A SCAMMER'S TOOLKIT

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

THIS MONTH'S TOPICS:

Spoofing - pg. 2

Keyloggers - pg. 3

Brute Force Attacks - pg. 3

Scam of the Month - pg.4

Building your Own Toolkit - pg. 5

We all face many challenges and tough decisions on a daily basis. For a cybercriminal or professional scammer, that tough decision is which trick are they going to use to try to rope in their next victim. With a myriad of available tools, these possible options and techniques are seemingly endless and evolve each day.

While intimidating, there are multiple ways we can protect ourselves. Understanding the tricks and tools of a scammer's trade will help you see into the mind of a scammer, which can better prepare you for when you are met with their challenge.

But just remember, for every tool a scammer has to try to trick you, you have one to protect yourself.

Spoofing

A popular tool used by many scammers is spoofing. Spoofing scams come in many different forms, but the most common ones are email spoofing, caller-id spoofing and website spoofing. **The goal?** Provide a false sense of security by impersonating someone or something else to trick you into providing confidential information.

Many of the tools required for perfecting these scams are easy to obtain and master, making them the perfect entry-level campaign for a cybercriminal.

Email spoofing is common in phishing emails. Scammers will take a well-known email address and adjust a letter or two, hoping you miss it. Example: billing@nationalbrank.com.

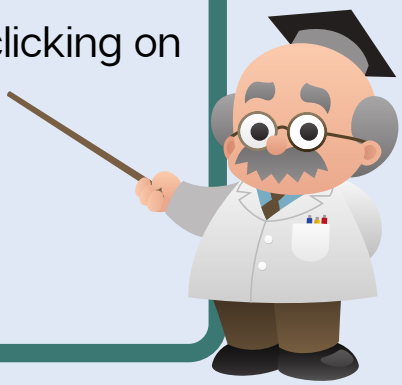
Caller-ID spoofing is when scammers manipulate the phone number they are calling from. By using a verified legitimate business phone number or a similar number to your own, the likelihood of you picking up the call increases dramatically.

Website spoofing is a scammer's way of getting you to think you are at a trusted website. By mimicking the look and feel of a real website, you are more likely to provide login credentials or sensitive information.

Key Takeaways

There is no magic tool that we can implement to stop these scams from happening, BUT the best defense is to stay attentive on all levels.

- Avoid answering calls from unknown numbers unless you absolutely have to
- Double-check email addresses before responding, clicking on a link or opening an attachment
- Carefully inspect the website domain before you click on a link provided in an email
- If you think you've fallen victim to a spoofing scam, contact your supervisor and IT immediately



KEYLOGGERS

A keylogger is a type of spyware that can **record and steal data** that is typed into a device. It's like having someone standing behind you and watching what you're typing. They can record your passwords and credit card data, view emails you send and record the web pages you access.

Keyloggers can only infect your device if you let it. This type of spyware will only work if you download/install it so scammers need to be creative to get you to take the bait. This could be through a phishing email directing you to open an attachment or through a phone scam where the scammer pretends to be helping you troubleshoot a technical issue or remove a virus.

The challenge with keyloggers is that they operate in the background, and you may not even know they are there, silently stealing your information. Take extra precautions when downloading files or programs and don't fall for tech-support scams.

BRUTE FORCE ATTACKS

Brute Force Attacks are automated computer programs that try to crack your username and password. Using a simple program, a barrage of credential combinations are fired in an attempt to break into your accounts. The more powerful the computer, the faster they reach their goal. Typically these attacks are broken into two categories.

ONLINE ATTACKS

An online attack is centered around a site's primary login page. Using their tools, scammers can try thousands of credential combinations per second in an attempt to break-in. Without intervention or account lockout, they will eventually break-in.

OFFLINE ATTACKS

Offline Brute Force Attacks are much faster because they aren't waiting for the response of a login page. Using password storage files that had been compromised previously by the hacker, a wealth of opportunities are available. The files they've stolen would not have the passwords stored in plain text and ready to use, but using different brute force attacks, the attacker can guess password combinations at a rapid rate, undetected.

