Phish swim at you from different directions

Phishing is when someone uses fake emails or texts – even phone calls – to get you to share valuable personal information like account numbers, Social Security numbers, or your account username and passwords. Scammers use this information to steal your money, your identity, or both. They may also try to get access to your computer or network. If you click on a link in one of these emails or texts, they can install ransomware or other programs that lock you out of your data. Scammers often use familiar company names or pretend to be someone you know. They pressure you to act now – or something bad will happen. When you think of phishing, you most likely think about email phishing, as 91% of phishing attacks start with this method of communication. However, phishing attacks are evolving every day. Phishing attacks are evolving every day becoming more sophisticated both in type and frequency.

Phishing Quiz

One of the best security defenses in protecting your online accounts and your password is being able to spot and recognize phishing emails. This quiz will show you how to check email addresses and URLs to identify scams.

IRS 2019 Tax Season Warning

It's income tax season, and as we get closer to the April 15th deadline, we can expect to see an increase in phishing attempts from scammers. In November 2018, the IRS posted a warning on their website about a surge of fraudulent emails impersonating the IRS and using tax transcripts as bait to entice users to open documents containing malware called Emotet.

This malware has been posing as the IRS and sending scam emails with an attachment labeled "Tax Account Transcript" or something similar, and the subject line uses some variation of the phrase "tax transcript."
The IRS reminds taxpayers it does not send unsolicited emails to the public, nor would it email a sensitive document such as a tax transcript, which is a summary of a tax return. The IRS urges taxpayers not to open the email or the attachment. If you receive a phishing email such as this, please report it to phish@kent.edu.

Tips for Staying Safe at Tax Time

Cybercriminals are crafty and continuously looking for ways to steal your personal information. Think about the enormous amounts of valuable information that is shared online during tax season alone! You provide personal and financial information online during tax season. Cybercriminals take advantage of this time of the year and have to enjoy the increased personal data exposure that happens. It is critical to take precautionary steps to use the internet securely. Keep in mind that your PERSONAL INFORMATION is like Money! You must value it and keep it locked up and safe.

- Ignore IRS scam calls - The IRS never calls you out of the blue if they want to reach you, they send multiple letters through the mail before they pick up a phone to call you.
- File your taxes as soon as you can...before the scammers do it for you!
- Don’t click on unknown links or links from unsolicited messages.
- Never conduct sensitive transactions over public networks (Free WiFi).
- File your tax forms on secure HTTPS sites only.