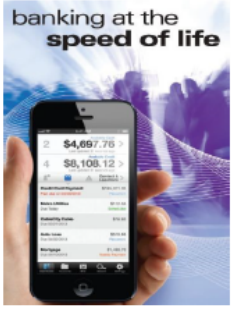
Mobile Banking App is HERE!



UNION BANK

2023 Cyber Security Newsletters

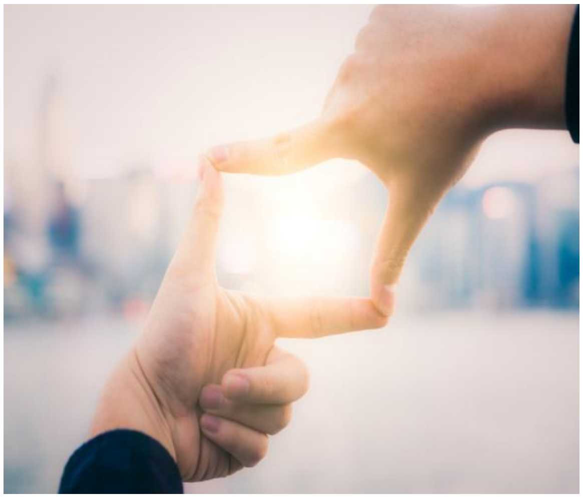
Contents

Mobile Banking App is HERE!

UNION BANK

January 2023

Cybercrime Outlook 2023: It’s All About the Economy



Who likes inflation, rising interest rates, layoffs and soaring gas and food prices? Cybercriminals. And because these struggles will likely continue impacting the economy in 2023, these online scammers should be happy, and wealthier, next year as they con unsuspecting people seeking financial relief.

Economic challenges cause many to change their daily behavior. Some will seek financial assistance from the government. Others will try to land side hustles to pad their bank accounts, while still others will be desperate enough to hope that surprise lottery "winnings" are real.

This creates the perfect environment for scammers, who can use texts, emails, and phone calls to trick desperate victims into surrendering their personal information, emptying their bank accounts, or spending big dollars for services or lottery winnings that never come.

It's the economy, then, that will have the greatest impact on the spread of cybercrime in 2023. Here are our predictions for why.

1. Economic trouble could lead to more scammers trying to earn money – and more victims desperate to save.

As inflation and interest rates continue to rise, consumers will struggle to keep their bank accounts full. Consumers are spending more at the pump and at the grocery store. Borrowing money to pay for cars and homes is getting more expensive thanks to soaring interest rates. These are difficult times for many.

Scammers know this. They also know that consumers are at their most vulnerable when they are worried about their financial health.

Expect a rise in several financial-based scams:

1. Assistance scams: Cybercriminals will reach out to consumers by text, phone, or email to inform them of fake government assistance programs. These messages might claim that consumers can qualify for reduced electric or heating bills or that they are eligible for low-cost government meals and utility subsidies. All the recipients of these messages must do is click on a link, send a small payment, or make a phone call.

This is all a scam, though. Consumers might click on a link that takes them to an online form. To qualify for government assistance, victims must provide personal information such as their name, birthdate, address

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

and Social Security number on the form. When they click "Submit," though, their Personal Identifiable Information – or PII -- is sent to a criminal.

That criminal can then use this information to take out loans or credit cards in the victim's names. They might use it to access their online bank and credit card accounts. They might sell the information on the Dark Web to the highest bidder.

2. Shopping deals: Scammers will send victims messages promoting low-cost clothing, electronics or groceries. They'll set up fake e-shops promoting brand-name items at bargain prices. Again, though, these deals are a scam. The fraudsters behind them will try to steal victims' personal information or convince them to send online payments for bargain products that aren't real. Once consumers send their payments? The entrepreneurs behind these deals and e-shops disappear.

3. A bit of romance? When the economy suffers, people may also be impacted emotionally. Whether they are struggling from recently losing their job or overall despair from financial instability, some might also be suffering from a bout of low self-esteem. This makes them especially vulnerable to online romance scams.

In these scams, criminals strike up a relationship with victims online, sending emails, communicating in chat rooms and buzzing their victims' phones with amorous texts. After building up trust, the scammers, after promising to soon meet their victims in person, ask for money or ask for you to help move money around.

As scammers and consumers get more desperate to pay their bills, we expect to see an increase in scams, and an increase in people falling victim to those scams. So stay alert as you navigate online.

2. Companies trying to cut costs could lead to more breaches caused by chaos and sabotage, which can trickle down to making consumers vulnerable.

The economy's troubles will impact companies in 2023 as well. We have already seen many technology companies reducing and reorganizing staff, and it is likely to continue into next year. And when companies are operating with smaller staff and the people are taking on new responsibilities, you can expect that some companies will become more vulnerable to data breaches, ransomware attacks, and other cybercrimes, because of the changes.

3. With more advanced and open generative AI frameworks available, more scammers could start to use these technologies in high-touch interactions such as romance scams.

Last year, we predicted that criminals would take advantage of improving AI technology to boost the effectiveness of their scams. That prediction turned out to be accurate. And next year? Expect scammers to continue to wield AI in their crimes as this technology becomes even more accessible and easier to use.

Programs such as Dall-E, Midjourney, and Stable Diffusion allow users to create images by describing a picture. These models will create several versions of the images that users describe. This technology can be a powerful tool when wielded by cybercriminals.

Con artists can use these AI tools to create images of the person they are pretending to be and even place them near specific geographic landmarks to add some veracity to their fake personas. It's a way to add more depth to an old scam and to more easily persuade a victim to send cash or pro- vide their credit card information.

4. Weaker versions of 2FA could be exploited, leading to breaches in companies, which can lead to more consumer information exposure.

Criminals are devising attacks meant to breach standard multi-factor authentication technology. Despite this, we still don't see many companies adopting stronger two-factor authentication (2FA) practices for either customers or employees in 2023, which can impact consumers.

That's a problem. Companies that continue to use weak 2FA are inviting cybercriminals to steal important credentials. That leads to serious data breaches and cybercrimes.

The key is for companies to turn to what are known as unphishable factors when setting up their 2FA systems. Unphishable factors are those that criminals can't trick employees into providing. They in- clude such factors as biometrics, device-level security checks, hard- ware security keys, and cryptographic security keys. Over time, com- panies will start to deploy these more secure authentication technol- ogies, but it won't happen anytime soon.

Unfortunately, too many companies rely on phishable factors, those that are easier for criminals to intercept. These phishable factors include passwords, security questions, SMS text messages, and time-based one-time passwords. All of these can be intercepted and used to authenticate.

Consumers can help protect themselves from these types of threats. Make sure your password is unique and avoid using the same one across different accounts.

The Final Word

Challenging economic times make people desperate, often desperate enough to fall for different types of scams. Stay alert this year while living your digital life, because scammers are always finding new ways to trick unsuspecting victims—especially when they are most vulnerable. Remember, if something seems too good to be true online, it probably is.

***Source:* Norton Labs , December 1, 2022**

5 Scams To Watch for in 2023

As cybercriminals find new paths to ill-gotten gains, here are the types of scams we can expect to see in the coming months.

1. Business Email Attacks

Business email compromise (BEC) attacks lead this list, as these scams can have attractive payouts. BEC-related losses totaled nearly $2.4 billion in 2021, according to the most recent report from the FBI's Internet Crime Complaint Center.

These scams involve spoofed emails that look like they're coming from a trusted source such as a company executive, employee or vendor. They typically ask the recipient to transfer funds urgently and rely on manipulative social engineering tactics to get their victims to act quickly.

One common attack is the payroll diversion scam. Scammers masquerading as an employee will email the payroll team to change their direct deposit account details. Sometimes the emails are obviously fake, filled with grammatical errors and sent five or six times a day to the same payroll employee.

Other times, the emails look legitimate and contain a good backstory to lend credibility. A year ago, fraudsters typically would impersonate company executives, presumably because their paychecks would be larger. Recently, we have observed a shift in tactics, with mid-level employees being impersonated more often.

2. Malware and Ransomware Threats

These incidents tend to garner a lot of media attention, like the Colonial Pipeline ransomware attack in 2021. It temporarily took out a major fuel supply system in the southeastern U.S. and resulted in a $4.4 million payday for the hackers.

We'll likely see more of this type of activity, particularly related to the conflict in Ukraine and the associated sanctions. Russian state-sponsored organized crime teams that excel at ransomware will help sustain the war efforts.

U.S. government agencies, defense contractors and other organizations assisting with Ukraine's defense will be targeted with phishing emails aimed at creating havoc.

3. Crypto Scams and 'Pig Butchering'

Using translation programs to communicate with global victims, scammers looking for a payout launch what authorities call "pig butchering" scams.

They'll message someone's phone, dating app or WhatsApp with a "Hey, are we still on for lunch Friday?" The goal is to see if they can get a response and then build an online friendship.

Eventually, they'll ask if the victim knows anything about crypto to lure them onto a sham website where the fraudsters say a friend made a lot of money.

If the victim invests, they'll see rapid returns that lure them into pouring in more money. The scammers are basically "fattening the pig" until it's time to butcher it—when they take all the money out of the account.

4. Innovation in the Cybercrime Cash-Out Process

The place where threat actors are most likely to get caught is in the cash-out. The reason is that law enforcement can start following suspicious activity more easily once transfers surpass $10,000 for standard bank accounts.

Cryptocurrency has been somewhat easier for authorities to track, which is leading to a rise in crypto mixing services. These evade scrutiny by taking in traceable "dirty" crypto and cleaning it so it can't be traced back to a ransomware attack or other cybercrime.

Gift cards present the lowest-risk cash-out for cybercriminals because there's little to no traceability. However, potential targets are smartening up and realizing that "the IRS" isn't going to ask for a payment using gift cards—or crypto, for that matter.

Given these dynamics, we'll likely see criminals seeking new ways to launder their illegal proceeds in the shadows.

5. Cybercrime and Scamming as a Service

Just like the rest of us, fraudsters like a good one-stop shop. Underground virtual marketplaces are springing up with end-to-end services that enable low-skill threat actors to fill their carts and pay with crypto.

They can procure sets of stolen credentials, credit card numbers, phone numbers, phishing kits, ready-to-roll malware and other tools to carry out bank fraud, ransomware attacks, phishing campaigns and more. We'll see an increase in these types of services in 2023.

Looking Ahead

Yes, scammers are inventive. Yes, they will continue to try and steal our money in dozens of resourceful ways.

But we're all becoming more educated cybercitizens, increasingly able to spot and fend off malicious campaigns.