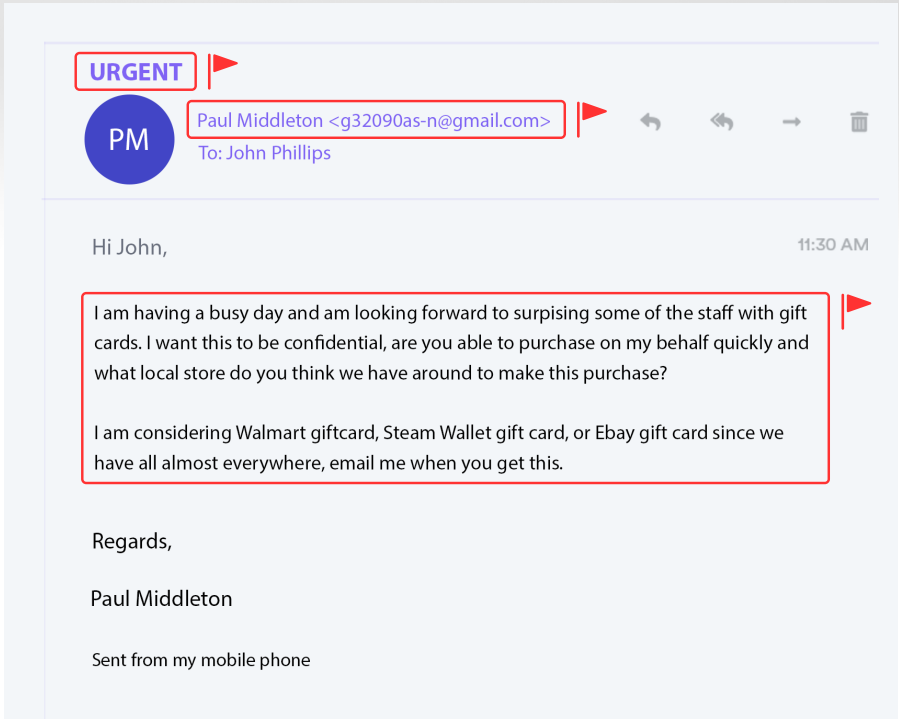
SCAM OF THE MONTH

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 *your* inbox.

This month's submission comes from "John." John received an email with an urgent request from his boss, "Paul" - or so he was meant to believe. To protect identities, the names have been changed in this scenario.

Did you spot the red flags?

- The "**Urgent**" subject line should be a red flag! Scams often invoke a sense of urgency to get you to respond or do what they're asking of you - quickly.
- The full name of John's boss appears next to the email address. This **name was spoofed,** knowing John had a better chance of responding to his superior.
- The email is asking John to purchase **gift cards** and respond. Purchasing gift cards is a common request in scams due to their lack of traceability and widespread availability. Be cautious of emails requesting anything monetary.



This is a perfect example of a **BEC (Business Email Compromise) scam**. The scammer must have done their homework to know the primary contact names at this organization. With some easy-to-find information online or through social media accounts, they were able to piece together a low risk, high reward scam that looks awfully convincing!

The email seems innocent, with no threats or preposterous lottery winning claims. John's "boss" is asking him to purchase some gift cards for the staff. Sweet! But this is becoming a **common request by scammers**. By requesting gift cards, the scammer is hoping to fly under the radar more than if they were asking for bitcoin or to transfer funds into a new account.

John took the correct action by not replying to the email, but rather **sent a new direct email** to his boss. He confirmed this was not his doing and they informed the rest of the staff to be on the lookout for future scam attempts by this scammer.

KEEP YOUR OWN SECURITY TOOLKIT STOCKED

While it may seem like we are outmatched when it comes to stopping a cybercriminal, in reality, there are many simple practices that we can follow to keep our information safe.

Key Takeaways

Keep your cybersecurity toolkit stocked and apply these best practices wherever possible to make spotting cybercrime second nature.

Use common sense - trust your instincts when something suspicious occurs. If something seems awry, it probably is. Most times, our brainpower is our best protection.

Use longer and more complex passwords - The longer and more complex your password is, the harder it will be to crack. Even adding one extra character can add days of extra cracking time for a cybercriminal. Passphrases are also a great option for creating strong, unique passwords. Consider setting up a password manager to make these passwords more complex and unique.

Enable two-factor authentication and/or account lockout - Account lockout will help prevent the online brute force attacks by limiting a cybercriminal's attempts. Two-factor authentication will force an extra credential when trying to log in, so even if your password is compromised, the culprit isn't able to circumvent the second layer.

Ensure Anti-malware and Anti-virus protections are turned on - To help stem the effects of a keylogger and other malware and spyware, make sure that you have the proper security protections for your devices and that these tools are up to date.

Cybercrime Word Search

Complete this week's activity and find the keywords from this month's newsletter in the word search below!

BRUTEFORCE
CALLERID
CYBERCRIMINAL
TOOLKIT
INSTALL
KEYLOGGER
OFFLINE
PASSWORD
PHISHING
SECURITY
SPOOF
SPYWARE

E C R O F E T U R B D R C F I
R L S Y R B M I N R Z Y W N Z
H E P E N U U O O I B R S L V
C U G G C J W W M E I T V M D
X P T G F U S S R L A F S X I
X D D G O S R C C L A O A T R
E C H X A L R I L H T O K O E
W Z B P P I Y E T F H P B O L
Z D U M M M N E R Y A S T L L
W A S I F F F T K A L U C K A
T E N I L F F O Y C W V R I C
A A I U Y Z U Y J I T Y C T Z
L P H I S H I N G R Q X P I L
G V S A I H J G N I R Z G S I
F B H Y M G C M C X V K J L I