USER NOTICE DOCUMENT

Released to all PRO-Active clients: 4/22/2016

AVOID GETTING CAUGHT IN A PHISHING SCAM

Don't take the bait. There has been a huge increase in phishing scams received in emails that appear to be harmless or legitimate, but lure you into their net then steal your privacy, infect your computer or hold your data hostage.

This can be very damaging and costly to the company and computer network. The following information is provided to help you educate your staff and prevent damaging infections.

Common Phishing Hooks:

LINKS IN THE EMAIL: links in the body of an email might look valid, but when you click on the link it takes you to a totally different address. If you hover over the "baited" link, most browsers will display the actual link you would be directed to in the bottom left corner.

EMAIL ADDRESS: Spammers use what is called "Spoofing" to present you with an email address that looks convincing, but it's actually hiding the bogus email account. Common scams include emails stating there is a package waiting at the post office or there has been a questionable charge on your credit card and you must sign in to confirm the charge. I, personally, don't click on any links in emails that relate to financial accounts such as credit cards or utilities. If I get an email – I open a browser and go to the site directly to verify account status or I call the company customer service line.

GRAMMAR: Most scams have incomplete sentences, poor grammar, and lack of customer brand and contact information. If it does not seem right, there is a good chance it is not valid.

ATTACHMENTS: Scammers will attach files that, when opened, will try to install malware and infect the computer. The best protection is not to open any attachments that you didn't expect or were not sent from a valid source. Do not enable any macros or approve the installation of software.

FREE SITES: Avoid websites that require you to install an application to access free files including fonts, music, videos, games or other applications. Validate the site is safe before downloading and installing any applications.

The latest lure in phishing scams is ransomware. The user is tricked into running a program or accessing a website that runs a program that will encrypt and lock all your data. Your data is held hostage and then requires payment to purchase the password to unencrypt your data. This can be a real sinker because it may encrypt all data across a corporate network, including network drives.

If you have received a questionable email,
contact the HELP DESK and have the email verified.

All applications should be approved before installing for both company acceptable usage and protection from malware infections.

If you would like to read the entire article on Avoid Getting Caught in a Phishing Scam or other articles from Intrada Technologies, visit: www.IntradaTech.com/knowledgebase.