INSIDER THREATS

A review of the latest security threats and how you can avoid them

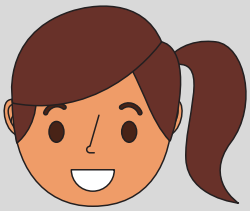
THIS MONTH'S TOPICS:

You've been sharpening your skills towards spotting phishing emails, scam calls, and improving your password security. All fantastic measures to help keep external bad actors at bay. However, these security protections may not be able to stop the threats from within which can be harder to spot and deliver a more dangerous end result.

Insider threats revolve around an employee's careless behavior or intentional disregard for company policies and procedures. Because of our access to sensitive information, we must never abuse our privileges and share that information with unauthorized individuals. Failure to abide by these rules could result in serious consequences to the organization and yourself.

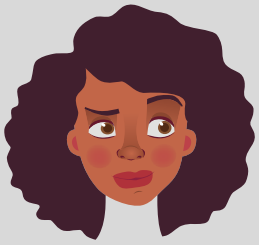
Insider Threats Come in Various Forms

Let's look at some examples of the possible threat actors you could see within your organization.



Name: Careless Carrie
Subgroup: Pawn
Description: Careless Carrie may be a hardworking employee with no ill-will towards her job or employer. With one simple mistake or lapse in judgment, Carrie could be opening her organization up to a breach.

Name: Danny the Double-Agent
Subgroup: Turncloak
Description: Danny the Double-Agent may have started out as a model employee, but his morals have shifted recently. Danny was approached by an external party with malicious intentions. Using his access privileges, Danny is feeding sensitive information to his malicious pal, who carries out the evil deed. It's possible that Danny doesn't comprehend the actions he's taking or their severity.



Name: Disgruntled Debbie
Subgroup: Turncloak
Description: Disgruntled Debbie is not a happy camper. She may be feeling slighted by her organization over a missed promotion, termination, or job restructuring. Her spite for being wronged could lead her down a path of willful neglect of sensitive information such as sharing company secrets, leaking sensitive data, or other acts of revenge.

Name: Malicious Michael
Subgroup: Turncloak
Description: Malicious Michael is using his access privileges for his own gain. Michael knows the actions he is committing are wrong, but he continues thinking he won't get caught.

While we can't always be perfect, it is important to strive to protect the information we have access to to the best of our ability.

Insider Threats: What's the Harm?

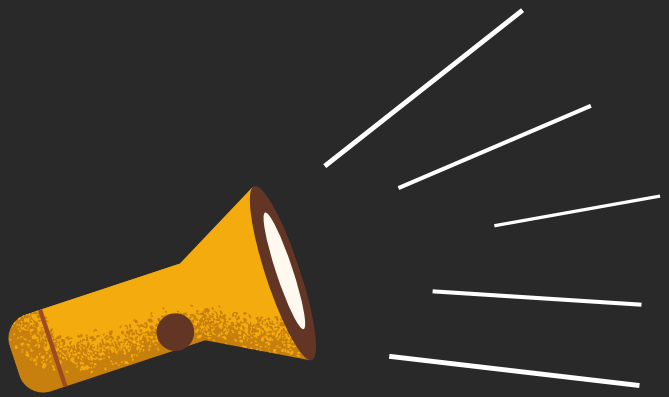
Some may think this type of activity is a victimless crime. Quite the contrary!

Identity Theft:
The unauthorized access of information brought about by an employee's abuse of their privileges could result in identity theft issues for those whose information was exposed.

Company Sabotage:
Sabotaging projects or selling/sharing company secrets can be damaging to the company and its employees. Leaked information could lead to reputation damage and a loss of business or investments. Major hits will result in employee layoffs.

If you do suspect or have knowledge of a co-worker's malicious intentions, do not keep it to yourself! Staying silent allows the activity to continue, resulting in damages. However, do not confront the individual on your own. Instead, reach out to your supervisor who can handle the situation appropriately.

Manager Spotlight: Mitigate the risks early



Tips for Managers

- Ensure you have a documented **termination policy** that is followed promptly after every termination.
- Review any **audit logs** to look for suspicious access by employees. This could be after-hours access or excessive access of data.
- Ensure that minimum **access controls** are in place based on employee job roles and restrict access where possible.

SCAM OF THE MONTH

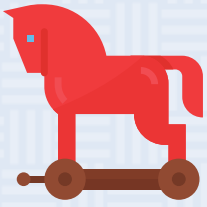
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits. To protect identities, the names have been changed in this scenario.

This month's submission comes from "Charles" who's curiosity got the best of him. Charles was walking into work one morning when he spotted a USB drive on the ground near the building entrance. On the back, the word "Important" was etched in Sharpie. He looked around to see if anyone was coming back for it, then picked it up and walked inside to his desk. His intentions were pure, he was just going to plug in the device and check out a file or two so he could pinpoint who it belonged to. After opening his first file, Charles received a ransomware notice and the rest was history.

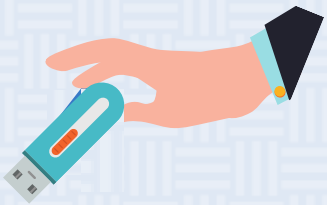
Did you spot the red flags?

- The USB drive was planted by a scammer who felt confident it would spark someone's interest and be utilized.
- The "Important" text on the back of the drive was an extra measure to help guarantee success.
- The malicious files can be placed within a file on the USB drive disguised as something innocuous.

USB drops, as they are commonly called, are becoming a popular trick among scammers. USB drives are cheap to purchase, and the malware installed on the drive is not difficult to initiate.



Think of the USB drives as a Trojan horse. By masquerading as a common object with value, there is a greater chance that it will be picked up and brought inside where it can initiate its attack. These scams do not just happen at work. They can be initiated in any public location such as a mall, park, school, or any area where there is a large amount of public foot traffic.



If you do spot a USB drive, pick it up! Though that might seem contrary to what you are learning, picking up the USB drive is the correct action. The issues come after it is picked up. If you do find and pick up a USB drive, do not plug it into your device, instead, hand it to your supervisor or IT. Leaving a device like this lay makes it available for the next victim who may cause an issue.

KEEPING OUR OFFICE SAFE

Key Takeaways

We've become well versed at spotting the external threats, but the threats from within the office can be just as damaging.

Always strive to try your best and follow company policies and procedures. If you do make a mistake, let your supervisor or IT know immediately.

Malicious access to information will be damaging to the company as well as to the individuals whose information was inappropriately used.

Keep your curiosity in check if you spot a suspicious USB drive. Pick it up but don't plug it in - hand it over to your supervisor or IT to take care of it properly.

Remember, if you do detect suspicious behavior from a co-worker, don't stay silent. Discuss your concerns with your supervisor and IT.

Cybersecurity Anagrams! - Some key words have been scrambled below. How many can you get without cheating?!

1. Bed Virus: ___ _____
2. Hairnets Tired: _____ _____
3. Boats Age: _____
4. Remain It Not: _____
5. Beagle Donut: _____ _____
6. Did Leg Turns: _____
7. Cola Trunk: _____
8. Sales Rec: _____
9. Roaster John: _____ _____

Answers: 1. USB Drive; 2. Insider Threat; 3. Sabotage; 4. Termination; 5. Double Agent; 6. Disgruntled; 7. Turncloak; 8. Careless; 9. Trojan Horse