First Bank & Trust Company

The Bank That Puts You First

Member FDIC

Member FDIC

EQUAL HOUSING LENDER

December 2022

The Top Five Cybersecurity Trends In 2023

In recent years we have seen the topic of cyber security move from the IT department to the board room. As attacks have proliferated and the potential penalties, both regulatory and in terms of loss of customer trust, have increased, it has become a priority at every organizational level.

We often think of cybersecurity as an ongoing battle between hackers and criminals, and security experts, which is constantly escalating due to constant advances in technology. This is the "glamorous" side of the business that we sometimes see depicted in TV shows and movies. And indeed, threats sometimes come from hostile foreign states or devious, tech-savvy criminal masterminds. In reality, however, threats are just as likely to emerge due to improperly secured networks leaving sensitive data accidentally exposed, or unwary or indiscreet employees using non-secured devices while working from home.

A shift to a culture of home and remote working that started during the Covid-19 pandemic and has persisted in many organizations, as well as the spread of the internet of things (IoT) into every area of business and society, means there has never been more opportunity for lax security to cause headaches and expense. Because of this, cybersecurity is top of everyone's agenda in 2023, so here's a look at some of the key trends in 2023:

Internet of Things and cloud security

The more devices we connect together and network, the more potential doors and windows exist that attackers can use to get in and access our data. And in 2023, analysts at Gartner predict, there will be 43 billion IoT-connected devices in the world.

IoT devices – ranging from smart wearables to home appliances, cars, building alarm systems and industrial machinery – have often proven to be a bugbear for those with responsibility for cybersecurity. This is because, as they are often not used to store sensitive data directly, manufacturers haven't always been focused on keeping them secure with frequent security patches and updates. That has changed recently, as it's been shown that even when they don't store data themselves, attackers can often find ways to use them as gateways to access other networked devices that might.

Continued on page 2

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-266-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
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
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan
Production Offices
Bedford, Virginia
540-583-5458
Daleville, Virginia
540-966-7006
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust
Mortgage Lending Division
Bristol, Virginia
276 -644-9900

In 2023, a number of governmental initiatives around the world should come into effect designed to increase security around connected devices, as well as the cloud systems and networks that tie them all together.

Work-from-home cybersecurity becomes a priority for businesses

Recently, a cybersecurity priority for many organizations has been to secure the millions of devices worldwide that are being used for home and remote working since the start of the pandemic. Pre-pandemic, when we were all office-based, it was simple enough for security agents, probably based in IT departments, to regularly check and update company laptops and smartphones. In 2023, when workers are more likely than ever to use personal devices to remotely connect to work networks, a new set of challenges has emerged.

International state-sponsored attackers target businesses as well as governments

Nation-states frequently take part in cyber-espionage and sabotage in an attempt to undermine unfriendly or competing governments or to access secrets. In this day and age, however, it's increasingly likely that companies and non-governmental organizations (NGOs) will find themselves targeted by state actors.

In 2023, more than 70 countries are due to hold governmental elections – events that are frequently a target for attack by hostile foreign interests. As well as hacking and cyberattacks on infrastructure, this will take the form of disinformation campaigns on social media. This often involves seeking to influence the results in favor of political parties whose victories would benefit the government of the hostile state.

Artificial intelligence (AI) plays an increasingly prominent role in cybersecurity

As the number of attempted cyberattacks has grown rapidly, it has become increasingly tricky for human cybersecurity experts to react to them all and predict where the most dangerous attacks will take place next. This is where AI comes into play. Machine learning algorithms can examine the vast amount of data moving across networks in real-time far more effectively than humans ever could and learn to recognize patterns that indicate a threat. According to IBM, companies that use AI and automation to detect and respond to data breaches save an average of $3 million compared to those that don't.

Unfortunately, thanks to the ever-growing availability of AI, hackers, and criminals are growing increasingly proficient at using it too. AI algorithms are used to identify systems with weak security or that are likely to contain valuable data among the millions of computers and networks connected to the internet. It can also be used to create large numbers of personalized phishing emails designed to trick receivers into divulging sensitive information and become increasingly good at evading automated email defense systems designed to filter out this type of mail.

Building a security-aware culture

Perhaps the most important step that can be taken at any organization is to ensure that it is working towards initiating and fostering a culture of awareness around cybersecurity issues. Today, it's no longer good enough for employers or employees to simply think of cybersecurity as an issue for the IT department to take care of. In fact, developing an awareness of the threats and taking basic precautions to ensure safety should be a fundamental part of everyone's job description in 2023!

Phishing attacks rely on "social engineering" methods to trick users into divulging valuable information or installing malware on their devices. No one needs technical skills to learn to become aware of these types of attacks and to take basic precautions to avoid falling victim. Likewise, basic security skills like the safe use of passwords and developing an understanding of two-factor authentication (2FA) should be taught across the board and continually updated. Taking basic precautions like this to foster a culture of cybersecurity-awareness should be a core element of business strategy at organizations that want to ensure they build resilience and preparedness over the coming 12 months.