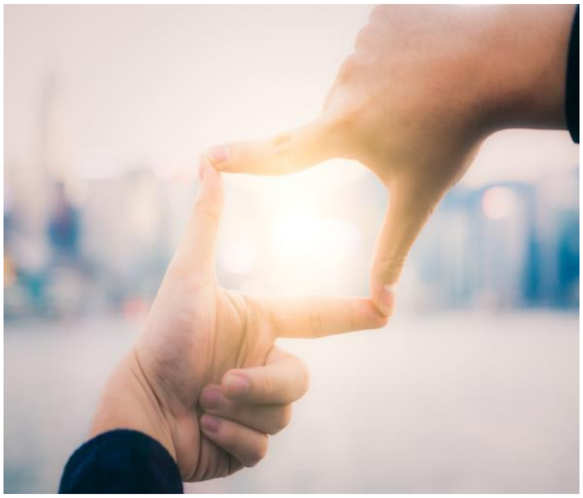
Source: Forbes, John Wilson, Contributor, December 19, 2022

UNION BANK

February 2023

Insider threats are a major security issue in the financial sector

The Financial industry is becoming a hot target for hackers and ransomware, and it's no surprise — the industry does deal with money, after all. The sector is 300 times more likely to experience a cyberattack than any other industry, and the industry is absorbing the highest cost with an average of $18.3 million lost per cyberattack. But it's not just the Scrooge McDuck-style pools of coins and cash that cause hackers to turn their eyes to financial institutions. It's the access. The industry has a vast amount of internal users that can quickly turn into insider threats.



What are insider threats?

An insider threat is simply a cybersecurity threat (the potential theft or compromise of critical data or assets) that comes from an internal user, i.e an employee. While insider threats can happen accidentally or on purpose, they are a threat to be taken seriously. According to the Ponemon Institute 2020 Cost of Insider Threats: Global Study, there were 4,716 insider attacks recorded across the globe, and the cost of an insider incident almost doubled between 2019 and 2020 from $493,093 to $871,686. These incidents can arise from an outside source paying the internal user, the termination gap where a terminated user still has access, or simply when human error comes into play. The financial industry, not unlike the healthcare industry, is rife with in- sider threats. While there is the obvious threat of those seeking financial gain, the financial industry is also prone to attack from nation-states, rival corporations, and cyber-espionage groups. That's a lot of darts getting thrown at one target.

Why is the finance industry at risk for insider threats?

On average, a financial services employee has access to nearly 11 million files the day they start work. Now expand that number across an organization or multiple organizations of the entire industry. It's unfathomable how many assets full of PII and other sensitive information (like bank account information) is being accessed at any given moment. Securing all those assets becomes a major challenge for financial organizations, and that's not even taking into account SOX 404, GLBA Safeguards Rule, and other regulatory demands. For hackers, it be- comes obvious that the fastest way in is through an internal user. Just look at PostBank, the South African post office bank that was forced to replace millions of bank cards at a cost of $58 million after an internal employee compromised customers bank data by copying a master key. That was just a compromise, not a full-fledged theft, and it still cost over $50 million. All it

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on Page 2

takes is one moment of human error, a moment of weakness, a well-placed phishing attack on an internal user with too much access to cause chaos. Not to mention that as financial institutions, like organizations in every industry, become more digitized and decentralized, they open themselves up to new threats and more vulnerable access points.

How the finance sector can stay safe from insider threats

There are a few building blocks of cybersecurity architecture that a financial organization can place to have a better founda- tion against mounting threats – both external and internal.

Create access policies that follow least privilege access. Your organization may not know who has access to what as- sets, but a hacker probably does. With malware, spyware, and other bugs gaining sophistication, it isn't a stretch for a deter- mined back actor to figure out which internal user has too much access and then target them with a phishing attack or straight- forward extortion. By never giving a user access to more than the minimum they need to do a task (and then deprovisioning that access after), an organization is preventing access creep and removing a potential attack surface.

Implement fine-grained controls that employ zero trust. The methodology behind access policies apply to access controls — trust no one. Internal users should be beholden to the same controls any external users are, and no one should be above that idea. From utilizing time-based controls to multi-factor authentication, a mix of access controls can prevent an attack before it even occurs.

Conduct regular access reviews. A user access review is a periodic inventory of access rights to certain networks and systems, and the users who have access permissions into those networks and systems. By regularly having IT and HR conduct those reviews, an organization can prevent access creep, the termination gap, or find credentials that were errantly given out. These kinds of reviews can also flag certain insider bad behavior like snooping. User access reviews also help a financial organization meet SOX compliance.

***Source:* Imprivata**

Three Types of Insider Threats

There are three common types of insider threats that financial companies and institutions face.

The first one is an intentional or malicious attack.

This is where some active employee has a grudge against the company, or turns traitor due to financial incentives or for some other reason. Then they use their legitimate credentials to attack the company.

For example, J.P. Morgan Chase's Peter Persaud sold personal identifying information (PII) and PIN numbers to outside parties, and many of the accounts were later targeted. Persaud received a sentence of four years in prison in 2018.

Or there's this case, where TD Bank employee Janelle Digby, a call center representative, worked with co-conspirators to hand over sensitive client information. Another party associated with Digby got people to open new accounts at the bank for the purposes of defrauding the institution and taking money out of the bogus accounts.

The second type of threat is an unintentional attack that can be called "negligent."

Here, employees aren't trying to hack the company, but the outsiders persuade them to turn over information through some kind of deceit or trickery.

How does this work? A telling case involving giant bank HSBC provides some detail. Here's how a reporter put it in coverage at the Royal Gazette in 2017:

"HSBC Bermuda yesterday apologized after it e-mailed personal information on customers to other account holders. The e-mails contained names, e-mail addresses, countries of residence, the name of the customers' relationship manager and HSBC customer identification numbers."

In these types of cases, the latent information can then be used by unscrupulous parties to conduct attacks, which is why HSBC's release was so grievous.

A third kind of insider threat involves recruitment where outsiders get insiders to flip or turn, to accomplish their objectives.

Late in 2021, the US District Court for the Eastern District of Virginia saw three men charged with money laundering and other crimes, in a case where they allegedly sent false emails to an employee so that they could get access to real transaction information. One of the accused reportedly was found to have worked at Bank of America for some time from 2015 to 2018. Coverage of this incident shows how the hackers had to deceive employees close to the banking transactions.

Whether it's a malicious insider attack, a case of negligence, or a recruiting setup, the results are still devastating, so businesses have to be on the lookout for all of these scenarios.

***Source:* Teramind**

12 Simple Things You Can Do to Be More Secure Online

1. Install an Antivirus and Keep It Updated

We call this type of software antivirus, but fending off actual computer viruses is just one small part of what they do. Ransomware encrypts your files and demands payment to restore them. Trojan horse programs seem like valid programs, but behind the scenes, they steal your private information. Bots turn your computer into a soldier in a zombie army, ready to engage in a denial-of-service attack, spew spam, or whatever the bot herder commands. An effective antivirus protects against these and many other kinds of malware.

In theory, you can set and forget your antivirus protection, letting it hum along in the background, download updates, and so on. In practice, you should look it over every now and then. Most antivirus utilities display a green banner or icon when everything is hunky-dory. If you open the utility and see yellow or red, follow the instructions to get things back on track.

One more thing. If your antivirus or security suite doesn't have ransomware protection, consider adding a separate layer of protection. Many ransomware-specific utilities are entirely free, so there's no reason not to try a few of them and select the one that suits you best.

2. Explore the Security Tools You Install

Many excellent apps and settings help protect your devices and your identity, but they're only valuable if you know how to use them properly. To get the maximum protective power from these tools, you must understand their features and settings. For example, your smartphone almost certainly includes an option to find it if lost, and you may have even turned it on. But did you actively try it out, so you'll know how to use it if needed?

Most antivirus tools have the power to fend off Potentially Unwanted Applications (PUAs), troublesome apps that aren't exactly malware but don't do anything beneficial. But not all of them enable PUA detection by default. Check the detection settings and make sure yours are configured to block these annoyances. Likewise, your security suite may have components that aren't active until you turn them on. When you install a new security product, flip through all the pages of the main window, and at least take a glance at the settings. If it offers an initial onboarding tour, don't skip it—rather, go through the tour methodically, paying attention to all the features.

3. Use Unique Passwords for Every Login

One of the easiest ways hackers steal information is by getting a batch of username and password combinations from one source and trying those same combinations elsewhere. For example, let's say hackers got your username and password by hacking an email provider. They might try to log into banking sites or major online stores using the same username and pass- word combination. The single best way to prevent one data breach from hav- ing a domino effect is to use a strong, unique password for every single online account you have.

Creating a unique and strong password for every account is not a job for a human. That is why you use the random password generator built into your password manager. Several very good password managers are free, and it takes little time to start using one. For-pay password managers generally offer more features, however.

4. Get a VPN and Use It

Any time you connect to the Internet using a Wi-Fi network that you don't own, you should use a virtual private network or VPN. Say you go to a coffee shop and connect to a free Wi-Fi network. You don't know anything about the security of that connection. It's possible that someone else on that network, without you knowing, could start looking through or stealing the files and data sent from your laptop or mobile device. The hotspot owner might be a crook, sniff- ing out secrets from all Wi-Fi connections. A VPN encrypts your internet traf- fic, routing it through a server owned by the VPN company. That means no- body, not even the owner of the free Wi-Fi network, can snoop on your data.

5. Use Multi-factor Authentication

Multi-factor authentication can be a pain, but it absolutely makes your accounts more secure. Multi-factor authentication means you need to pass another layer of authentication, not just a username and password, to get into your accounts. If the data or personal information in an account is sensitive or valuable, and the account offers multi-factor authentication, you should enable it. Gmail, Evernote, and Dropbox are a few examples of online services that offer multi-factor authentication.

Multi-factor authentication verifies your identity using at least two different forms of authentication: something you are, something you have, or something you know. Something you know is the password, naturally. Something you are could mean authentication using a fingerprint, or facial recognition. Something you have could be your mobile phone. You might be asked to enter a code sent via text or tap a confirmation button on a mobile app. Some- thing you have could also be a physical Security Key; Google and Microsoft have announced a push toward this kind of authentication.

6. Use Passcodes Even When They Are Optional

Apply a passcode lock wherever available, even if it's optional. Think of all the personal data and connections on your smartphone. Going without a passcode lock is unthinkable.

Many smartphones offer a four-digit PIN by default. Don't settle for that. Use biometric authentication when available, and set a strong passcode, not a stupid four-digit PIN. Remember, even when you use Touch ID or equivalent, you can still authenticate with the passcode, so it needs to be strong.

7. Pay With Your Smartphone

The system of credit card use is outdated and not very secure at all. That's not your fault, but there is something you can do about it. Instead of whipping out the old credit card, use Apple Pay or an Android equivalent everywhere you can. There are tons of choices when it comes to apps.

8. Use Different Email Addresses for Different Kinds of Accounts

People who are both highly organized and methodical about their security often use different email addresses for different purposes, to keep the online identities associated with them separate. If a phishing email claiming to be from your bank comes to the account you use only for social media, you know it's fake.

