Cybersecurity: Best practices to keep your data safe

MARGARET WAAGE
mwaage@cherokeetribune.com

Chances are that everyone who uses a computer has been subjected to at least one attempted cyberattack.

They can range from email pitches asking for financial account information, to official looking emails that encourage you to click on a link that exposes your computer to malware and website links that can transmit viruses.

Mostly everyone who uses smartphones and computers are subject to data sharing through any number of apps installed on these devices.

Robert Herjavec, a cybersecurity expert and star of ABC's "Shark Tank" told CNBC's "Mad Money" host Jim Cramer, "People need to wake up when it comes to protecting their data."

The recent story detailing how Facebook allowed third-party developers to access user data through its login tool shows how social media terms of service agreements

SEE **DATA**, A3

DATA

From A1

are either overlooked by users or users are unaware of the potential for misuse by companies with other intentions besides creating an app for its own sake.

How can people protect themselves? Experts say awareness and diligence can help.

RECRUITING SCAMS

A job recruiting scam preys on the out-of-work with a text message appearing to come from a potential employer with instructions to download a Google app called hangout to proceed to the interview process. For job offers that seem too good to be true, be advised they're probably fake. It's likely your data was obtained from job boards where resumes are posted.

Susan P. Joyce, publisher of Job-Hunt.org, advocates, "The best defense against job scams is to do research before you apply or respond to a recruiter's email. If the employer or the staffing agency name is not in the job posting or email, ask for it before you apply. You don't want to waste your time applying for a fake job."

FAKE PRIZES

Messages about winning a foreign lottery rely on the excitement of a big win to get you to pay processing taxes, duties or fees. Lottery hustlers use bank account information to make unauthorized withdrawals or use the credit/debit card to make additional charges. Never send money on the promise of a pay-out later — that's a warning sign to delete the message. The FTC cautions consumers thinking about responding to a foreign lottery that it's a violation of federal law.

Cybersecurity Illustration by Margaret Waage

TAX SCAMS

Tax season can prompt tax scams that range from unsolicited calls from what appears to be the IRS, done through caller ID spoofing, requesting payment for bogus tax bills, or other personal information. The Treasury Inspector General for Tax Administration, has received reports of about 766,000 scam contacts since October 2013 where nearly 4,550 victims have collectively paid over $23 million as a result of the scam. According to the IRS, tax scams can happen any time of year, not just at tax time and consumers are urged to visit "Tax Scams and Consumer Alerts" on IRS.gov to learn about various tactics that are used.

John Veith of North Georgia CPA, Inc., said he's required to file all returns electronically, unless a client requests not to. Veith says the most common fear customers have is scammers getting their information. Each year you will get a new identity protection PIN from the IRS to enter before e-filing your return as a preventative measure.

"The IRS will not call you to request money by threatening that you will go to jail," said Veith. In his article, 'Tips for Stronger Cyber Security' Veith advises, "Don't open email from someone you don't know and never click on any links. For my clients who get calls with tax threats, I tell them to give the caller my number. I've yet to be contacted from anyone!"

The best way to handle fraudulent emails, texts or calls is to educate yourself on the variety of forms they take and report them. The Federal Trade Commission features a scam alert section on their site and lists recent schemes and older ones dating back to 2012.

If you receive an email you think is spam, forward it to the FTC at spam@uce.gov. If the email appears to be impersonating a company, organization or bank, contact that organization directly.

If you responded to an email that may be a scam, file a report with the FTC at www.ftc.gov/complaint or report it to your state Attorney General, using contact information at naag.org. Be informed as a best practice against identity theft by getting familiar with FTC's identity theft website at ftc.gov/idtheft to minimize your risk.

When it comes to protecting your data the more you know the better your odds are for maintaining privacy. For those seeking to work in this field, Chattahoochee Technical College offers an Associate of Applied Science Degree with a concentration in Computer Information Systems and Cybersecurity. The basic competency courses are taught with specialized areas of study in Security, Network Defenses & Countermeasures, Computer Forensics, and Ethical Hacking and Penetration Hacking. To learn more about the program, visit www.chattahoocheetech.edu/cybersecurity or plan on attending an information session at the Mountain View Open House Tuesday, March 27 at 2680 Gordy Parkway in Marietta from 5-7 pm.