WHAT YOU NEED TO KNOW: Beware of Phishing Emails

What is Phishing?

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

Typically, a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email than trying to break through a computer's defenses. Phishing campaigns are often built around the year's major events, holidays and anniversaries, or take advantage of breaking news stories, both true and fictitious.

To make phishing messages look like they are genuinely from a well-known company, they include logos and other identifying information taken directly from that company's website. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization. The use of subdomains and misspelled URLs (typosquatting) are common tricks, as is homograph spoofing – URLs created using different logical characters to read exactly like a trusted domain. Some phishing scams use JavaScript to place a picture of a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be changed by using JavaScript. *From TechTarget*

10 Tips to Prevent Phishing Attacks

1 Learn to Identify Suspected Phishing Emails There are some qualities that identify an attack through an email:

- It could duplicate the image of a real company.
- The email may copy the name of a company or an actual employee of the company.
- It might include sites that are visually similar to a real business.
- It may promote gifts, or the loss of an existing account.

2 Check the Source of Information from Incoming Mail Your bank will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.

3 Never Go to Your Bank's Website by Clicking on Links Included in Emails Do not click on hyperlinks or links attached in the email, as it might direct you to a fraudulent website. Type in the URL directly into your browser or use bookmarks / favorites if you want to go faster.

4 Enhance the Security of Your Computer Common sense and good judgement are as vital as keeping your computer protected with a good antivirus to block this type of attack. In addition, you should always have the most recent update on your operating system and web browsers.

5 Enter Your Sensitive Data in Secure Websites Only In order for a site to be 'safe', it must begin with **'https://'** and your browser should show an icon of a closed lock.

6 Periodically Check Your Accounts It never hurts to check your bank accounts periodically to be aware of any irregularities in your online transactions.

7 Phishing Doesn't Only Pertain to Online Banking Most phishing attacks are against banks, but attacks can use any popular website to steal personal data such as eBay, Facebook, PayPal, etc.

8 Phishing Knows All Languages Phishing knows no boundaries, and can reach you in any language. In general, they are poorly written or translated, so this may be another indicator that something is wrong. If you never go to the Spanish website of your bank, why should your statements now be in this language?

9 Have the Slightest Doubt, Do Not Risk It The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data. Delete these emails and call your bank to clarify any doubts. *1-9 From PandaSecurity.com*

10 Change Your Passwords Frequently and When in Doubt Change your passwords regularly – at least 4 times a year. Change it more if you can stand it. If you suspect you have been tricked by a phishing email, immediately change the password and notify your bank.