CYBER SECURITY

THE BEST GROUP

CYBER SECURITY SOLUTIONS

ADVANCE-FEE FRAUD

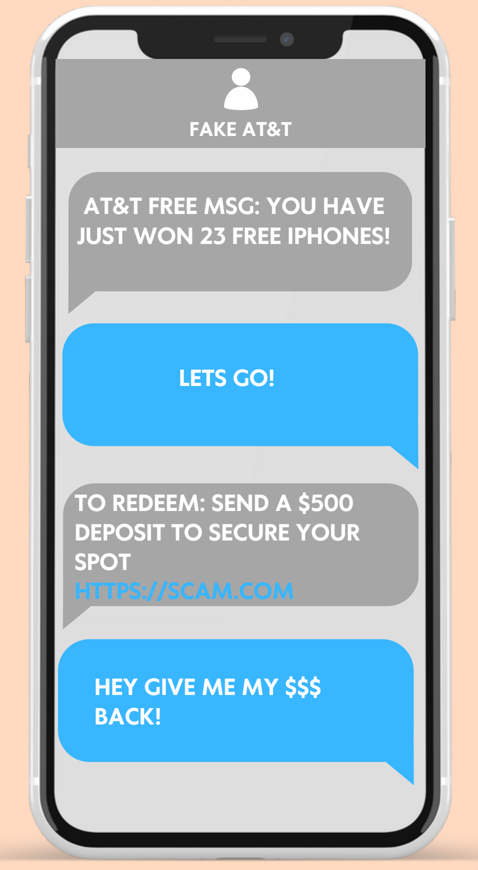
Just received a text/email that is too good to be true?

Don't:

- Click on any link
- Send any money
- Send any information that can be traced back to you

Do:

- Ask questions
- Research and verify before you invest
- Protect your information



FAKE AT&T

AT&T FREE MSG: YOU HAVE JUST WON 23 FREE IPHONES!

LETS GO!

TO REDEEM: SEND A $500 DEPOSIT TO SECURE YOUR SPOT HTTPS://SCAM.COM

HEY GIVE ME MY $$$ BACK!

PHISHING

Scammers are after your: Login Info, Personal information, Card Numbers

Be on the Lookout for:

- Sender you don't know, or weren't expecting an email or call from.
- Urgency in the email asking you to perform an action and/or enter information
- Spelling & Grammar Errors

When in doubt, BE SUSPICIOUS!

- If the email is pretending to be someone you know, try to call and verify the authenticity with the person.
- Always navigate to the related company or institution by searching in your web address to verify legitimacy rather than clicking any links within the email

SPOOFING

What is Spoofing?

- Spoofing is when a scammer falsifies their information to pretend to be someone or something else they are not in order to gain trust, information or advantage.

Examples of Common Spoofs

- Website Spoofing - A website is forged to look legitimate. Ex: faceboook.com
- Email Spoofing - An email is forged to look like legitimate person/entity.. Ex: jeffbezos@amazonn.com
- Caller ID Spoofing - A call is forged to look like it is from an official or your local area.

Prevention Steps:

- Double check links, e-mail, addresses, and numbers.
- Contact the sender/caller elsewhere to verify it is them.
- Turn on spam filter and use a cybersecurity software.

WORMS

What are computer worms?

- Computer worms are self-replicating viruses that often appear in the form of an executable file. Worms are programmed to stay alive for as long as possible on a system and to spread to as many other vulnerable systems as it can. The goal behind these attacks are usually monetarily driven, with worms often attempting to extort money out of users through ransomware tactics.

Prevention Steps:

- Be wary of files sent to you regardless of who the sender is. Computer worms will often take the contact list of infected systems and mass send malicious executables containing the worm in order to replicate itself onto other systems.

HARDWARE ATTACKS

What are Hardware-Based Attacks?

- Attackers can utilize a number of techniques known as "hardware-based attacks" to take advantage of the physical hardware of a computer or system in order to undermine security, steal data, or inflict harm.

Common Methods of Attack:

- USB Drive Malware - USB attacks can exploit existing flaws in the way computers and USB devices interact, famous example being the infamous Stuxnet Worm was spread by USB drives.
- RFID Scanning Attack - Sensitive information from your contactless cards using RFID scanners.

Ways to Protect Yourself:

- Don't plug random USBs.
- Update your device firmware and security.
- Use RFID-blocking wallets or sleeves.

DENIAL-OF-SERVICE (DOS)

What is Denial-Of-Service?

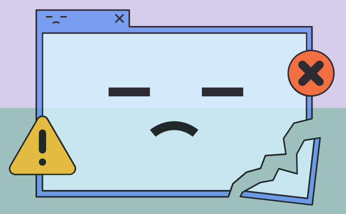
- Denial-of-Service is an attack that prohibits legitimate users from accessing a computer's systems. This is done by the attacker sending a large amount of information or connection requests to that target. These requests overload the system preventing user access.

Most likely to DOS to happen to you is Mail Bombing

- Denial-of-Service attack that overwhelms the receiver's email with large quantities of spam.

Prevention Steps

- Don't give your email out to untrustworthy sites
- Setup automatic junk for unwanted emails
- Block traffic from suspicious or known malicious sources



Questions? Contact Us!

thebestgroup@email.com