IT'S A SLIPPERY SLOPE

The perils of cyberscams and how to navigate them

THIS MONTH'S TOPICS:

Green Circle:

So you clicked the link...

Blue Square:

You've been scammed...

Black Diamond:

Scam of the month...

Cyber Zen Den:

Self & Cyber Awareness

Look at you, slaloming through the internet like a pro. If cybersecurity was a Winter Olympic sport, you'd win gold: maneuvering through emails with ease, swerving around phishing attempts.

But what if, one day, there was a little too much zig in your zag, and you tumbled down Scammer's Hill?

Having an "Emergency Game Plan," or an "Oopsie Checklist," not only helps lessen the damage if you ever do fall victim to a scam, but it also paints a greater picture of what it means to be cyber-aware.

The reality is that accidents do happen, and it's your responsibility to be prepared when it comes time to take action.

So you clicked the link...

You knew you shouldn't have the moment you did...

Now what do you do next?

1. Do not enter any PII, or login details.
2. If on a work device, inform IT right away and await further instructions. If on a personal device, immediately disconnect from the internet.
3. If on your personal device, run an anti-malware scan.
4. For safe measure, change your credentials, and backup your files on your personal device. Request best practice from IT for work devices.

FINISH

Learn from this moment. Reflect on where you went wrong, and take precautions to prevent making the same mistake in the future.

GREEN CIRCLE

TODAY'S CYBERSECURITY CONDITIONS: - You've been scammed!

As of 4:38pm EST

-1,100 $

High chance of worry and panic:

- Scams fallen for on work devices should be reported to IT to help improve conditions.
- Take the following precautions on personal devices immediately to improve expected delays.

- Update your passwords.
- Notify credit agencies and credit card companies (if this information was exposed) to inform them of the potential account compromise.

- Update software and run a virus scan if concerned of infection.
- Encrypt sensitive files and back up important documents.

- Regularly check accounts for suspicious activity.
- Set fraud alerts or credit freezes if deemed necessary.
- Consider reporting scam to local internet crime centers.

Becoming a victim might lead to a temporary rainy season, but bright skies can still lay ahead.

Improve your security standing and learn from any previous missteps.

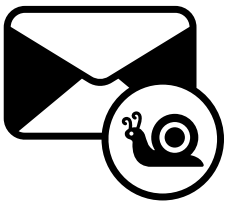
SCAM OF THE MONTH

Each month we highlight a REAL scam that demonstrates tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

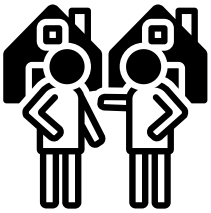
One frosty morning, Lewis received a letter stamped "urgent" which he thought was a late bill.
Upon opening the letter, he read a very polite, well written note explaining that he "had been caught in the secret he's been keeping from his wife." The writer claimed to "have evidence of what's been hidden" and threatened to send that evidence to Lewis' family and friends if he did not pay the "$15,500 in Bitcoin within 24 hours, as a confidentiality fee, to the following address..." Lewis felt unsettled as he threw the note away. He did not have a wife, nor any nefarious secrets, and he was shocked that it was possible to receive a scam through snail mail at his home address. Later that day, when speaking to his neighbors, he learned that they too received the same scam letter in the mail, along with many other men in the area.

Did you spot the red flags?

- Lewis' letter was intimidating, and used high-pressure tactics such as threats and time constraints, similar to what might be found within an email phishing scam.
- The letter also consisted of Bitcoin Blackmail as a means of extortion.
- Lewis later learned that he was actually one of many involved in this demographically targeted attack.



Snail Mail scams may be less common than other technologically advanced Phishing attempts, but they do still happen. If you receive blackmail or scam-based letters in the mail, report it to your local postal inspection services.



Lewis conversed with his neighbors, and ended up learning more about the scam, but you can also search the web for one or two sentences in a letter you think is suspicious to confirm if it is actually a scam.

With Snail Mail scams, though your name and address were likely found through public records, for additional peace of mind, you can always double check for recent data breaches that may have compromised your information.

Key Takeaways

There are a lot of scams out there, and part of being cyber-aware consists of knowing what steps to take in the event that you do, one day, accidentally fall for one.

Similar to any other emergency plan, it's important to take the time to think through what you should do in such a situation to protect yourself and your PII.

For work devices: accidentally interacting with a scam should immediately be brought to the attention of your IT department, as time may be of the essence.

For personal devices: Depending on the type of scam you may have interacted with, and in what capacity, it may be beneficial to run an anti-virus scan, and update passwords.

After the dust has settled: Continue to keep an eye on your accounts to quickly catch any residual suspicious activity.

Self-awareness

Being self-aware is the conscious knowledge of one's own character.

How does this relate to cybersecurity?

Greater self-awareness can play off of and enhance a greater cyber-awareness. By knowing yourself on a deeper level, you are attuned to your strengths and weaknesses. You can then evaluate these characteristics objectively, and change course if necessary.

Now apply this concept to cyber-awareness.

What are your strengths and weaknesses when it comes to cybersecurity? Do you have strong passwords, and utilize a password manager? Do you have an "emergency" game plan if you were to click on a scam link? Consider your current cybersecurity standing objectively, and make any necessary adjustments before it's too late.