SCAM ALERT: Understanding Email Scams

Email provides us a convenient and powerful communications tool. Unfortunately, it also provides scammers and other malicious individuals an easy means for luring potential victims. The scams they attempt run from bogus business opportunities to phishing schemes using a combination of email and bogus web sites to trick victims into divulging sensitive information. To protect yourself from these scams, you should understand what they are, what they look like, how they work, and what you can do to avoid them.

Bogus Business Opportunities are scams that promise the opportunity to make a great deal of money with very little effort. They're normally full of enticements such as "Work only hours a week," "Be your own boss," "Set your own hours," and "Work from home."

Spear Phishing is an email targeted at a specific Individual or department within an organization that appears to be from a trusted source. It's actually cybercriminals attempting to steal confidential information. 91% of cyberattacks and the resulting data breaching begin with "spear phishing" email, according to research from security software firm Trend Micro. Spear phishing is an increasingly common form of phishing that makes use of information about a target to make attacks more specific and "personal". These attacks may, for instance, refer to their targets by their specific name or job position, instead of using generic titles like in broader phishing campaigns.

Trojan Horse is an email that offers the promise of something you might be interested in—an attachment containing a joke, a photograph, or a patch for a software vulnerability. When opened, however, the attachment may do any or all of the following: create a security vulnerability on your computer, open a secret "back-door" to allow an attacker future illicit access to your computer, install software that logs your keystrokes and sends the logs to an attacker, allowing the attacker to ferret out your passwords and other important information, install software that monitors your online transactions and activities, provide an attacker access to your files, and turn your computer into a "bot" an attacker can use to send spam, launch denial-of-service attacks, or spread the virus to other computers.

Scammers use clever schemes in order to defraud people. It is important to stay a step ahead and be aware of their tricks. Be cautious about opening any attachments or downloading files from emails you receive, even if it looks like it is from a friend or co-worker–unless you are expecting it or know what it is. If you send an email with an attached file, include a message explaining what it is. Listed below are some recommendations that can minimize your chances of falling victim to an email scam:

- Filter spam.
- Don't trust unsolicited email.
- Treat email attachments with caution.
- Don't click links in email messages.
- Install anti-virus software and keep it up to date.
- Install a personal firewall and keep it up to date.
- Configure your email client for security.

If you have further questions, please contact us at 336.879.5684.