9. Clear Your Cache

Never underestimate how much your browser's cache knows about you. Saved cookies, saved searches, and Web history could point to home ad- dress, family information, and other personal data.

To better protect that information that may be lurking in your Web history, be sure to delete browser cookies and clear your browser history on a regular basis.

10. Turn Off the 'Save Password' Feature in Browsers

Speaking of what your browser may know about you, most browsers include a built-in password management solution.

11. Don't Fall Prey to Click Bait or Phishing Scams

Part of securing your online life is being smart about what you click. Clickbait doesn't just refer to cat compilation videos and catchy headlines. It can also comprise links in email, messaging apps, and Facebook. Phishing links masquerade as secure websites, hoping to trick you into giving them your credentials. Drive-by download pages can cause malware to automatically download and infect your device.

Don't click links in emails or text messages, unless they come from a source you trust. Even then, be cautious; your trusted source might have been compromised, or the message might be fake. The same goes for links on social media sites, even in posts that seem to be from your friends. If a post seems unlike the style of your social media buddy, it could be a hack.

12. Protect Your Social Media Privacy

There's a common saying: if you're not paying for a service, you're not a customer; you're the product. Social media sites make it easy for you to share your thoughts and pictures with friends, but it's easy to wind up sharing too much.

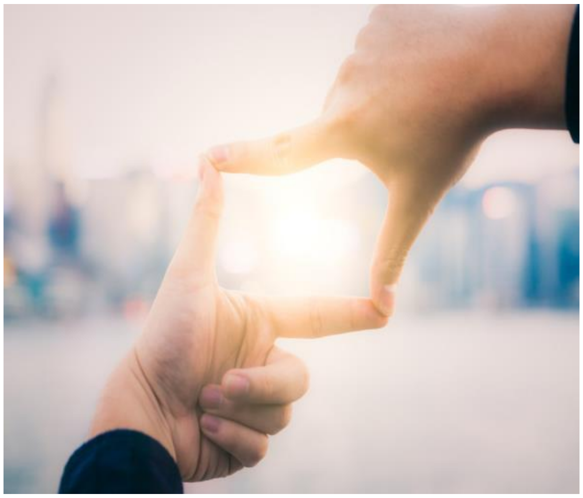
Source: PCMag, Neil J. Rubenking & Jill Duffy, Updated August 29, 2022

UNION BANK

March 2023

How To Shop Online Safely (Without Getting Scammed)

Can You Get Scammed While Shopping Online?



Online shopping is convenient and easy. But is it safe?

According to the FBI, the second most common internet crime of 2021 was related to online shopping — non-delivery of goods purchased. Just last year, online shoppers lost $337 million to fraudulent online stores.

Fraudsters create fake online stores and then use social media ads to lure you in to become a customer. But the products either don't arrive, aren't what you expected, or come with huge hidden fees.

But it doesn't stop with fake products and unreasonable fees. Shopping from fake online stores can also lead to identity theft.

Criminals use the information you provided — like your name, address, and credit card details — to take over your identity, drain your bank account, and commit financial fraud.

But this doesn't mean you need to give up shopping online entirely. Here are some essential steps to take to ensure you're getting a great deal and not a scam while shopping online.

What Are the Most Common Online Shopping Scams?

Unfortunately, there are more online shopping scams than ever.

According to the Better Business Bureau's (BBB) 2021 Online Purchase Scams Report, 79% of victims lost money — making online shopping the riskiest scam type of all.

So, how are fraudsters trying to scam you while you shop online?

- **Fake online stores**: The most common online shopping scam is when fraudsters create a fake shopping website or app. These sites may look legitimate, but they're designed to steal your sensitive information and credit card numbers.
- **Using Instagram and Facebook ads to fool you**: According to one study, 40% of all online shopping scams come from Facebook and Instagram ads. These flashy ads often use hacked accounts and stolen photos, but the products either don't arrive or are cheap knockoffs of what was advertised.

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

- Selling discounted “luxury” goods: Many online shoppers are scammed by looking at deals that are too good to be true. Crimi- nals create ads for steeply discounted luxury items like designer sunglasses or bags. But the items either don’t arrive or are counterfeit. Be especially careful when shopping for popular or difficult-to-find items.
- Sending shipping notifications for products that never arrive: The COVID-19 pandemic has caused significant shipping delays for almost all online retailers. One common Covid Scam is when scammers use this to their advantage and send fake shipping “updates” to stop you from reporting their scam.
- Using fake reviews to make you think they’re a legitimate site: Most of us believe an online store if they have reviews. But scammers use what’s called a brushing scam to create fake reviews on sites like Amazon or eBay.

These online shopping scams can appear in legitimate search results, pop up while you’re on social media, or get shared by friends.

14 Essential Tips for Shopping Online Safely

1. **Buy from online retailers you recognize**
2. **Choose stores that use secure websites**
3. **Scrutinize the details of any online store**
4. **Insist on using safe payment services**
5. **Learn the warning signs of a scam email**
6. **Always check shipping costs and terms**
7. **Never store your credit card details with a store**
8. **Create strong, secure passwords**
9. **Monitor your credit and bank statements**
10. **Check to see if your account details were leaked**
11. **Secure your devices with antivirus software**
12. **Watch your back when shopping in public**
13. **Use official shopping apps**
14. **Sign up for identity theft protection**

Were You Scammed by an Online Store? Here’s What To Do

Even if you’re careful, online shopping scammers are getting better at tricking you. If you’ve given your financial and personal information to a fake store, here’s what to do next:

- **Check your insurance policy.** If you’re signed up for identity theft protection, you should have access to a fraud resolution team that can handle many of the next steps for you. Some companies also offer identity theft protection as part of their benefits package.
- **Notify your bank and credit card company.** Contact your bank and any lenders to let them know that your identity has been stolen and to stop fraudulent transactions. They’ll close your accounts and help you open new ones.
- **File an official identity theft report with the FTC.** Go to IdentityTheft.gov and file an official report with the FTC. This is an essential step if you need to dispute fraudulent charges.
- **File a police report.** You can also file a police report for identity theft with your local law enforcement agency. This is an optional step. But you should do it if you have any information about the scammer that could help lead to their arrest.
- **Regularly check your credit report and bank statements.** Scammers are almost always after your financial accounts. Check for the warning signs of identity theft — such as strange charges on your bank statement or accounts you don’t recognize. An identity theft protection service can monitor your credit and statements for you and alert you to any signs of fraud.
- **Set up a fraud alert on your credit report.** Contact one of the three credit reporting bureaus — Experian, Equifax, or TransUnion — and alert them of the fraud. They’ll set up a fraud alert to protect your credit score from the scammers.
- **Change your online passwords.** If one of your accounts has been compromised, you can assume others are too. Up- date all of your passwords (especially for sites where you’ve used your credit card).
- **Dispute fraudulent charges and new accounts.** Contact any company where fraud has occurred and let them know what happened. They’ll request your FTC report and then cancel any outstanding fraudulent debts.
- **Let others know about the scam.** Online shopping scams only work if no one speaks up. Send a report to the BBB’s Scam Tracker and post negative reviews and comments on shopping sites where you were scammed.
- **Consider signing up for identity theft protection.**

The Bottom Line: Shop Safely Online All Year Round

Online shopping scams are rampant during the holiday season. But that’s not the only time to be careful. Any time you provide your banking information online is an opportunity for a scammer to strike.

Source: Aura

Be cyber secure: Do’s and don’ts for your family

Advice for helping protect yourself and your family from cyber threats

ODDS ARE YOU WOULDN’T DISCLOSE personal details, like when you’re planning to go on vacation and leave your house empty, to a random stranger on the street. But many people happily post that sort of information on their social feeds for anyone to see — and if you aren’t divulging your family’s schedule (and secrets) online, your teens just might be. Review the following do’s and don’ts to help you and your family stay safe in today’s super-connected world.

DO educate your family about cyber risks.

Children may not understand the risks of the online world. It's up to parents to teach them the dangers of sharing photos and personal information, like vacation routines or daily schedules — information that could be used by others to harm them. Teach them, too, that it’s a good practice to avoid downloading apps from obscure or untrustworthy developers and playing games or taking online surveys that ask for personal information.

DO keep your personal info private.

Be careful about sharing valuable personal information, such as Social Security numbers, credit card information and birth dates, in a text or email with people you don’t know well or trust. If you are shopping online, ensure you are on a reputable site before entering any sensitive information. And use a strong password, passcode or biometric login to protect your accounts online.

DO consider setting up a VPN.

A virtual private network (VPN) is a tool that encrypts your communications, from banking to shopping to tex- ting to emailing, when you're connecting to the internet via Wi-Fi. Best of all, it can be used anywhere in the world. Setting one up can be easy and affordable, but it’s important to choose a VPN you can trust. Talk with a security expert to determine which is best for you. Be aware, though, that you may have difficulty accessing some financial firms’ websites through a VPN because of the anti-fraud protections they’ve put in place. If you en- counter that problem, turn off your VPN and move to a location where you can use a secure, trusted internet connection.

DON’T leave your home network unprotected.

Be sure to change the password on your router as soon as you install it. The router is the gateway to your home and touches all of your connected devices, from phones to smart home gadgets. Also, don’t forget to configure security and privacy settings on your devices, and invest in reputable antivirus software for your computers. Download software updates on all the programs you use — automatically, if that’s an option. Software companies often discover vulnerabilities before cyber criminals do and rush to fix them. The longer you wait to update your software (or operating system), the greater the chance you’ll be targeted.

DON’T drop your guard on public Wi-Fi.

We’re so used to using our devices everywhere (or so concerned about hitting the data cap from our cell phone provider) that most of us don’t think twice about logging on to the free public Wi-Fi system at the airport, coffee shop or dentist’s office. Some Wi-Fi connections can’t be trusted; cyber criminals can infiltrate these systems and collect data that’s sent through them. That’s why it’s always best to take the precaution of connecting to sites through secure connections or a VPN.

DON’T use easily guessed passwords.

Despite repeated advice from all corners, some people still use the most basic of passwords for their email, shopping and financial accounts. Or worse, they use the same password for all of their online accounts, making those accounts especially vulnerable to cyber criminals. Variety and randomness are your best bets, so if one password is discovered, your other accounts won’t be at risk. Even better, consider using a password manager, which assigns a random password to accounts. That way you only have to remember a single master password — for the manager itself. (You can find password managers in your app store.) For tips on creating your own strong passwords, read “Be cyber secure: Hone your password-writing skills with this quiz.”

If you suspect that you or a family member has been targeted by cyber criminals, read “Cyber security checklist: Consider taking these steps if your family’s devices have been targeted.”

