Monthly Cybersecurity Newsletter

January 2021 Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Stay Safe from Cybercrime During Tax Time

It is tax season again, which means it's also time for tax scams. The enormous amounts of valuable personal and financial information shared online during this time of year make it a haven for cyber thieves – and they are doing everything they can to take full advantage of the opportunity tax season brings them.

During this time of increased potential for having your personal information exposed, it is important to take steps to use the internet safely. Remember that your personal information is like money. Identity thieves continue their tax-time fraud exploits on two fronts: tax identity fraud and IRS imposter scams. By making informed choices when sharing your personal information, by filing your tax returns as early as possible and by verifying that you are speaking to the IRS, you can thwart these identity thieves.

Here are four ways cybercriminals try to take advantage of taxpayers during tax season:

- **IRS impersonation scams:** Callers claiming to be IRS employees might call and insist that you owe money and that it must be paid as soon as possible via gift card or wire service. If the call is not picked up, they leave an emergency callback message. It is important to remember the IRS will never call you to demand immediate payment. They will mail you a bill if you owe money.
- **Marked increase in phishing, email and malware schemes:** Watch for unsolicited emails, texts, social media posts or fake websites that might prompt you to click a link or share personal and financial information. Cybercriminals can use such information to steal your money and/or your identity. Unfamiliar links or attachments can also contain viruses, spyware or other malware that get installed on your computer or mobile device without your knowledge.
- **Fraudulent tax returns:** File your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If you file early, it becomes impossible for a fraudster to submit another return with your personal information.
- **Tax preparer fraud:** The overwhelming majority of tax preparers provide honest services, but some dishonest individuals might target unsuspecting taxpayers, and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return that their preparer must sign it with their IRS preparer identification number.

Here are a few resources that can help you protect your identity and be safer and more secure online this tax season – and year-round:

- STOP. THINK. CONNECT.™ Tips and Advice
- Identity Theft Resource Center
- The Federal Trade Commission's IdentityTheft.gov
- The Internal Revenue Service's Tax Scams and Consumer Alerts

If you believe you are a victim of identity theft or identity fraud, the following are some steps to take:

- File a report with your local law enforcement agency.
- File a report with the Federal Trade Commission (FTC).
- File a report with the three major credit bureaus (Equifax, Experian, and TransUnion) and request a "fraud alert" for your account.

If you receive spam or a phishing email about your taxes, do not click on the links or open any attachments. Instead, forward the email to phishing@irs.gov. Other tax scams or frauds can be reported by following this IRS guide.

Cruel Phishing Attack: "You're Fired" (Not Really, Just Hacked)

Cybercriminals are using phishing emails that inform people they have been terminated from their jobs, according to Linn Freedman, a partner at Robinson & Cole LLP, writing for the National Law Review. These types of attacks are particularly effective (and cruel) during the COVID-19 pandemic since many people are worried about losing their jobs.

According to Freedman, "The scheme works like this: an email is sent to an employee from an authority in the Human Relations department stating that the individual has been terminated. An attachment to the email provides further information about the termination and the severance payout, which appears to be on Google Docs. When the victim clicks on the attachment, they are directed to a fake Google Docs page and told to click on another link. When they click on that link, they are directed to a URL to download a file."

Many employees are tempted to open such an email, even if they think it is unusual or suspicious. A message that says "You're fired" is meant to play on one's emotions and elicit a response, which is exactly what the attacker wants. Since a message like this is so drastic and final, it is hard to resist opening it. It is important to remember that employers do not usually terminate their employees with an email.

Freedman offers the following advice:

- Be wary of termination emails – if you receive one, it is probably fake.
- If you really are terminated, human resources will get in touch with you one way or the other.
- Continue to be vigilant about phishing schemes and spoofing campaigns using executives' identities.
- Think twice before you click or say, "I agree."
- Don't open any attachments or click on any links that you are not expecting.
- Pick up the phone to confirm suspicious emails, links or attachments.

