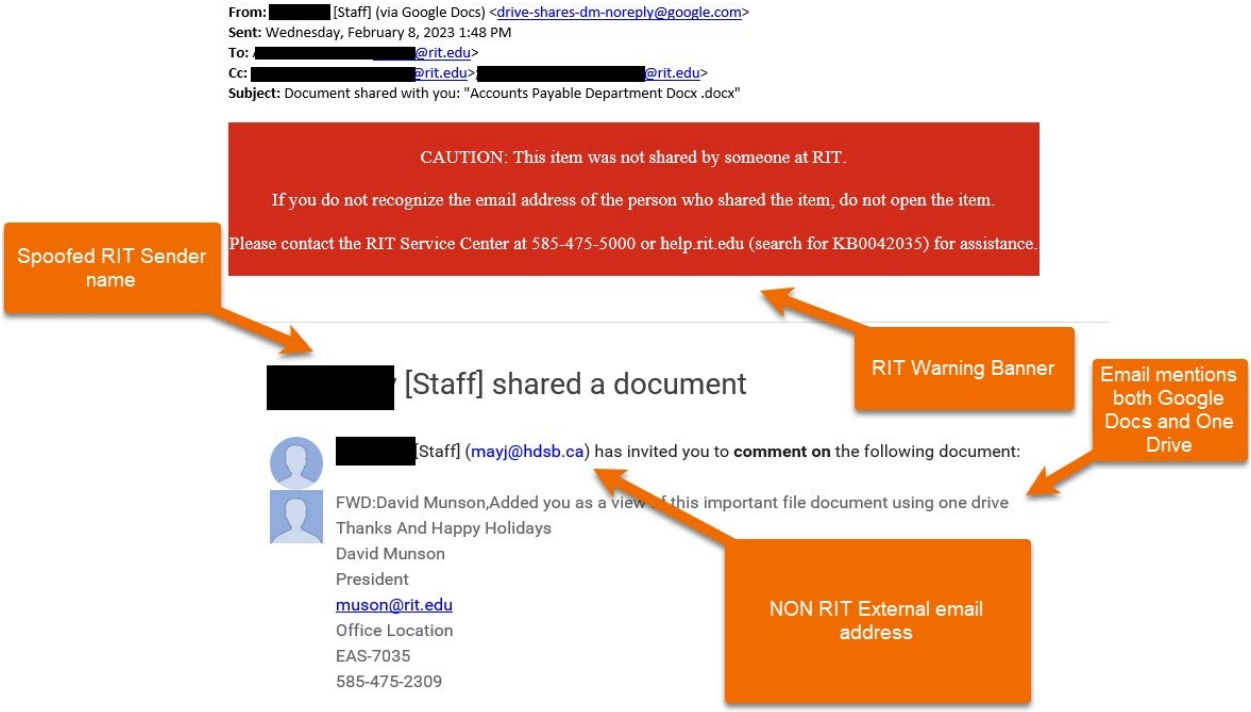
What to look for:

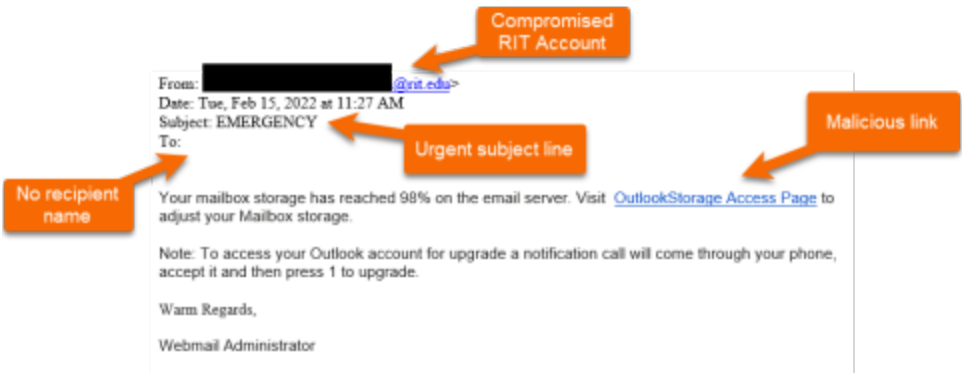
- **Sender**: Verify the email sender's identity. If you don't recognize the sender or the reply address seems unfamiliar or unusual, the email could be a phishing attempt.
- **Links:** Check for suspicious links in the email. Hover over the link before clicking to identify the web address.
- **Attachments:** An unexpected email that includes an attachment is a red flag.
- **Emotion:** Phishing emails often utilize urgency or fear to pressure the victim into clicking on a link or completing a task that benefits the sender.
- **Data:** Phishing scams may aim to obtain personal information, such as passwords or social security numbers. It's important to never disclose such information.

In the smart manufacturing industry, links and attachments are common vectors for malware, such as ransomware and information-stealing Trojans. These types of attacks can result in significant damage, including data loss, financial losses, and disruptions to production. Malware can be embedded in seemingly harmless links or attachments, making it challenging to detect.

Examples:

These examples demonstrate real-life phishing attacks that have targeted the Rochester Institute of Technology, and similar emails may be encountered by anyone. It's important to remain vigilant and apply the strategies for identifying phishing attacks that were discussed earlier.





What to do if you suspect you received a phishing email:

- Never respond with any personal information.
- Do not click any links or open any attachments.
- Change your account password if you feel as though your password has been compromised.
- Back up your data on a regular basis to limit the impact of a phishing scam.
- Report the email to your IT department.

Wrap-up:

To summarize, this phishing email exercise has equipped students with the knowledge and tools needed to recognize and prevent phishing attacks in the smart manufacturing industry. By being aware of the various techniques that cybercriminals use, such as social engineering and emotional manipulation, workers can protect themselves and their organizations from potential cyber threats. It's essential to remain vigilant and apply effective cybersecurity measures, such as verifying the sender's identity, checking for suspicious links and attachments, and avoiding disclosing personal information. By staying informed and adopting good cybersecurity practices, we can create a safer digital landscape for all.

Resources:

Phishing. RIT. (n.d.). Retrieved February 27, 2023, from https://www.rit.edu/security/phishing.

Rit Phish bowl. RIT. (n.d.). Retrieved February 27, 2023, from https://www.rit.edu/security/rit-phish-bowl.

“Practical Social Engineering.” Joe Gray. No Starch Press, Inc. 2022. Accessed via RIT Library subscription to O’Reilly.