YES, YOU ARE A TARGET!

Many people mistakenly believe they are not a target for cyber attackers: that they, their systems, or accounts do not have any value. This could not be further from the truth. If you use technology in any way, at work or at home, trust us you have value to the bad guys. But, you are in luck! You already have the best defense there is against these cyber-attacks - **YOU.** So why would any of them want to attack you? It's not just your bank accounts and credit cards that attract cybercriminals, they are interested in your online accounts and personal information. Your Information is valuable! Please view the following examples:

- Any account that can send money or gift cards is very desirable.
- Uber accounts are hacked so they get free rides while you handle the bill.
- Email accounts they hack can be used to send spam and phishing messages. The email account is used to trick your friends, family and co-workers into sending money or clicking malicious links.
- Accounts on remote services like Dropbox, Google Drive, or OneDrive can be used to host or share malware or illegal files.
- Your private information can give details about where you live, and can lead to identity theft, burglary, harassment, etc.

Cybercriminals use various tactics to obtain your personal information and make money from it.

So what can you do to protect yourself?

1. Do **NOT** use the same password across different websites either at work or home. If a hacker gains access to one site, they will have access to your email address you used to sign up and your password. They will then plug that same information into other login portals and sites. Also, if they have access to your email then they could possibly reset any account password connected to that account.
2. Don't fall for online scams and phishing emails. Take the training on how to detect a phish provided on SecureIt.kent.edu to become cyber aware.
3. Make sure your computer is secure and apply patches and updates when they are available. Enable automatic updating.
4. Always use two-factor authentication when available, especially for all online financial accounts.
5. Never tell anyone your password over the phone. Legitimate companies will not ever ask for your password.
6. Limit what you share online! Don't share your birthdate, address, phone numbers or personal identifiable information on social media sites.
7. Lie when setting up your online security questions. It's very easy to find your mother's maiden name online, especially if you are sharing personal information about yourself.
8. Set up alerts with your bank and credit cards. Many will allow you to set up real time text, email or mobile app alerts. You can request a notification any time there is a transaction on your account.

Tax Season Reminder

This may be a good time to remind your family and friends about the IRS scams and other phone-based scams. Many taxpayers have encountered individuals impersonating IRS officials – in person, over the telephone and via email. Don't get scammed. The IRS initiates most contacts through regular mail delivered by the United States Postal Service.

Note that the IRS DOES NOT

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Demand that you pay taxes without the opportunity to question or appeal the amount they say you owe. You should also be advised of your rights as a taxpayer.
- Threaten to bring in local police, immigration officers or other law-enforcement to have you arrested for not paying. The IRS also cannot revoke your driver's license, business licenses, or immigration status. Threats like these are common tactics scam artists use to trick victims into buying into their schemes.
- Require you to use a specific payment method for your taxes, such as a prepaid debit card, gift card or wire transfer.
- Ask for credit or debit card numbers over the phone.
- The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.

Please view our website for the most common tax season scams.

TIPS to Protect Yourself

- Never send your income tax return using public Wi-Fi.
- Use strong passwords and 2 factor authentication when using tax software online.
- Ignore or delete any emails that request personal information from anyone purporting to be from the IRS.
- Do not click on links or download attachments in emails from anyone claiming to be from the IRS.
- Do not engage in telephone calls from someone claiming to be from the IRS.