June 2018

- **Learn to Recognize Phishing Scams**

What is Phishing?

Phishing is one of the easiest ways for criminals to steal your data, including your login credentials, banking information, and credit card numbers. It's usually carried out via email, but it has now spread to social media, messaging services, and apps.

In its basic form, phishing occurs when an attacker that's masquerading as a trusted entity fools a victim into opening an email, instant message, or text. And the recipient is tricked into clicking a malicious link or to reveal sensitive information that could include email addresses, user ID's, and passwords. It can even include various forms of financial data like credit card lenders or online banking sites. Sometimes, personal data like his or her date of birth, address, and social security number is taken. If an attack results in unauthorized purchases, the stealing of funds, or any kind of identity theft, it can have devastating effects – especially if they're tied to a corporation or government entity. A phishing attack on a business network can lead to the installation of malware or the freezing of the system as part of a ransomware attack, which can give this person a more immediate profit.

More complex phishing schemes involve hackers who use fake social media profiles and emails to build a rapport with the victim over the months or even years. And in these cases, specific victims are targeted for a certain type of data that they would hand over to someone they trusted. If you want to learn more about phishing emails, be sure to visit the National Cyber Security Alliance at staysafeonline.org

Beymar Rozo
IT Director
Elite Marketing Group
Direct 713.507.1014
Fax 713.507.1090
www.elitemktg.net