UTHSC G.U.A.R.D.

March 2019

IN THIS ISSUE

Personalized Scams on the Rise

by Chris Madeksho, Information Security Coordinator

Cyber criminals continue to come up with new and creative ways to fool people. A new type of scam is gaining popularity, personalized scams. Cyber criminals find or purchase information about millions of people, then use that information to personalize their attacks.

A personalized scam is different than the easy-to-spot generic phish; the cyber criminals research and create a customized message for each target. Many times, this involves purchasing a database of names, passwords, phone numbers, or other information from previous successful hacks. It is surprisingly easy to find this type of information due to all the websites that have been hacked.

To check if your email has been a victim of one of these breaches, you can check the website https://haveibeenpwned.com. The recommendation is to check every email address you and your family have, not just your UTHSC email.

The best defense is to recognize that these emails are scams. Some clues to look for are:

- ✓ There is a sense of urgency, or use fear as a tactic to rush you into a decision
- ✓ There is a demand for payment in Bitcoin, gift cards or other untraceable means
- ✓ Google search to discover if other people have reported similar attacks
- ✓ If sent to your UTHSC email, forward the email to abuse@uthsc.edu so the Information Security Team can research

For more information, contact the UTHSC Information Security Team at (901) 448-1880 or itsecurity@uthsc.edu.

Personalized scams?

Your information might have been bought, not stolen

Tax Season=Scam Season

Be careful of IRS tax scams

IRS: Be Vigilant against Phone Scams

by Internal Revenue Service News Briefing, March 05, 2019

As the April filing deadline approaches, the Internal Revenue Service is warning taxpayers to be alert to tax time phone scams where aggressive criminals pose as IRS agents in hopes of stealing money or personal information.

Phone scams or "vishing" (voice phishing) continue to pose a major threat. The scam has cost thousands of people millions of dollars in recent years, and the IRS continues to see variations on these aggressive calling schemes.

"Taxpayers should be on the lookout for unexpected and aggressive phone calls purportedly coming from the IRS," said IRS Commissioner Chuck Rettig. "These calls can feature scam artists aggressively ordering immediate payment and making threats against a person. Don't fall for these."

Beginning early in the filing season, the IRS generally sees an upswing in scam phone calls threatening arrest, deportation or license revocation, if the victim doesn't pay a bogus tax bill. These calls most often take the form of a "robo-call" (a text-to-speech recorded voicemail with instructions to call back a specific telephone number), but in some cases may be made by a real person. These con artists may have some of the taxpayer's information, including their address, the last four digits of their Social Security number or other personal details.

The Treasury Inspector General for Tax Administration (TIGTA), the federal agency that investigates tax-related phone scams, says these types of scams have cost 14,700 victims a total of more than $72 million since October 2013.

The IRS will never:

- 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.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.
- Call about an unexpected refund.

Stay alert to scams that use the IRS or other legitimate companies and agencies as a lure. Tax scams can happen any time of year, not just at tax time. For more information visit Tax Scams and Consumer Alerts on IRS.gov.