Source:* *Merrill

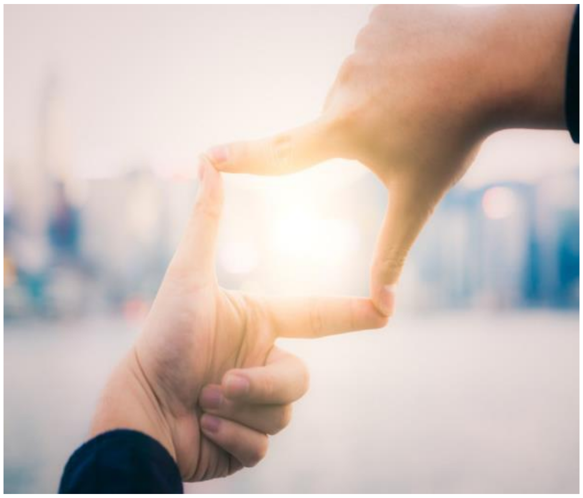
> ***Children may not understand the risks of the online world. It’s up to parents to teach them the dangers of sharing photos and personal information.***

UNION BANK

April 2023

How to Stop Those Annoying Spam Calls You Get Every Day

You shouldn't be afraid to pick up your phone.



You probably receive a handful of calls every day. Not from friends or family, but from scammers and telemarketers, notifying you that you've "won tickets to Hawaii" or pretending to be the IRS and threatening you so you'll pay up.

In January 2023 alone, Americans received 5.51 billion robocalls, which is nearly 20 spam calls for every single person in the US, according to Robokiller, a company that specializes in blocking spam calls and robocalls.

And these calls come in all shapes and sizes. You're likely familiar with the good ol' "scam likely" calls, but there are also more sophisticated attacks that involve spoofing local numbers and those of popular companies, to convince you to give up your personal information and cash. More recently, these attacks have moved over to SMS, where there are phishing text messages that come from your own phone number.

No matter what the calls say, one thing is certain -- they need to stop.

Over the last couple of years, the Federal Communications Commission aimed to wrangle the robocall problem by requiring major wireless carriers to start using Stir/Shaken technology. Stir/Shaken verifies all incoming and outgoing calls for wireless carriers that are routed through their networks. By verifying each call, carriers can reduce the number of fake or spoofed calls. But it only stops robocalls on one avenue -- it's not the be-all and end-all. You may still get spam calls for free trips or fake notices that your student loan payment is overdue.

You can read more about Stir/Shaken here. As the FCC continues its crusade, keep reading this story for things you can do to help curb the number of times your phone rings throughout the day with calls from potential fraudsters.

How to keep annoying robocalls at a minimum

According to the FCC, there are some easy steps you can take to help reduce robocalls:

- Don't answer calls from blocked or unknown numbers.
- Don't answer calls from numbers you don't recognize.
- Don't assume an incoming call is really from a local number just because it looks like itis.

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

- Don't respond to any questions that can be answered with a "Yes."
- If someone calls you and claims to be with XYZ company, hang up and call the company yourself. Use the company's website to find an official number.
- If you do answer a call and hear a recording such as, "Hello, can you hear me?" just hang up.
- The same goes for a call where you're asked to press a number before being connected to a representative.

When you answer a call and interact with the voice prompt or by pressing a number, it lets spammers know your number is real. They can then sell your number to another company or begin targeting your number more frequently.

When it first launched, Google's Call Screen feature arguably went against the FCC's advice by answering and interacting with the robocall on your behalf. However, Google added new features to Call Screen for its Pixel phone lineup. The feature can now detect robocalls and spam calls and block them before they reach you. Google Assistant will interact with the caller, and if it determines that the call is legitimate, it will route the call to your phone.

Apple's iPhone has an option to Silence Unknown Callers, which adds the option to route calls from numbers not found in your Contacts, Mail or Messages straight to voicemail. Any legitimate callers can leave a message. But that's the rub: We often receive important calls from numbers we don't store on our phones, like a doctor's office or a repairman, so you could miss important calls this way. But if all else fails and you're desperate to stop robocalls, this is a valid option.

If you find yourself receiving a lot of spam text messages, you can forward the message to the number 7726 (which spells "spam"). It won't stop the number from texting you right away, but it will allow your carrier to look into where it came from and put an end to it.

Check with your wireless carrier

All four major wireless carriers offer some sort of call-blocking feature. All have a free option and a premium tier.

AT&T ActiveArmor is available for iOS and Android. The free version blocks spam and fraud calls and provides nuisance warning labels and a personal block list, and you can block all unknown callers. AT&T's paid ActiveArmor Advanced offers additional benefits of caller ID for unknown numbers, reverse number lookup, identity monitoring and public Wi-Fi protection.

Verizon's Call Filter app is automatically enabled for Android users on a postpaid plan. The service offers spam detection, a spam filter, a call log for blocked or spam calls, the ability to allow calls from specific numbers (iOS only) and the option to report numbers for free. For a fee, you can get caller ID, spam lookup, a personal block list and a spam risk meter. Call Filter is built into most Android devices out of the box but is also available in the App Store for iOS users.

T-Mobile's Scam Shield is free to all customers and includes multiple features designed to protect you from robocalls and sharing your personal information. Dial #662# from your phone to turn on Scam Block, or download the free Scam Shield app in your phone's respective app store. With Scam Shield enabled, you'll get full caller ID, scam reporting, scam blocking before your phone ever rings and the option to mark numbers as favorites so they still ring your phone.

Use a third-party app to limit the number of robocalls you get

If your provider doesn't offer an app or service to cut back on robocalls, or does but it's too expensive, there are plenty of third-party apps available. You want to find an app that works on your device, offers automatic call blocking and spam alerts for suspicious calls and makes it easy to report a number if a call slips through.

Some options are:

Hiya
Nomorobo
YouMail
RoboKiller
Firewall app

Another option is to get a free Google Voice phone number that you can use to sign up for things instead of giving out your real number -- and once the robocalls start coming in on that Google Voice number, use the block feature. Just know that blocking calls may end up being a lot of work, as robocallers are constantly spoofing different phone numbers.

None of the above solutions is perfect, but they supplement your carrier's integration of technology now required to check for caller ID spoofing. So right now you have to do some extra work to keep the number of robocalls you receive to a minimum. Between being cautious about calls from unknown numbers and using a service (paid or free), you can reduce the amount of unwanted calls and spam you have to deal with.

In sum, carriers have started using Stir/Shaken technology to verify callers, which so far hasn't significantly cut down on the number of robocalls we all receive. So for those with an iPhone, learn where the setting is to block unknown callers, but remember using it could mean you miss calls from doctors' offices and the like. And for those with a Pixel phone, Google's Call Screen feature will surely help, and may even entertain you.

Source: cnet.com, Jason Cipriani, Nelson Aguilar, Feb. 8, 2023

Tax season update: beware of email, text scams

The Internal Revenue Service (IRS) is urging taxpayers to be mindful of scammers using emails and text messages to trick people into providing their personal and tax information. In a press release issued this week, the IRS warned against clicking on or opening emails or text messages claiming to be from the agency, as the IRS never "initiate contact with taxpayers by email, text or social media regarding a bill or tax refund." We're sharing the full press release below for your convenience:

WASHINGTON – With the filing deadline quickly approaching, the Internal Revenue Service today urged everyone to remain vigilant against email and text scams aimed at tricking taxpayers about refunds or tax issues.

In day two of the annual Dirty Dozen tax scams campaign, the IRS again includes a warning about phishing and smishing schemes where cybercriminals try to steal a taxpayer's information through scam emails or text messages.

"Email and text scams are relentless, and scammers frequently use tax season as a way of tricking people," said IRS Commissioner Danny Werfel. "With people anxious to receive the latest information about a refund or other tax issue, scammers will regularly pose as the IRS, a state tax agency or others in the tax industry in emails and texts. People should be incredibly wary about unexpected messages like this that can be a trap, especially during filing season."

As a member of the Security Summit, the IRS, with state tax agencies and the nation's tax industry, have taken numerous steps over the last eight years to warn people to watch out for common scams and schemes each tax season that can contribute to identity theft. Along with the Security Summit initiative, the Dirty Dozen aims to protect taxpayers, businesses and the tax system from identity thieves and various hoaxes designed to steal money and information.

The Dirty Dozen is an annual IRS list of 12 scams and schemes that put taxpayers and the tax professional community at risk of losing money, personal data and more. Some items on the list are new, and some make a return visit. While the list is not a legal document or a formal listing of agency enforcement priorities, it is intended to alert taxpayers, businesses and tax preparers about scams at large.

Phish or smish: Avoid getting hooked by either

Taxpayers and tax professionals should be alert to fake communications posing as legitimate organizations in the tax and financial community, including the IRS and states. These messages arrive in the form of an unsolicited text or email to lure unsuspecting victims to provide valuable personal and financial information that can lead to identity theft. There are two main types:

- **Phishing** is an email sent by fraudsters claiming to come from the IRS or another legitimate organization, including state tax organizations or a financial firm. The email lures the victims into the scam by a variety of ruses such as enticing victims with a phony tax refund or frightening them with false legal/criminal charges for tax fraud.

- **Smishing** is a text or smartphone SMS message that uses the same technique as phishing. Scammers often use alarming language like, "Your account has now been put on hold," or "Unusual Activity Report" with a bogus "Solutions" link to restore the recipient's account. Unexpected tax refunds are another potential target for scam artists.

The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund.

Never click on any unsolicited communication claiming to be the IRS as it may surreptitiously load malware. It may also be a way for malicious hackers to load ransomware that keeps the legitimate user from accessing their system and files.

Individuals should never respond to tax-related phishing or smishing or click on the URL link. Instead, the scams should be reported by sending the email or a copy of the text/SMS as an attachment to phishing@irs.gov. The report should include the caller ID (email or phone number), date, time and time zone, and the number that received the message.

Taxpayers can also report scams to the Treasury Inspector General for Tax Administration or the Internet Crime Complaint Center. The Report Phishing and Online Scams page at IRS.gov provides complete details. The Federal Communications Commission's Smartphone Security Checker is a useful tool against mobile security threats.

The IRS also warns taxpayers to be wary of messages that appear to be from friends or family but that are possibly stolen or compromised email or text accounts from someone they know. This remains a popular way to target individuals and tax preparers for a variety of scams. Individuals should verify the identity of the sender by using another communication method; for instance, calling a number they independently know to be accurate, not the number provided in the email or text."

Read the IRS press release to learn more.

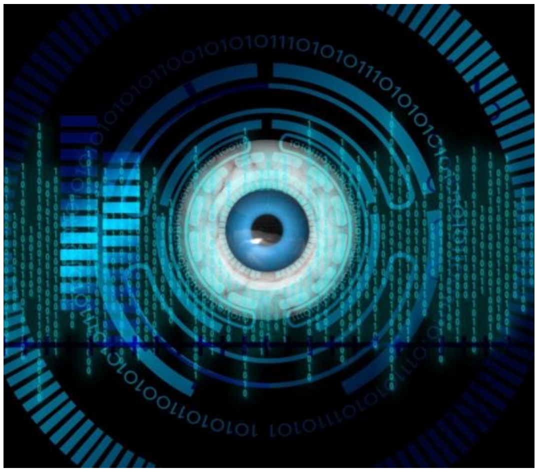
Source: ***City of Philadelphia, Fatoumata Fofana-Bility , March 23, 2023***

Mobile Banking App is HERE!

