Pegasus Protects- May 2024 Imposter Scams

This month we will focus on a few different types of imposter scams where fraudsters use deceptive tactics in order to obtain sensitive information for a monetary purpose.

Imposter Scams:

Imposter scams usually involve someone *supposedly* spotting fraud or criminal activity on one of your accounts, and they are offering to help "protect" your money. During this conversation they may ask you to share verification codes, as well as always telling you to move money from your bank, investment, or retirement account to a "safer" place. The fraudster will prey on the victim's trust and feign urgency to gain the information they want.

These scams often involve impersonating government agencies, tech support, or financial institutions. Whether it is an email, phone call, or even a knock at the door, always verify the legitimacy of the request before sharing any sensitive information or making payments. Remember, legitimate organizations will never pressure you into immediate action or ask for personal details over unsolicited communication channels.

Some key tips to remember are:

- Never move or transfer your money to "protect it."
- Anyone who asks you for the account verification code is a scammer. Do not share this.
- If they tell you to not tell anyone or that it is a secret, it is a scam.

Phishing

Phishing is a prevalent form of cybercrime where attackers use fraudulent emails, messages or websites to trick individuals into revealing sensitive information such as passwords, credit card numbers or social security numbers. These deceptive communications often appear to be from reputable sources like banks, social media platforms, or online retailers, enticing recipients to click on malicious links or provide personal data.

The fraudster will usually attach a link to the email, message or website to have you click on it. Once you click on that link you're sent to a spoofed website that might look nearly identical to the real thing—like your bank or credit card site—and asked to enter sensitive information like passwords, credit card numbers, banking PINs, etc. These fake websites are used solely to steal your information.

Phishing has evolved and now has several variations that use similar techniques:

- **Vishing** scams happen over the phone, voice email, or VoIP (voice over Internet Protocol) calls.

- **Smishing** scams happen through SMS (text) messages.

- **Pharming** scams happen when malicious code is installed on your computer to redirect you to fake websites.

Some key tips to remember are:

- Stay vigilant against phishing attempts by scrutinizing the sender's email address, checking for spelling errors or unusual requests, and avoiding clicking on suspicious links or attachments.

- Remember to report any suspected phishing attempts to the appropriate authorities or organizations to help protect yourself and others from falling victim to these scams.

- When attempting to log in to your account, use a link that you have verified, and is found on the legitimate website. If you are unsure of its validity contact the company directly.

Spoofing

Spoofing is a deceptive tactic used by scammers to manipulate caller ID, email addresses or websites to appear as if they're from a trusted source. In most cases they will change one letter, symbol, or number, making it look like you are interacting with a trusted source. Whether it's phone spoofing, email spoofing, or website spoofing, these techniques aim to trick individuals into believing they're interacting with a legitimate entity.

Some key tips to remember are:

- Be cautious of unexpected communications requesting sensitive information or urgent action, as spoofing can make it difficult to distinguish between genuine and fraudulent contacts.
- Verify the authenticity of communication channels independently and refrain from sharing personal or financial information unless you're certain of the sender's legitimacy. Best practice is to speak with someone you are familiar with to verify the details.

The FBI has been working diligently to crack down on imposter scams. They have provided the fraud alert below to help report imposter scams.

Reporting

If you suspect you have fallen victim to a type of scam above, report it to the Federal Trade Commission. They compile data as well as attempt to shut down any links, emails and websites reported to them. Report at the link below:

https://reportfraud.ftc.gov/

AT& T customers can report suspicious text messages by forwarding it to 7726 (SPAM). If you are unable to view the number you can forward the message to abuse@att.net

Find out more about reporting to AT&T at this link: https://www.att.com/support/article/my-account/KM1212535/

Verizon customers can report suspicious text messages by forwarding it to 7726 (SPAM).

To find out more about reporting to Verizon click this link: https://www.verizon.com/support/knowledge-base-301493/#:~:text=Verizon%20takes%20our%20customers'%20privacy,or%20receiving%20texts%20to%207726.

T-Mobile customers can report suspicious text messages and callers through T-Mobile Scam Shield.
Find the steps to do that at this link: https://www.t-mobile.com/support/tutorials/device/app/ios/topic/t-mobile-scam-shield/how-to-report-scam-calls/6

(END)

Resources

https://www.fcc.gov/spoofing

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

https://www.ic3.gov/Media/Y2024/PSA240412

https://www.ic3.gov/Content/PDF/IC3-Fraud-Alert.pdf

https://consumer.ftc.gov/consumer-alerts/2024/03/whats-verification-code-and-why-would-someone-ask-me-it

https://consumer.ftc.gov/consumer-alerts/2024/03/never-move-your-money-protect-it-thats-scam

https://consumer.ftc.gov/features/how-avoid-imposter-scams

https://consumer.ftc.gov/consumer-alerts/2024/03/sure-ways-spot-scammer

https://consumer.ftc.gov/consumer-alerts/2024/03/will-your-bank-or-investment-fund-stop-transfer-scammer-probably-not

https://consumer.ftc.gov/consumer-alerts/2024/03/new-tech-support-scammers-want-your-life-savings

https://consumer.gov/scams-identity-theft/imposter-scams

https://www.investopedia.com/terms/s/spoofing.asp

https://www.chase.com/digital/resources/privacy-security/security/how-to-spot-scams