UNDERSTANDING YOUR NETWORK:

PHISHING

409-899-4438

936-634-1952

www.cmsiptech.com

CMS IP TECHNOLOGIES

Delivering Technology - Making a Difference

PHISHING

Phishing

An attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

The word is a neologism created as a homophone of "fishing" due to the similarity of using a bait in an attempt to catch a victim.

***As defined by Wikipedia**

How is Phishing Different?

Unlike malware & viruses, phishing tries to fool you into handing over valuable information.

And because it relies more on targeting people than the use of technology, it can be sometimes referred to as a "social engineering" attack. Also, because it does not always install malware, regular antivirus programs may not protect against it.

Phishing Attacks are Growing

The use of phishing for the gathering of vital data has continued to grow each year.

The purpose of this documentation is to make users aware of the cyberthreats that are out there and how to avoid them. Even with all the available technology, the best tool to fighting these attacks are user awareness and best practices.

PHISHING

Where does a Phishing Attack Come From?

There are multiple sources for phishing attacks, but basically, they come from emails, websites, and SMS.

Emails may be the most common type of phishing attack. It begins when you receive what appears to be a harmless email. The email appears to be legitimate, possibly from someone you do business with like the BBB or PayPal, and they want you to confirm an account number. The email may even threaten you to take action or there will be severe consequences. Regardless, the email is fake and you have now shared private information with a criminal.

Websites are another source of phishing attacks. Just like the emails, attackers will have copy-cat websites. This website may have the same look and feel of a website you know, it may even have their logo. And just like the emails, it's all about getting you to enter in your personal information.

One other source is **SMS**. SMS phishing, also called smishing, is an attack where cybercriminals send text messages with URL links. User who click the link are taken to a phishing website where, again, they are asked to enter personal information.

PHISHING

Types of Attacks or Attack Schemas

Phishing Attack— As we mentioned previously, a copy-cat email, website, or text message that appears to be legitimate but is not and contains malicious links with the purpose of getting your personal information.

Spear-phishing— A variant that is typically aimed towards a specific organization or company instead of a wide audience with the sole purpose of gaining unauthorized access in order to collect intellectual property or trade secrets.

Watering hole— A new type of spear-phishing attack that targets an entire website in order to infect a group of individuals that regularly visit it. The term "watering hole" comes from the fact the attackers corrupt the website and essentially wait for victims to come to the website instead of inviting them by email or text messages.

Whaling Attack— Another type of attack that has evolved from the previous that received its name based on the target, known as the "big fish". Whaling attacks use social engineering techniques to target executives of private business and government agencies in order to steal confidential information and access restricted resources that may have a higher dollar value. Emails sent to victims appear to come from a legitimate sender and may include content designed for upper management. By opening a "classified report" or a "subpoena" users could be installing malware like keyloggers.

Social Phishing— This attack uses the social network platforms like Facebook, Twitter, LinkedIn and others to gather confidential information and gain access to your personal data. It still begins with a message containing a link to a malicious website, but it is sent through the social network platform. Typically, the message or ad will offer something such as attractive discounts, desirable products or latest Hollywood gossip to entice users to click on the link. Clicking on the link begins the process again of acquiring access to your data.

PHISHING

How to Protect Yourself

Take These Action Steps to Avoid Phishing

- **Security Software.** Use trusted antivirus security software and keep it updated
- **Use a firewall with content-filtering.** Content filtering, like your antivirus, can help reduce your risk. ***Remember though, nothing is 100% fool-proof.***
- **Don't send everything via email.** Don't email personal or financial information, unless you have a secure email encryption software in place.
- **Do your own typing.** Only provide personal or financial information though an organization's website if you typed the address yourself and it begins with https:
- **Read your statements.** Review credit card and bank statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and your account balance.
- **Pick up the phone to verify.** Be cautious about opening email attachments or downloading files, even if they do appear to be legitimate. It's always okay to call someone and ask if they sent an email to you with an attachment.
- **Beware unknown senders.** Don't click on links or download files from senders you do not know.
- **Beware of popups.** Never enter personal information into popup screens.

PHISHING

In Conclusion

Nothing is fool-proof, but with user awareness and proper network security policies in place, we can reduce the likelihood of loss of data and the spread of infection.

ABOUT CMS IP TECHNOLOGIES

www.cmsiptech.com

Interested in What Managed Services Can Do For You?

CMS IP Technologies offers over 30 years of IT experience. As the demand for network security has grown, so has CMS. With offices located in both Beaumont and Lufkin, we are prepared to answer your questions.

409-899-4438

936-634-1952

www.cmsiptech.com

CMS IP TECHNOLOGIES

Delivering Technology - Making a Difference