UNION BANK

May 2023

Biometrics – Making Security Simple



Overview

Do you hate passwords? Are you tired of constantly logging into new websites or can't remember all of your complex passwords? Frustrated by having to generate new passwords for new accounts or having to change old passwords for existing accounts? We have good news for you. There is a solution called biometrics that helps make cybersecurity easier for you. Below we explain what biometrics are, how they make your life simpler and why you will start seeing more of them.

First, Why Password?

Passwords are part of something called authentication, the process of proving who you are. There have typically been two things you can provide to prove your identity: something you know (like your passwords) and something you have (like an ATM card or your mobile device). Traditionally authentication has been done with passwords. Passwords were first adopted as it was one of the easiest authentication solutions to deploy. However, over the years our lives have become far more complicated with far more accounts than anyone ever expected. It is quite common for a person to have over 100 passwords in their work and personal life.

In addition, cyber attackers have become quite good at guessing, stealing or cracking passwords. This is why you see so many rules about passwords, such as making them long (so they are hard to guess) and using a unique password for every account (so if one of your accounts is hacked, your other accounts are still safe). The problem with all of the password requirements is they make being cybersecure more difficult. Password managers dramatically help as they securely remember all of your passwords and log you into websites for you, but is there a better way? This is where biometrics can help by providing a third thing to prove your identity–something you are.

Biometrics

Like passwords, biometrics are another way to prove who you are. The difference is instead of having to remember something (like your passwords) you use an element of who you are to prove your identity, such as using your fingerprint to gain access to your phone. Biometrics are much simpler as you don't have to remember or type anything, you just authenticate using who you are. There are many different types of biometric such as your voice, how you walk, or your iris prints. However, fingerprints and facial recognition are the two most common, especially for mobile devices. While biometrics have a tremendous number of advantages, they also have some disadvantages, one of the biggest being if your fingerprint or face is copied by cyber attackers, you cannot change them.

Passkeys

Over the coming months and years, you should start seeing biometrics replacing passwords with a new

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on Page 2

technology called Passkeys. This technology is being adopted by Microsoft, Apple and Google and you should soon see it being adopted at more and more websites over time. Passkeys replace passwords by allowing you to prove who you are by simply using biometrics combined with your mobile device. When you create an account at a website (such as Google or Apple) instead of creating a password you register your mobile device. Moving forward you log into that website by authenticating with your mobile device using biometrics, such as your fingerprint or facial recognition. The website trusts your mobile device, and your mobile device confirms it's you using biometrics. In addition, your biometric data (fingerprint or face) is not sent to any website. Instead, your biometrics is securely stored locally on your device. It's just used to unlock the "Passkey", a unique key, created for each site, which your device sends to the site while protecting your biometric data. While no solution is perfect, biometrics and solutions like Passkeys can help keep you secure while simplifying security.

Sources:
Article: *Dr. Johannes Ulrich, Dean of Research for the SANS Technology Institute college, SANS OUCH! Newsletter, January 4, 2023*
Images: *Gerd Altmann, Public Domain Pictures*
Pete Linforth, Pixaby

The Use of Biometrics Technology in Everyday Life

Biometrics has become a buzzword in the last few years, gradually becoming one of the most important industries in the digital universe. According to MarketsandMarkets, the global biometric technology market is expected to grow from USD 42.9 billion in 2022 to USD 82.2 billion by 2027. Increasing advancements in biometric technology across various sectors, rising demand for authentication and identification solutions, and security surveillance solutions are the primary factors driving the market growth.

But what makes this technology so important? How does it affect the world as we know it? While most people believe biometric technology is jeopardizing personal security and privacy, the fact remains that it brings substantial benefits to our everyday lives for a few reasons:

Biometrics ensures accuracy.

- The system eliminates the vast majority of safety threats.
- Many biometrics solutions are cost-effective.
- It is easy to use.
- User acceptance is increasing

Here are some common uses for biometrics in everyday life:

Airport Security

Biometric systems have been in use at airport for quite some time. As facilitating passengers' passage through airports is a universal priority, some of the world's largest airports have utilized biometric technology to verify passenger identities for many years, and this practice is gradually spreading.

Law Enforcement

Biometrics is widely used across law enforcement, with agencies such as the FBI and Interpol utilizing biometrics in criminal investigations. M2SYS technology has been working with law enforcement agencies worldwide to deliver biometric solutions to identify criminals in the last two decades. A collection of solutions designed to meet government law enforcement agency identification & data management requirements while delivering fast, secure, and reliable results.

School

Many developing countries have already implemented biometric technology on school premises. It is also a growing technology that other countries follow to implement in the education sector. Authorities of educational institutes are implementing biometric identification for several reasons. These reasons are mainly segregated into two — one is for internal control, and the other to ensure safety and security. In recent years, many unwanted incidents, like terrorist attacks, vandalism, and mass shootings, have been taking place in educational institutions worldwide, influencing us to rethink security measures in schools, colleges, and universities.

Hospitals

In modern hospitals and clinics, biometric identification is utilized for secure, reliable access to patient's medical records and personal information. The patient's medical history is protected, and no duplicate is created, greatly assisting the healthcare industry. In addition to saving the lives of unconscious patients, quick identification with biometric technology lets hospitals make better treatment decisions based on patient's medical histories.

Blood Collection

Blood is collected from donors and stored in blood banks. However, there are still significant dangers associated with receiving blood from professional or proxy donors. Instead of saving lives, blood donations could take one if the donor isn't adequately screened. Because of this, blood banks now use biometric identification technology to enroll donors, keep track of their medical history, and screen out unqualified donors.

Summary

Whether we like it or not, biometrics are becoming a fundamental part of our daily lives. Many of us will rely on biometrics as a standard method of gaining access to the many products and services we use daily as technology advances. M2SYS aims to simplify the whole process, so anyone can access it without breaking the bank. All you need is to contact us. We'll give you the whole "Turnkey" solution according to your requirement.

Source: *Stanly Palma, M2SYS*

Top Tips for Spotting Deepfakes Online

Deepfakes—digital manipulations of media that use artificial intelligence to create realistic, altered images or videos—can be used to create seemingly genuine footage of people saying or doing things that they never actually said or did.

Researchers, visual effects specialists, amateur enthusiasts, and even porn producers are all creating deepfakes now. It's also possible that political parties and governments are producing deepfakes to try to discredit extremist groups or opponents.

While deepfakes have the potential to revolutionize certain industries, they also pose significant risks to society. Nefarious parties can easily spread misinformation and propaganda using deepfake technology, potentially leading to harmful consequences.

It's important that we, as internet users, build our digital literacy skills so we can successfully navigate our online world—in everyday life, in education, and at work.

A big part of digital literacy is learning how to think critically about what we see and hear online. One important digital literacy skill is being able to identify and debunk deepfake content to protect ourselves and others from being misled.

How to spot a deepfake

If you'd like to see some very convincing deepfake videos, you can look at this Morgan Freeman video from Dutch YouTube creator Diep Nep, or check out the series of fake Tom Cruise videos from visual and AI effects artist Chris Umé.

There are positive uses for deepfake technology—like creating digital voices for people, or updating film footage instead of reshooting—however, as the tools get more sophisticated, the potential for malicious use of deepfakes is concerning.

For example, if malicious actors were to present a deepfake of a world leader as a genuine communication, it could pose a threat to global security. Given the speed at which "fake news" can spread around the world, there is a real threat that people or organizations could use deepfakes to manip- ulate public opinion and deceive others into believing they are authentic representations.

Here are 4 things to look for if you suspect you might be looking at a deepfake:

Unnatural facial or eye movements

It's difficult for deepfake producers to accurately reproduce eye or facial movements and imitate the ways humans blink. When examining questionable videos, look for strange eye movements or a face that doesn't display nor- mal-looking emotions that match what's being said.

Mismatches in lighting and color

Does the skin tone of the person in the video look odd? Is the lighting peculiar, or are there strangely-positioned shad- ows on the person's face? Take note of discrepancies in the video, and if possible, compare the lighting and color to an original reference photo or video.

Poor audio quality

Producers of deepfake videos often focus more on visuals than on sounds, so watch out for poor lip-syncing, strange word pronunciation, robotic-sounding voices, or digital background noise.

Problems with body movement

If the person in the video appears distorted when they turn to the side or move their head—or if their movements look disconnected or choppy from one frame to the next—you might be looking at a deepfake video.

Awkward posture

Deepfake technology often concentrates on facial features rather than on the entire body, so it can be easy to detect body position and posture anomalies.

If the person's body shape doesn't look natural in the video, or if their body or head is positioned inconsistently or awkwardly, you could be looking at a deepfake video.

Deepfakes are not a passing trend and will be a continuing presence online. As deepfake technology continues to advance, it will become even more important for audiences to be vigilant in identifying fake videos so they don't fall victim to manipulation.

***Sources: Article:** Bernard Marr, Readers Digest, January 27, 2023*
***Image:** Gerd Altmann, Public Domain Pictures*

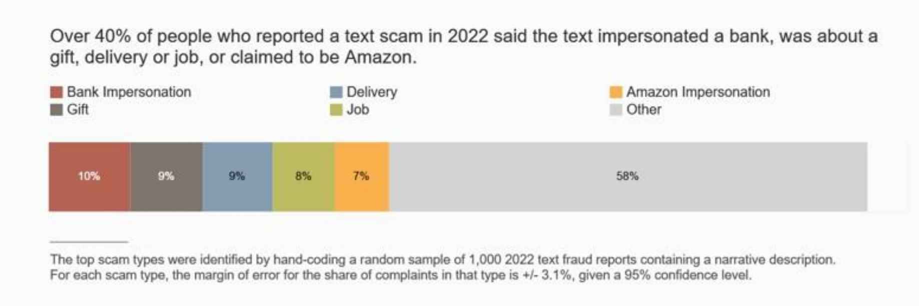
UNION BANK

June 2023

Can You Spot the 5 Most Common Text Message Scams?

According to reports in the FTC’s Consumer Sentinel database, text message scams took consumers for $330 million in 2022. The latest Consumer Protection Data Spotlight focuses on this form of fraud. With reported losses more than doubling in 2021 and nearly five times what people reported in 2019, would you be able to spot the five most common text message scams?

First, some background about what may be behind the proliferation of this form of fraud. It’s estimated that text message open rates are as high as 98%, compared to email open rates of 20% – and they cost next to nothing to send. So people may have grown accustomed to responding to that ping with an automatic click. The growth of text scams should be of particular concern to businesses. Aside from the fact that your family and friends may be among the consumers who have reported median personal losses of $1,000, a lot of the messages take on a distinctly “office-y” tone that may target staff – fake deliveries, bogus job offers, and the like. It should also concern businesses that scammers often do their dirty work by stealing the names of well-known companies, with 51% of reports of text fraud categorized in Consumer Sentinel as business imposters.