Source: Bernard Marr, Forbes, November 11, 2022

Some of the Most Common Internet Scams in 2022

2022 is almost behind us, and according to some experts, in 2023, we may be on the verge of a "scampocolapyse", as online cons are growing at an unprecedented rate. In this environment, it is imperative for internet users to be aware of the high potential of fraud and how to protect themselves against scams. The five internet scams described below have been listed as some of the common scams in 2022.

1. Smishing

Smishing is a type of fraud that happens through deceptive text messages or SMS, hence the name "SMiShing". Smishing attacks are becoming increasingly common as it is shown that people are more likely to trust a text message than an email. In a fraudulent text message, scammers will impersonate banks, charities, or other organizations to gather personal or bank account information. They will try to get victims to click on links to confirm "suspicious bank or credit card charges." Another tactic scammers will attempt is trying to get the victim to donate to "charitable causes" such as COVID-19 or hurricane relief.

How to Protect Yourself:

- Don't click on any links. Do not call any number provided in a text (if one is provided), call the number that is listed on the source's website.
- Update your phone software. Additionally, install an antivirus app that can scan your phone for these scams.
- Don't reply. Even if the message that was sent to you indicates that you can "Text STOP" to avoid messages, don't reply. Replying will let the scammer know the number is active.
- Always be on the lookout for any strange messages from a familiar phone number. Spammers can fake a caller ID to make it look as if it were a local number or someone you know. This is called spoofing, which makes the number appear as one you may know but is actually fake.

2. The Grandparent Scam

Grandparent scams are on the rise as scammers continue to target the elderly population. These scammers exploit the love grandparents have for their grandchildren by posing as their grandchild who is in a dire situation and needs cash immediately. Usually, they claim that they're in trouble and need bail, or need to leave a foreign destination.

How to Protect Yourself:

- Resist the urge to act immediately.
- Verify identity.
- Make your social media pages private. This will limit the amount of personal knowledge scammers have about you.

3. Fake Checks and Overpayments

There has been a recent increase in fake checks and overpayment scams as more people are selling items online. A scammer will try and buy an item from you online and "accidentally" send you a check more than the listed price. They will then ask you to refund the balance. Fake checks can look identical to real checks and even after depositing the check, it may take weeks for the check was counterfeit.

How to Protect Yourself:

- Do not accept any checks when selling items online. Furthermore, do not try to deposit any checks that are more than the listed price.
- Do not refund. If asked to refund the overpayment, you can count on it being a scam. Do not send any gift cards or wires, as you will more than likely never get that money back.

4. Local Tax Imposters

Tax imposter scams happen when scammers contact you by phone or email pretending to work for the IRS or a local government. Usually, the fraudster will send a message about taxes being owed and request a money transfer or payment by check. These messages are fear tactics and may threaten you by saying that you can be arrested if payment is no made by the due date.

How to Protect Yourself:

- Be alert if you receive a message about unpaid taxes. It is important to note that you will always receive a letter in the mail from the IRS before they give you a call about an unpaid tax liability. Always be aware of any messages containing hyperlinks or requesting money or alternatively, something of value.
- If you do receive this call and are suspicious (as you should be), ask the caller to provide their name, badge number and callback number. Then you should proceed to call TIGTA at 1-800-366-4484 to figure out if the caller is truly an IRS employee with a valid reason to contact you. If they notify you that it is a legitimate call, you can call them back. Otherwise, report the person to TIGTA.
- Don't be alarmed by threats of arrest. The IRS won't threaten to have law enforcement arrest you if the bill is not paid.

5. Employment scams

There are many online employment platforms (i.e., LinkedIn, Glassdoor, Zip Recruiter etc.). Companies use these to be cost effective and convenient when hiring. Unfortunately, scammers can use these websites to gain access to the personal information of their targets.

How to Protect Yourself:

- Do not respond to suspicious messages. If you receive a message about a job, that you are unsure you applied to leave it alone.
- Research. Make sure to thoroughly research the company you applied for to make sure it is a legitimate business. Usually companies will have a "careers" tab on their website, which allows you to verify that they are hiring for the job you applied for on a third-party job page.
- Trust your instincts. If you feel as if anything is suspicious about a position you are applying to, then the best thing is to stop and look for something else.

Cybersecurity attacks have been prevalent for quite some time, but they pose greater risks now than ever before. Protecting yourself against scammers should be at the top of everyone's mind going forward. Internet fraud will only increase in quantity as fraudsters become more cunning and skilled at turning these scams into profits.

Source: *Phil Rogers, Vision Capital, September 29, 2022*