Remember, it only takes one person to fall for a phishing attack for an attacker to gain a foothold on your organization's network. To read the complete article from the for the National Law Review, visit https://www.natlawreview.com/article/privacy-tip-260-don-t-fall-worrisome-termination-email-sent-your-boss.

2020 Top Phishing and Vishing Attacks and Trends by Roger Grimes

It's an extra-challenging year, harder than most, to choose the most impactful cybersecurity events. The year ended with a bang – the SolarWinds supply chain attack – which possibly impacted up to 18,000 potential victims, including almost all of the Fortune 500, involved a top-tier computer security vendor, at least a half-dozen top U.S. government agencies, and essentially brought the long feared, nation-state-sponsored, supply chain attack into reality.

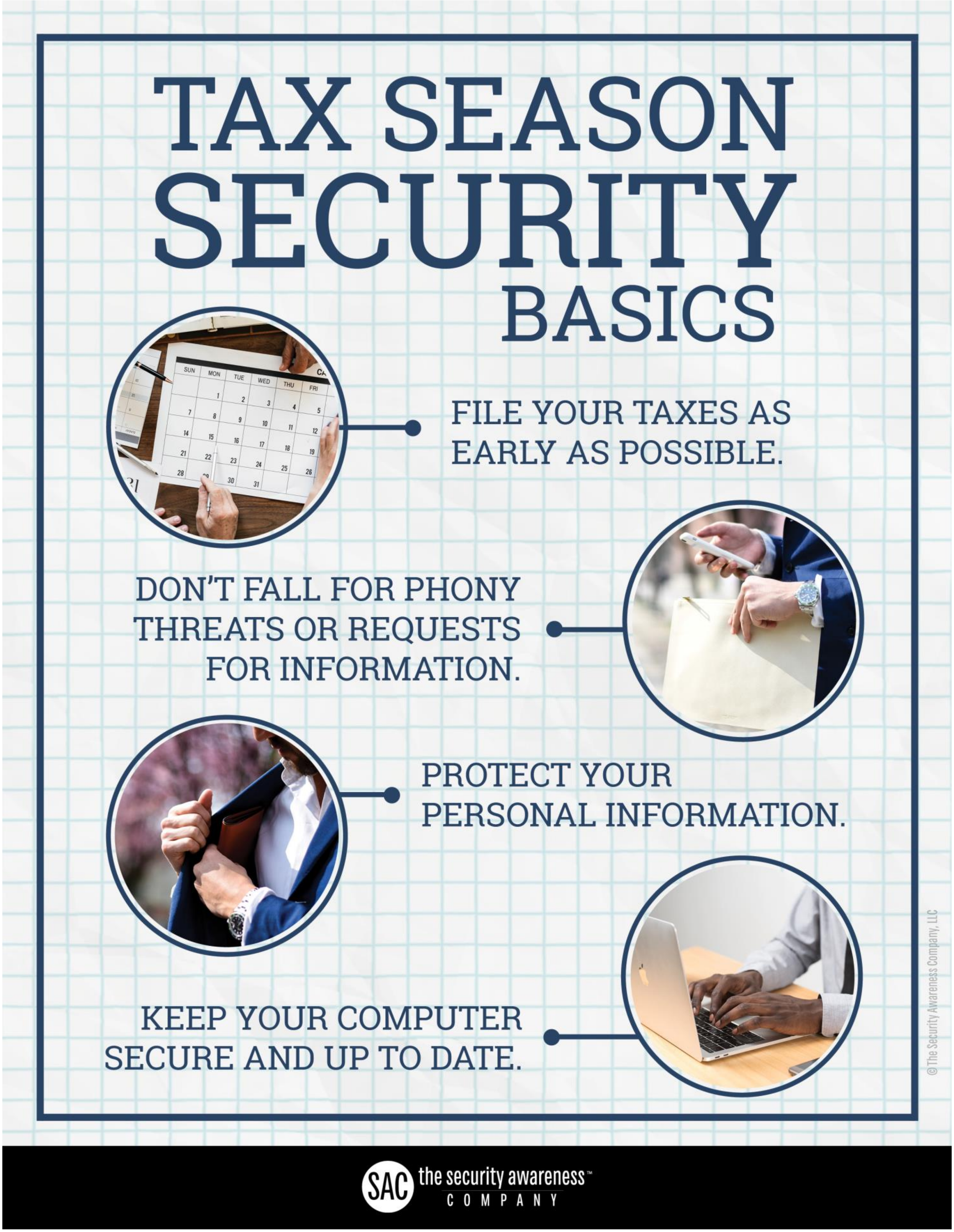
The SolarWinds attack was notable for a bunch of other reasons, including that it went undetected by everyone for over half a year and that it is one of the few attacks that may have not started with a phishing attack; although we still don't know how SolarWinds was first compromised, so who knows?