Over 40% of people who reported a text scam in 2022 said the text impersonated a bank, was about a gift, delivery or job, or claimed to be Amazon.

The top scam types were identified by hand-coding a random sample of 1,000 2022 text fraud reports containing a narrative description. For each scam type, the margin of error for the share of complaints in that type is +/- 3.1%, given a 95% confidence level.

The Data Spotlight focuses on these five common text message scams:

1. Copycat bank fraud prevention alerts. According to the Data Spotlight, reports about texts impersonating banks are up nearly twentyfold since 2019 with median reported individual losses of $3,000 last year. People get a text supposedly from a bank asking them to call a number ASAP about suspicious activity or to reply YES or NO to verify whether a transaction was authorized. If they reply, they’ll get a call from a phony “fraud department” claiming they want to “help get your money back.” What they really want to do is make unauthorized transfers. What’s more, they may ask for personal information like Social Security numbers, setting people up for possible identity theft.

2. Bogus “gifts” that can cost you. What about those texts claiming to be from a well-known company offering a free gift or reward? If people click the link and use their credit card to cover the small “shipping fee,” they’ve just handed over their account information to a scammer. Reports to Consumer Sentinel tell us that fraudulent charges are likely to follow.

3. Fake package delivery problems. On any given day, what home or business *isn’t* expecting a delivery? Scammers understand how our shopping habits have changed and have updated their sleazy tactics accordingly. People may get a text pretending to be from the U.S. Postal Service, FedEx, or UPS claiming there’s a problem with a delivery. The text links to a convincing-looking – but utterly bogus – website that asks for a credit card number to cover a small “redelivery fee.”

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office

103 Dodd Street Middlebourne, WV 26149

304-758-2191

Sistersville Office

700 Wells Street Sistersville, WV 26175

304-652-3511

St. Marys Office

401 Second Street St. Mary's, WV 26170

304-684-2427

Hundred Office

3924 Hornet Hwy, Hundred WV 26575

304-775-2265

Ellenboro Office

90 Main Street Ellenboro, WV 26346

304-869-3232

Harrisville Office

1500 E. Main Street Harrisville, WV 26362

304-643-2974

Pennsboro Office

214 Masonic Ave. Pennsboro, WV 26415

304-659-2964

Marietta-Loan Production

Kroger Plaza 19 Acme Street Marietta, OH 45750

740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office

638 N SR 2 New Martinsville, WV 26155

304-455-2967

Continued on Page 2

4. Phony job offers. With workplaces in transition, some scammers are using texts to perpetrate old-school forms of fraud – for example, fake “mystery shopper” jobs or bogus money-making offers for driving around with cars wrapped in ads. Other texts target people who post their resumes on employment websites. They claim to offer jobs and even send job seekers checks, usually with instructions to send some of the money to a different address for materials, training, or the like. By the time the check bounces, the person’s money – and the phony “employer” – are long gone.

5. Not-really-from-Amazon security alerts. People may get what looks like a message from “Amazon,” asking to verify a big-ticket order they didn’t place. Concerned about the security of their account, people call the number in the text and are connected to a phony Amazon rep who offers to “fix” their account. But oopsie! Several zeroes are mistakenly added to the “refund” and the “operator” needs the caller to return the overpayment, often in the form of gift card PIN numbers.

According to the Data Spotlight, reporting can help stop scam text messages. Forward the text to 7726 (SPAM). This helps your wireless provider block similar messages. Report it on either the Apple iMessages app or Google’s Messages app for Android users. And report it to the FTC at

ReportFraud.ftc.gov.

Here is additional advice for you:

- Don’t click on links or respond to unexpected texts. If you aren’t sure if a text legit, contact the company directly using a phone number or website you know is real – for example, the 24-hour toll-free number on the back of your credit or bank card. Don’t use the information in the text message.
- Filter unwanted texts before they reach you. The FTC has advice on blocking unwanted texts.

Sources/Credit:

Article: Lesley Fair, June 8, 2023, FTC.gov

Images: Chart: FTC.gov; Traffic Sign: Author: geralt, Attribution: Pixabay, License Details: Pixabay Terms of Service; Traffic Signs Attention A Notice royalty-free stock illustration. Free for use & download

What To Do if You Were Scammed

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. And they're good at what they do. Here’s what to do if you paid someone you think is a scammer or gave them your personal information or access to your computer or phone. If you paid a scammer, your money might be gone already. No matter how you paid, it’s always worth asking the company you used to send the money if there’s a way to get it back.

Here are some steps to take if you unwittingly paid a scammer:

Did you pay with a credit card or debit card?

Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.

Did a scammer make an unauthorized transfer from your bank account?

Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.

Did you pay with a gift card?

Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.

Did you send a wire transfer through a company like Western Union or MoneyGram?

Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

- MoneyGram at 1-800-926-9400
- Western Union at 1-800-448-1492
- Ria (non-Walmart transfers) at 1-877-443-1399
- Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144

Did you send a wire transfer through your bank?

Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

Did you send money through a money transfer app?

Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

Did you pay with cryptocurrency?

Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back. But contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible.

Did you send cash?

If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics.

If you used another delivery service, contact them as soon as possible.

For more information, check out the FTC’s Consumer Advice website.

Are Public Wi-Fi Networks Safe? What You Need To Know

Public Wi-Fi networks, or hotspots, in coffee shops, malls, airports, hotels, and other places are convenient. In the early days of the internet, they often weren't secure. But things have changed. Here's what you need to know about your safety when you connect to a public Wi-Fi network.

How You Know Your Information Is Safe When You're Using a Public Wi-Fi Network

When you connect to a website, information travels from your device to the website. That could include sensitive data like the log in information for your financial, email, or social media accounts.

In the past, if you used a public Wi-Fi network to get online, your information was at risk. That's because most websites didn't use encryption to scramble the data and protect it from hackers snooping on the network.

Today, most websites **do** use encryption to protect your information. Because of the widespread use of encryption, connecting through a public Wi-Fi network is usually safe.

How do you know your connection is encrypted? Look for a lock symbol or https in the address bar to the left of the website address. This works on a mobile browser, too. It can be hard to tell if a mobile app uses encryption, but the majority do.

Best Practices for Protecting Your Personal Information Online

No matter how you get online, it's always a good idea to take some steps to protect your personal information. Start with these.

Protect your online accounts and devices

Create and use strong passwords and turn on two-factor authentication when it's available.

If you use a computer to get online, make sure your security software, operating system, and internet browser are up to date. Update your phone's operating system, too. And turn on automatic updates to keep up with the latest protections.

Recognize scammers

Scammers pretend to be someone they're not, like a representative from a well-known company or the government, to rip you off or steal your personal information. They also create fake websites and encrypt them to make you think they're safe when they're not. If you visit a scammer's website, your data may be encrypted on its way to the site, **but it won't be safe from scammers operating the site**.

Report Scammers

Report scammers to the FTC at ReportFraud.ftc.gov.

Sources: Article: FTC.gov Consumer Advice, February 2023

Image: Creator: User ID: 472301; Attribution: Pixabay; License Details: Pixabay Terms of Service; Wireless Technology Three Dimensional Shape royalty-free stock illustration. Free for use & download

Mobile Banking App is HERE!

UNION BANK

July 2023

Identity Theft Statistics to Keep in Mind

It seems like only yesterday the word “theft” brought to mind visions of home breaches or street muggings. While these weren’t exactly harmless, they were at least evils we could see. With ID theft the new big thing, similar risks are largely out of sight.

Here’s the deal:

As a quick look at the latest identity theft stats reveals, breaches can now come from all angles, and controlling them isn’t as easy as installing CCTV. As we share ever more data online, we’re all increasingly at risk of third-parties.

Now:

While identity theft statistics may be enough to put the fear in you, they’re crucial to consider. Understanding the numbers behind crimes like these is, after all, our best chance at staying safe!

ID theft occurs when someone steals another person’s sensitive personal information. It’s slightly different from ID fraud, which involves the actual use of someone else’s sensitive information in a fraudulent or deceptive way.

To get a thorough look at identity theft patterns over the last year, we analyzed recent relevant data from the Federal Trade Commission and other government agencies that deal with theft and fraud. We’ve outlined these insights in a more digestible format below.

Key insights

- Recorded instances of identity theft have soared by 584% over the last 20 years. In the last decade, Louisiana, Delaware and Pennsylvania saw the largest increase in identity theft reports per 100,000 people.
- Thirty-somethings reported identity theft more frequently than any other age group in 2022, accounting for almost 26% of all reported cases in 2022.
- Georgia had the highest number of reported identity theft cases per capita in 2022.

There were 441,822 cases of credit card fraud reported over the past year, making it the most common type of ID theft in 2022.

ID Theft By State

According to The Federal Trade Commission’s “ 2022 Consumer Sentinel Network Data Book,” Georgia saw the highest number of ID theft reports per capita in 2022. There were 574 reported cases per 100,000 residents in Georgia last year; Louisiana, second on the list, had 534 per

Continued on Page 2

EQUAL HOUSING LENDER Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

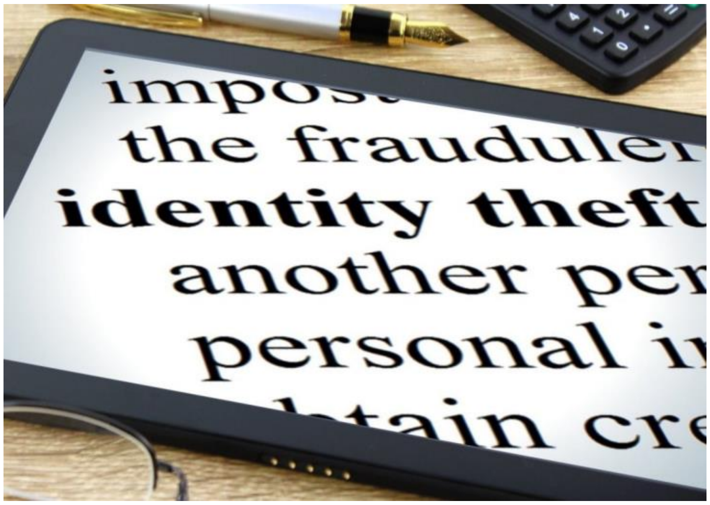
Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967



100,000 residents, and Florida, third, had 524 per 100,000 people.

1. Georgia
2. Louisiana
3. Florida
4. Delaware
5. Nevada
6. Texas
7. Pennsylvania
8. Alabama
9. South Carolina
10. Mississippi

Who's Most Vulnerable to ID Theft?

Of the 1,108,609 total identity theft reports in 2022, 30 - to 39-year-olds made up 25.9% of victims in the U.S. This group reported more cases of every type of ID theft (with credit card theft topping the charts, followed by "other" ID theft and loan or lease fraud) than any other group.

