PHISHING SCAMS

YOUR DATA PRIVACY IS IMPORTANT!
DON'T GET REELED IN!

WHAT'S A “PHISHING” SCAM?

Phishing scams use voice or electronic messages that appear to be from a legitimate organization you do business with or a person you know. Scammers attempt to gain your trust so you will enter a fraudulent website, share private information, or open an attachment on your phone, tablet or computer.

Clicking on a link or opening an attachment in one of these messages may install malware, like viruses, spyware, or ransomware, on your device. It could also be used to simply steal your password by getting you to type it into a malicious webpage that they control. This is all done behind the scenes, so it is undetectable to the average user. Once the malware has been installed, it could harvest your sensitive information, send out more phishing emails, texts and other message types to contacts in your address book or provide a scammer with remote access to your device. If your credentials are stolen, they can use them to login to your email account or any other services where you used the same username and password.

PROTECT YOURSELF AND/OR YOUR COMPANY

✓ Educate yourself and employees and conduct training sessions with mock phishing scenarios.

✓ Deploy a SPAM filter that detects viruses, blank senders, etc.

✓ Keep all systems current with the latest security patches and updates.

✓ Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.

✓ Develop a security policy that includes but isn’t limited to password expiration and complexity.

✓ Deploy a web filter to block malicious websites.

✓ Encrypt all sensitive company information.

✓ Require encryption for employees that are telecommuting.

✓ Eliminate threats as they evolve. Keep a pulse on the current phishing strategies and confirm security policies and solutions.

✓ Enable two-factor or multi-factor authentication on your account.

HOW TO SPOT A PHISH

VARIOUS PHISHING TECHNIQUES USED BY ATTACKERS

EMAIL PHISHING

The attempt to obtain personal information over email by impersonating a known company vendor or IT department.

WHAT TO LOOK FOR:

- Embedding a link in an email that redirects to an unsecure website that requests sensitive information.
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information.
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information.

“VISHING”

Short for voice phishing. The attempt to obtain personal information over the phone by impersonating a known company vendor or IT department.

WHAT TO LISTEN FOR:

- The use of persuasive tactics “too good to be true”.
- The use of fear tactics “your money is in danger” or “IRS threat“.

“SMISHING”

Short for SMS (Short Message Service) phishing. The attempt to obtain personal information over SMS messaging by impersonating a known company vendor or IT department.

WHAT TO LOOK FOR:

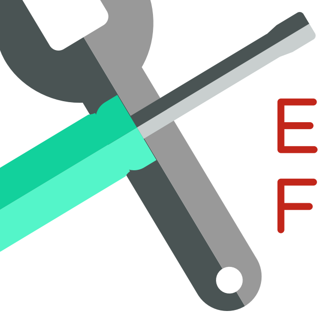
- Spoofed website spellings and gramatical errors.
- Unknown phone numbers. For example “5000” or other non cell numbers can be used by scammers using email to text services.

SOCIAL MEDIA PHISHING

The attempt to obtain personal information over social media by impersonating a known company vendor or IT department.

WHAT TO LOOK FOR:

- Messages from replica friend accounts saying that a friend’s account has been re-created or offers links to requests for personal information entry.
- Bogus posts linking to requests for personal information entry.



ELECTRONIC DEVICE RECOVERY FOLLOWING A PHISHING ATTACK

DISCONNECT YOUR DEVICE

The first thing you need to do is immediately disconnect the device from the Internet.

If you are connected through Wi-Fi, you should locate your Wi-Fi settings on your device and disconnect from the current network. If you cannot locate your Wi-Fi network settings on your device, then go to your Wi-Fi router and shut it off.

WHY? This will reduce the risk of malware spreading to other devices on your network, prevent the malware from sending out sensitive information from your device, and keep someone from remotely accessing your device.

BACKUP YOUR FILES

Now that you are disconnected from the Internet, you should backup your files. If you regularly backup your files using methods like an external hard drive, USB thumb drive or cloud storage, then you may only need to backup files that have been updated or created since the last backup. Focus on protecting particularly sensitive documents and information as well as irreplaceable files like family photos.

WHY? Data can be destroyed or erased in the process of recovering from a phishing attack.

SCAN YOUR SYSTEM FOR MALWARE

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware.

Whom you choose to carry out the next few steps depends on your level of technological expertise. If you are not very tech savvy, take your device to a professional to have it checked for malware. Be sure to ask your friends and family for references. Remember: just because someone says they fix computers does not mean they know how to identify and safely remove malware.

WHY? Doing this will reduce the risk for further problems.

CHECK YOUR EMAIL ACCOUNT FOR "AUTO-FORWARD RULES"

Delete any rules that you did not create.

WHY? This tactic is used by criminals to maintain access to the emails that are coming and going from your account even after you have secured the account with a password change and enabling 2FA/MFA.

CHANGE YOUR CREDENTIALS

If you think you have been tricked into acting on a phishing message, change your online credentials immediately. This applies to all online accounts including email, banking, social media, and shopping accounts.

Do not make the mistake of using the same username and password for all of your online accounts. This makes it easier for criminals to steal your identity and access funds.

WHY? Malware may be used to harvest sensitive information, including online usernames and passwords, credit cards numbers, bank account numbers, and other identifying information.

SET UP A FRAUD ALERT

Contact one of the major credit bureaus and ask for a free 90-day fraud alert to be placed on your credit report. The three major bureaus are Experian, Equifax and TransUnion. Once you have notified one of these bureaus, they are required by law to notify the other two on your behalf.

WHY? This will make it more difficult for fraudsters to open new accounts in your name. This may seem like overkill, but it is better to be safe than sorry.

REPORT THE SCAM AND PROCEED WITH CAUTION

Forward phishing scams to:
THE US DEPARTMENT OF HOMELAND SECURITY
via their email address: phishing-report@us-cert.gov

WHY? Phishing emails have become a dangerous, yet unavoidable, threat in the digital age. Your best protection is to err on the side of caution and use the "delete" button on emails that seem sketchy. Remember, a legitimate organization or business will never ask you to share sensitive, personal information via insecure channels like email, text or pop-up messages. If the message is truly important, the sender will attempt to contact you through verified methods like telephone or snail mail.

TNT
TEXAS NATIONAL TITLE
A MOTHER LODE COMPANY
WWW.TEXASNATIONALTITLE.COM

| The information herein has been obtained from sources believed to be reliable. However, no investigation has been made to determine the accuracy of such information. No person or entity should rely on the accuracy of these materials without conducting a thorough, independent investigation of same. Texas National Title, its officers, agents and employees have no liability, expressed or implied, relating to these materials.