Volume 4, Issue 4

April 2018

First Bank & Trust Company
Member FDIC

INSIDE THIS ISSUE:

Member FDIC EQUAL HOUSING LENDER

Abingdon Virginia, East
276-628-3838

Abingdon Virginia, West
276-628-9558

Bridgewater Virginia
540-828-2020

Bristol Virginia, East
276-466-9222

Bristol Virginia, West
276-669-1122

Bristol Tennessee, Volunteer Pkwy
423-652-2022

Christiansburg Virginia
540-260-9060

Fairlawn Virginia
540-633-3793

Gray Tennessee
423-467-9966

Harrisonburg Virginia
540-434-0671

Johnson City Tennessee
423-975-9900

Kingsport Tennessee
423-246-3700

Lebanon Virginia, East
276-889-3401

Lebanon Virginia, West
276-889-4622

Lynchburg Virginia
434-455-0888

Norton Virginia
276-679-7401

Staunton Virginia
540-885-8000

Verona Virginia
540-248-7700

Waynesboro Virginia
540-943-5020

Wise Virginia
276-328-3439

Wytheville Virginia
276-228-1125

2018 Dirty Dozen List

It's that time of year again! Another tax season is here and along with that comes prime opportunities for criminals to hit a huge payday. Every year the IRS puts together a list of scams that taxpayers should be on the lookout for. The IRS believes that hackers are becoming more aggressive with their tactics and are urging tax filers, along with tax preparers, to remain vigilant and keep their eyes and ears open for potential fraud.

There are twelve warnings on the list, however, there are three that seem more prevalent and continually appear on the yearly list: phishing scams, phone scams and identity theft.

Phishing Scams– Although phishing scams are not a new trend, hackers are becoming savvier with their methods and that is what has the IRS alarmed. It is getting more and more difficult to decipher between a fake email and a real one. Additionally, hackers have also managed to create fake websites that look extremely legitimate. One of the most recent scams the IRS has been tracking for the 2018 tax year involves a tax filer receiving an email from an organization they trust or have done recent business with such as a bank, credit card company or even a tax professional in hopes the victim would divulge personal information such as social security numbers, birth dates, etc. Opening one of these fraudulent emails can have a detrimental impact on an individual because some of those emails may contain dangerous malware or viruses that can infect a user's computer or, even worse, be a ransomware where the hackers demand money in exchange for releasing the user's computer and data.

Phone Scams– Also on the rise is phone scams. Criminals are calling tax filers pretending to be representatives of the IRS or other legitimate tax preparer companies. During these types of phone calls the criminal demands payment from a tax filer claiming they owe the IRS money. They request funds to be sent via a wire transfer or a prepaid debit card or gift card. Many of these scammers leave messages on voicemails stating the matter is "urgent" and needs "immediate attention" and provide the tax filers name, address and even date of birth which makes the victim believe the person calling is legitimate. While the scammers have become more sophisticated in their attacks, they also still rely on old school methods of trying to bully and intimidate their victim into sending money by using bogus threats.

Identity Theft-Identity thieves will go to any lengths to get unwitting victims to give up their Social Security number, credit card numbers, bank account numbers or any other valuable piece of information that can help them steal an identity. This tactic is extremely common. Although the amount of identity theft reported to the IRS dropped in 2017, it remains one of the more popular tactics for criminals. Having one's identity stolen can be a very long and painful process to get resolved.

Continue page 2

These are just three out of the twelve on the list. As always, we can try to thwart these attempts to rob us of our identity, money or data.

⇒ Always remember, if you receive unsolicited emails that claim to be from the IRS, report it to phishing@irs.gov. The IRS does not communicate by email and most definitely would not request personal financial information via their website; nor do they communicate by text message or through social media channels.

⇒ Be skeptical of phone calls that claim to be from IRS representatives. The IRS also does not bully or use aggressive tactics when a taxpayer owes money. And nine out of ten times, the IRS will communicate in writing regarding any payment owed or refund that will be received. If you are unsure of who is on the other end of the phone call, hang up and call the IRS back directly.

⇒ To help prevent identify theft, protect personal data by ensuring your personal information such as Social Security card and tax records are secured. Don't leave bills or other pertinent information that may contain information, such as date of birth or address, lying around and be sure to shred any docs that contain personal information. Scammers have been known to search dumpsters to retrieve information needed for them to carry out their crimes. Your trash can be a potential treasure trove for a determined criminal.

⇒ Make sure security software is up to date and firewall protections are activated and when possible encrypt sensitive files such as tax records stored on computers.

To learn more about the IRS Dirty Dozen and how you can protect yourself during this tax season, visit https://www.irs.gov/newsroom/dirty-dozen.

Sources:
https://www.irs.gov/newsroom/dirty-dozen

DATA EXTORTION IS NOT GOING ANYWHERE

Each year, security firms not only discuss upcoming security trends, but also valuable lessons learned from the previous year. One of the items they continue to discuss each year is data extortion, also known as cyber extortion.

Over the years, cyber extortion has morphed into multiple forms, all focused on encrypting data and holding it hostage, stealing data, threatening exposure and denying access to data. At the core, fear plays a major part of any successful extortion scheme. Digital extortion is extremely lucrative for cyber criminals and they do not discriminate on what type of corporations they target. So far, ransomware has been the popular and effective method hacker's use and there has been an increase in data extortion threats, in part due to the availability of digital currency such as Bitcoins. This makes it easy for a criminal to collect payment without being easily tracked, hence allowing the culprit to, more often than not, get away with the crime.

Many times, extortionists threaten to disrupt a company's website, thus preventing customers from accessing it. They also may warn that they will release sensitive customer and employee data unless they are paid off. They use these intimidation tactics hoping the victim will roll over and pay up. If the criminal follows through with their threats, it can have long-lasting financial and reputational effects on a company.

Authorities and experts don't believe these types of crimes will stop, in fact quite the opposite. As our society moves closer and closer to an all-out digital world, these types of attacks will become more frequent and larger in scale. However, while threats continue to evolve and cybercriminals employ new strategies, user awareness and partnerships with law enforcement and private organizations have provided great success in taking down the cybercriminals who commit cyber extortion.

Continue page 3

Here are some steps to take to try to avoid becoming a victim:

- Protect the most critical data.
- Continually review business continuity plans to prepare for any disruption, and, if it does occur, know how to avoid excessive disruptions to the business.
- Take the threat seriously, and have an incident response team to deal with any such attacks or threats.
- Ask employees to refrain from posting too many details on social media.
- Make sure all devices and accounts are secured with solid passwords and security software.
- Do not give in to the cybercriminals' demands and be sure to report all threats to the proper authorities.

Most experts agree that abiding by criminals' demands provides you no guarantee that they will not attack now or in the future. Experts believe that giving into them gives the cybercriminals more motivation to continue with their threats against your company and others.

Today, most companies realize that cybersecurity has become increasingly important for defending against persistent and evolving threats. Security is multilayer and will require an all-encompassing approach to ensure your company is prepared.

Sources:
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/security-101-digital-extortion