It's worth noting, however, that 30- to 39-year-olds made up the largest percentage of Americans in 2021, with30 -somethings accounting for almost 13.7% of the U.S. population that year. Still, on a per-capita basis, 30- to 39-year-olds reported ID theft at a higher rate than any other age group (0.6%). Those in their 40s reported ID theft at the second-highest rate (0.5%).

One distinction to remember is the difference between ID theft and ID fraud. ID theft is stealing someone's sensitive information, and ID fraud is the act of using that information to steal money or commit other crimes. In 2022, 30- to 39-year-olds reported higher instances of both ID theft and fraud than any other age group. In terms of money stolen due to ID fraud, however, 40 - to 49-year- olds experienced the biggest total dollar loss ($840 million).

Most Common Types of ID Theft in 2022

Credit card fraud was the most common type of ID theft in 2022, with 441,822 reported cases in 2022.This type of fraud, which ac- counted for about 40% of more than 1.1 million ID theft reports in 2022, involves thieves using your personal information to either steal from an existing credit card account or to open a new one in your name.

"Other" identity theft made up about 29% of all reports in 2022. This category includes fraud related to online shopping, payment accounts, emails and social media, medical services, insurance and more.

People in their 30s reported the most of each type of fraud. Americans 80 and over reported the fewest cases in almost all categories, though those 19 and younger reported the fewest instances of bank and credit card fraud.

There were also 14,501 credit card fraud reports from military consumers in 2022. Credit card fraud was the most common type of identity theft reported by military consumers, followed by bank fraud.

How do identity thieves get our information?

Phishing and ransomware were among the most common categories of cyberattacks leading to data breaches in 2022, the Identity Theft Resource Center's annual report states. Cybercriminals in 2022 seemed to focus their energy on resetting passwords, modifying authentication processes and attacking identities rather than deactivating antivirus and firewall technologies and log-tampering efforts, according to CrowdStrike's 2023 Global Threat Report.

How to prevent ID theft

Most people operating in today's financial world are vulnerable to identity theft in some way, unfortunately. Once someone has hold of your Social Security number, for instance, they might have enough information to access your bank accounts.

Over the last year, among fraud reports with a contact method identified, text messaging was most common, accounting for 22% of total reports, the FTC report says. Fraud through phone calls (20%) and email (19%) was also common.

Whether you're texting, calling, emailing or just browsing the internet, make sure to be vigilant in protecting your privacy — and your identity. The FTC recommends employing two-factor authentication and unique passwords, especially for email and online bank accounts.

You can freeze your credit with Experian, Equifax and TransUnion so no one can use your credit to their advantage. There are also services that let you monitor your credit and alert you to any suspicious activity.

It's also important to keep track of your wallet and cards and to keep any PIN information to yourself. When you're online, use secure websites (these start with "https") and keep your private information off public servers and computers.

Are solutions coming?

In March 2023, the White House proposed spending $600 million on fraud and identity theft prevention measures and $400 million to help victims of identity theft. It also announced an executive order that will aid federal agencies in preventing identity theft, calling for $300 million toward improving identity verification systems.

The American Rescue Plan Act, which President Joe Biden signed into law in 2021, includes $1.6 billion in funds to help prevent fraud and identity fraud that will be available to states by June 2023.

Sources:

Article: Jenifer Kuadli, March 30, 2023, LegalJobs

ConsumerAffairs

Images: The Blue Diamond Gallery, Title: Identity Theft, License: Creative Commons 3, Required Attribution: Alpha Stock Images, Original Author: Nick Youngson, No changes have been made to the original image; The Blue Diamond Gallery, Title: Tablet Dictionary Identity Theft Image, License: Creative Commons 3, Required Attribution: Alpha Stock Images, Original Author: Nick Youngson, No changes have been made to the original image

What Is a Keylogger? Definition, Prevention, and Removal

A keystroke logger, also known as a keylogger, is a software program or hardware device that logs and records every keystroke input on a computer. Bad actors can use it to steal sensitive data like passwords, financial information, and other confidential information. Keyloggers can also be used legitimately by parents to monitor their kids' online activities, and employers can use them to track employees' computer usage.

Keyloggers can be broken down into two distinct definitions:

Keystroke logging: The process of recording and storing every key that's pressed on a keyboard.

Keylogger tools: Devices or programs designed to log a user's keystrokes.

In addition to recording keystrokes, keylogger software can also collect user data through other methods, such as capturing screenshots, recording web searches and visits, and monitoring clipboard activity.

2 types of keyloggers

Keyloggers are either hardware-based or software-based.

Hardware-based keyloggers

Hardware keyloggers are physical devices used to monitor and record a user's activity on a computer. These devices are plugged into the back of a computer keyboard and have their own internal memory. The data is recorded directly to the device's memory and can be retrieved later by the attacker.

Hardware keyloggers are more difficult to detect than software keyloggers, as they are hardly visible on the computer's system. To prevent hardware keyloggers from being installed, physically inspect your computer's ports and cables periodically for any suspicious devices that may have been installed without your knowledge.

Software-based keyloggers

A software keylogger is a type of monitoring and tracking software that logs keystrokes from a computer keyboard. These keystrokes are recorded and stored in an encrypted log file that the attacker can access remotely.

Software keyloggers can be disseminated when you click on malicious links, download malware, visit a website with dangerous code, or open files that have been infected with malware. Although more easily detectable than hardware keyloggers, software-based keyloggers can be installed remotely, without needing physical access to your system.

How do keyloggers work?

Hardware-based and software-based keyloggers work differently. Generally, both types of keyloggers track and record every keystroke made on a computer based on a predefined command. These commands include:

- Length of the key press
- Number of keystrokes
- Key sequence
- Time of keypress
- Clipboard content

In the case of hardware keyloggers, a physical device is plugged into a computer's keyboard connection and records every keystroke that is entered into the keyboard. These keyloggers require physical access to a computer in order to be installed and are usually undetectable because computer users rarely pay attention to devices plugged into the backside of the computer.

On the other hand, software keyloggers are programs installed on the user's computer and run invisibly in the background. They include two files thatare installed in the same directory: a dynamic link library (DLL) and an executable file. The DLL file will monitor the system and record keystrokes into a file, while the executable file is responsible for launching the keylogger when the computer is turned on.

4 best practices to prevent keylogging

1. Avoid clicking on suspicious links
2. Update software and OS regularly
3. Enable firewalls and antivirus protection
4. Use strong passwords

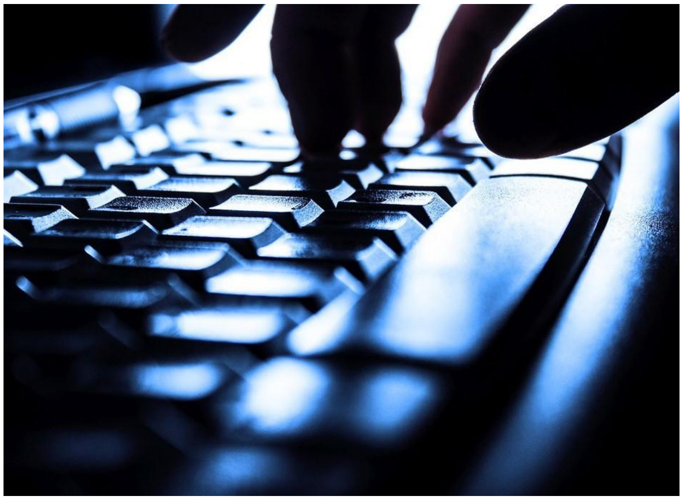
How to detect and remove keyloggers in 6 steps

If you find or suspect that a keylogger has compromised your system, here are the steps you can follow to detect and remove it.

1. **Use an anti-malware program:** An anti-malware program can scan your computer for malware, including keyloggers. Install a reputable anti-malware program and run a full scan of your system.
2. **Check task manager**: Open your task manager and look for any unfamiliar or suspicious processes running on your system. Keyloggers often run in the background and can be difficult to detect, but you might notice a process with a strange name or high CPU usage. Research them online to determine whether they're legitimate or malicious.
3. **Check your startup programs**: Keyloggers may start automatically with your computer. Check your startup programs and look for any suspicious entries. You can use the Windows system configuration tool or a third-party program to manage your startup programs.
4. **Change your passwords**: If you suspect that your computer has been compromised by a keylogger, change your passwords for all your accounts immediately. Use a strong, unique password for each account.
5. **Inspect your system for hidden devices**: Check your computer for any unusual hardware that can be used to capture keystrokes. This may include USB drives, external hard drives, or other connected hardware.
6. **Reinstall your operating system**: If all else fails, the best way to remove a keylogger is to reinstall your operating system. This will erase all programs and data on your computer, including any software keyloggers that might be present.

***Sources: Article:** Aminu Abdullahi, March 14, 2023, Enterprise Networking Planet*

***Image: Creator:** Christoph Scholz, Creative Commons License*



Union Bank

August 2023

How To Secure Your Home Wi-Fi Network

Seven easy steps to keep hackers and malware off your Wi-Fi network.

Wi-Fi is the backbone of home connectivity. Be it your laptop, smartphone, or the dozens of smart home devices strewn across your home, they are all connected to your Wi-Fi router to enable a world of experiences. But going online also means leaving yourself vulnerable to a range of threats like viruses, hacking, or network intrusion. Learning how to secure your home Wi-Fi network is critical to ensuring a safe online experience.

The best way to secure your Wi-Fi network is to set a unique SSID or broadcast name and to use a complex alphanumeric password ranging between eight to twelve characters. You should also change the default username and password for your router's administration page.

Change the default SSID and password

Most routers ship with a default name that is broadcast as the router's SSID. This SSID, also known as Wi-Fi name, can give away what brand of router you are using. Router manufacturers often use insecure passwords, or might even reuse passwords across devices, and as such, changing the SSID and Wi-Fi password is the first thing you should do while setting up your router.

The exact procedure for changing the Wi-Fi password can vary depending on the specific model you use, but look for the Wi-Fi or WLAN setting under your router's admin page. This page can usually be accessed by heading over to 192.168.1.1 via your browser. From there, set any recognizable name as your SSID. Feel free to get creative with it.

As for the password, it is highly recommended that you choose an alphanumeric combination with at least 8—12 characters. For added complexity, you can even include different cases and special characters. The harder it is to guess, the more secure is your Wi-Fi network. If your password gets too complex to remember, we recommend using a password manager app alongside.

Change the router username and password

While a complex Wi-Fi password will do the lion's share of keeping your home network secure, it can still be breached if someone manages to brute force or guess the password. Blocking off access to your router's administration page is the next step to follow. Most routers will have admin as the default username. This is, obviously, very easy to guess.

Head to user settings under your router's settings page and change the default user's name to a unique username. Follow the same advice as for Wi-Fi passwords to change the password for the admin account.