Phishing attacks are involved in 70% to 90% of all malicious data breaches and it has been that way for decades.

With that said, I decided to pick out the top attacks of 2020 which involved phishing, and some of them aren't specific attacks, but trends.

- Ransomware Gone Nuclear
- COVID-19 Themed Phishes
- Healthcare Targeting
- Twitter Bitcoin Attack
- GoDaddy Employee Hacks
- Trickbot Takedown

The full post is available at the KnowBe4 blog, with each of these six detailed: https://blog.knowbe4.com/2020-top-phishing-vishing-attacks-and-trends



TAX SEASON SECURITY BASICS

FILE YOUR TAXES AS EARLY AS POSSIBLE.

DON'T FALL FOR PHONY THREATS OR REQUESTS FOR INFORMATION.

PROTECT YOUR PERSONAL INFORMATION.

KEEP YOUR COMPUTER SECURE AND UP TO DATE.

SAC the security awareness™ COMPANY

Have a High School Student in Your Life? If So, Listen Up.

North Carolina high school students have an amazing opportunity to explore potential careers in cybersecurity and computer science while competing for scholarships and prizes as part of the free online CyberStart America competition.

Registration is now open at www.cyberstartamerica.org.
The deadline to register is March 8, 2021.

What is CyberStart America?

CyberStart America is a series of free challenges in which young men and women act as “cyber protection agents” to solve cybersecurity-related puzzles and explore related topics, such as code breaking, programming, networking and digital forensics.

Students do not need knowledge or experience in information technology or cybersecurity to participate.

Awarded when you join the game. Welcome to CFA agent!

Awarded when you complete your first challenge.

Awarded if you complete a challenge in under 30 seconds.

Why is CyberStart America important?

According to the N.C. Department of Commerce, the state is projecting a shortfall of IT and cybersecurity professionals by 2022. This deficit could be filled by local talent, but for that to happen, it is important to expose young people early to potential careers as well as educational resources that can help put them on a cybersecurity and IT career paths.

For years, the program’s sponsor, SANS Institute, has used the competition (formerly called Girls Go CyberStart) to help expose thousands of students – even those with little or no interest in computers – to possible careers.

“Before I recruited girls to be a part of this wonderful program, I struggled to get them to realize they could be a computer scientist,” one educator said. “I had girls actually saying they were too stupid to do this, until I said, ‘Just try it.’

“Some found out they were good at puzzles, some found out they liked programming. I now have girls who are asking our counselor about computer science degrees at our local community college.”

Stay Safe While Working from Home

Working remotely has its benefits, ***but*** it comes with added responsibility. Click here for tips on how to stay secure while working from home.

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. ***Note****: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/security-awareness-training/ouch-newsletter

January 18, 2021: Martin Luther King, Jr. Birthday

January 19, 2021: Tech Tuesday Workshop – Healthcare's Top Threats in 2021 and What You Can Do About Them

January 27, 2021: Resilience in Philadelphia: A Case Study

January 28, 2021: Data Privacy Day

February 2, 2021: How to Stay Ahead of Cyberthreats webcast

Also…for a list of upcoming SANS webcasts, visit here!

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*

Disclaimer*: Vendors, references, and links in this newsletter are for informational purposes only and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*