Continued on Page 2

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Taking it a step further, it is always a good idea to disable the default admin account as well, as it usually has access to all the router settings.

Enable encryption

Encryption makes sure that the traffic or data moving between your phone or laptop and the Wi-Fi router cannot be intercepted. This interception technique is called packet sniffing. Most modern routers will automatically select WPA2 encryption as the default, however, it is a good idea to check that you are on the latest standards. Head on over to the Wi-Fi page under your router's admin settings and make sure that it is set to WPA2 or WPA3. Note, that WPA and WEP are insecure protocols and have long been compromised. In the unlikely case that your router does not support any higher standard than WPA or WEP, it might be a good idea to upgrade to a new one from this list of best Wi-Fi routers.

Enable the firewall

A firewall, as the name suggests, acts as a filter between incoming and outgoing network traffic. It acts as a barrier against untrustworthy internet traffic in the form of attacks or hacking attempts by comparing your incoming internet traffic against a set of security rules and protocols. If the firewall thinks that an unauthorized computer is trying to access your network, it can alert you or block the threat automatically.

Most routers ship with at least a rudimentary firewall built-in. This is usually tucked away under advanced settings. On entry-level routers, a firewall can impact the overall speed of the network due to the added task of processing the traffic, but enabling it is well worth the minor hit to speed.

Turn off remote management and UPNP

Mid-range and premium routers often ship with a remote management utility built-in. These apps can help you keep a tab on your router's current status, speed, and access point-related information from a remote location. Some might even let you use the router for downloading files. Unfortunately, the services are rarely kept secure and up-to-date over the years. It's a good idea to disable them for additional security. In case you do want to access your router remotely, a reverse proxy service like no-IP or DynDNS can do the same but with much more peace of mind.

Similarly, UPNP was created to enable easy discovery of other devices on your network. However, it is an antiquated and insecure protocol that can be hacked into. Disabling it in Wi-Fi settings is generally a good idea.

Keep your router's software updated

Your router runs on its own software (often called firmware). There is a possibility that this software is found to have some flaws or security vulnerabilities. In such instances, the router manufacturer will issue a firmware update that will fix the vulnerability.

Your router should ideally keep itself auto-updated. However, it is good practice to routinely check for an update and ensure that you are on the latest possible firmware. This habit will minimize your exposure to any vulnerability that compromises the security of your network.

Some routers will also let you manually update through a local firmware file that can be downloaded from the manufacturer's website. However, we do not recommend most users attempt a manual firmware upgrade.

If you do not see a firmware update section in your router's settings, you may not have the requisite permissions. This can happen in instances where the router was supplied by your broadband provider. If you spot that the firmware version is several years old, it is worth contacting your broadband provider to ask if there is a firmware update available. Chances are that they will upgrade your router hardware if it is too old (at a cost sometimes, so please check with your broadband provider about any charges).

Create a guest network for temporary connections

You are bound to have guests come over to your house, and some may expect to use your Wi-Fi connection. In situations like these, it may be impolite to decline their request. At the same time, granting access to your primary Wi-Fi to devices you do not completely trust is also a big security issue. Doing so opens up access to other devices connected to your home network, such as smart home devices, printers, NAS devices, and shared folders on the network.

In such situations, you can create a guest network for these temporary connections to your Wi-Fi. This way, your guests will have access to the internet without having access to the other devices on your primary network. You can also share the password of the guest network without revealing the password of your primary network. And once the guests leave, you can change the guest network password or disable the guest network entirely — all without affecting your primary network and devices connected to it.

Most routers will ship with the ability to create a guest network. The feature usually resides under the WLAN/Wireless Network settings page. There, you can enable the guest network, and give it a name and password. Some routers will also present a setting for enabling/disabling access to your local network, with the default being off. And some routers will allow you to set a timer for the guest network, switching off the guest network at the end of it.

If you want to double down on security, you can enable the guest network and then hide your primary network's SSID. This way, your primary network will not be visible to people scanning for it, and they'll need to know the exact SSID as well as the password to connect to your primary network. Guests will see your guest network, which you can toggle off once you no longer need to share access.

Sources/Credit:

Article: ***Android Authority, How to secure your home Wi-Fi network, By Dhruv Bhutani, March 8, 2023***

Images: ***Smart Home House Symbol, Image by Roman from Pixabay;***
Royalty-free stock illustration. Free for use & download;
Privacy, Security, Internet image, Image by Arthur Bowers from Pixabay; Free for use

How To Stop Oversharing on Social Media

In today's digital age, social media plays a significant role in our lives. It has become a platform for sharing daily updates, thoughts, and experiences with friends and others. While sharing is a natural aspect of human behavior, oversharing can have its downsides. Oversharing on social media can lead to privacy violations, emotional burdens, social backlash, and even cyberbullying. Therefore, it is crucial to know how to stop oversharing on social media and strike a balance between sharing and privacy.

What is Considered Oversharing on Social Media?

Oversharing on social media is based on exposing intimate details about your personal life such as relationships, friendships, family matters or your daily routine. Some examples include:

- Regularly posting who you are with
- Posting intimate details about your relationships, friendships, family members and personal drama
- Enabling the geographic location on every post
- Constantly posting pictures of what you are wearing
- Posting work-related information on your account

Simple details about your routine or geographical location make you vulnerable because it's gateway information for becoming a victim of crimes both in the digital and real world. More on that later. Work-related information should always stay confidential, both because it's most companies' policy and because oversharing can put your company at risk of getting breached.

What are the Risks of Oversharing on Social Media?

There are many risks that come with oversharing your personal life on social media. Falling victim to cybercriminals is one of them.

You can become a victim of oversharing on social media if you often find yourself sharing too much information about your relationship, your children or yourself. For example, your child's name, age or birthdate are three key pieces of information that can cause you to fall victim to fraud. You might be wondering how that's possible. Well, people often create passwords based on personal information. These passwords are typically weak and easy to guess.

Oversharing is a risk because you can make it easier for cybercriminals to learn important information that can give them access to your online accounts. Some of the risks are:

- ***Account Takeover***

A cyberattack wherein cybercriminals utilize usernames and passwords that have been stolen to seize control of online accounts.

- ***Social Engineering***

Social engineering is the psychological manipulation used to get others to do things or reveal private information. This method is often seen through phishing emails.

- ***Physical security***

Protecting people, equipment, software, networks and data from potentially harmful physical acts and events.

- ***Reputation***

Protecting the reputation of who you are in your personal and professional life could be jeopardized if you overshare a bit too much in your accounts.

Here are some tips on how to stop oversharing on social media:

1. Set boundaries: Before posting anything on social media, ask yourself if you would be comfortable with sharing the same information with a stranger. If not, don't post it. Set some boundaries for yourself about the kind of information you want to share publicly.

2. Avoid posting too often: Posting too frequently can make it seem like you are constantly seeking attention or validation. Limit your posts to a few times a week or even less if possible.

3. Think before posting: Take time to think through your post or status update before sharing it. Ask yourself, "Is this relevant? Is it necessary to share? What impact will it have?"

4. Don't post personal details: Avoid posting sensitive personal information like your address, phone number, social security number, or financial information. This information can be used against you by hackers or identity thieves.

5. Be mindful of others: Be considerate of other people's feelings and privacy when posting pictures or information that involves them. Always ask for their permission before sharing any personal details about them.

6. Keep some things for yourself: Not everything needs to be shared on social media. Some things are best kept private, and sharing them online can be harmful.

7. Use privacy settings: Utilize privacy settings on social media platforms to control who can see your posts and information. Adjust your settings to limit the audience to your close friends and family.

In conclusion, oversharing on social media can have grave consequences, and it is vital to know how to stop it. By setting boundaries, avoiding posting too often, thinking before posting, limiting personal details, being mindful of others, keeping some things for yourself, and using privacy settings, you can strike a balance between sharing and privacy on social media. Remember, oversharing online can have real-world consequences, so always be careful about what you share.

Sources: Article: How To Stop Oversharing on Social Media, BY MATTHEW LYNCH, JUNE 22, 2023; How Oversharing on Social Media Affects Your Privacy, By Manuela Escobar Velasquez, December 23, 2022

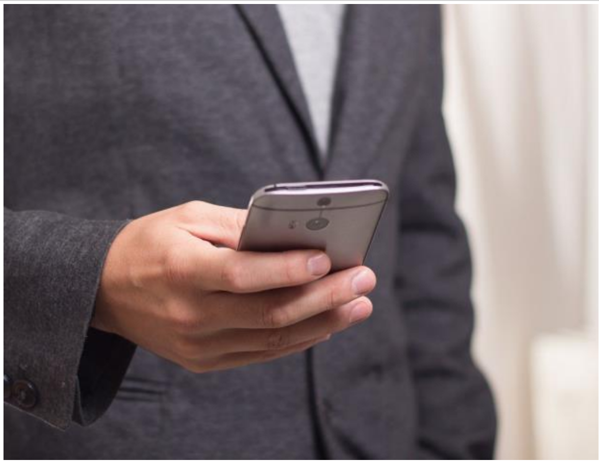
Image: Social Media Connections Networking, Image by Gordon Johnson from Pixabay; Royalty-free vectorgraphic. Free for use & download

UNION BANK

September 2023

Mobile Banking App is HERE!

What Is Smishing? Definition, Examples & Protection



Modern communication is largely dominated by mobile devices and cybercriminals have devised new ways to exploit unsuspecting users. One such method that has gained significant attention is smishing—a malicious practice that aims to deceive and defraud people through text messages. Short for "SMS phishing," smishing utilizes persuasive messages to trick recipients into revealing sensitive information or downloading harmful content.

Definition of Smishing (SMS Phishing)

Smishing, derived from "SMS" and "phishing," is a type of cybercrime that uses deceptive text messages to manipulate victims into divulging sensitive personal information such as bank account details, credit card numbers and login credentials.

Just as with phishing emails, the goal of smishing is to trick individuals into revealing private information that can be used for identity theft, financial theft or other fraudulent activities. Given the prevalence of text messaging as a form of communication, smishing has become a significant concern in cybersecurity.

Smishing vs. Phishing

Both smishing and phishing are forms of cyberattacks that trick individuals into providing personal, sensitive information. They primarily differ in their methods of delivery and the technologies they exploit.

Phishing

This is a broader term for a method of deceptive communication intending to trick recipients into revealing sensitive information, such as usernames, passwords, credit card numbers or Social Security numbers. Typically, phishing attacks occur via email. The attacker sends a seemingly legitimate email that encourages the recipient to click on a link. This link then leads to a fraudulent website that resembles a trusted site where the recipient is prompted to enter their sensitive information.

Smishing

This is a form of phishing that uses Short Message Service (SMS), commonly known as text messages, instead of email. Typically, the scammer poses as a legitimate institution, such as a bank, a service provider or a reputed company. The text message they send creates a sense of urgency or threatens consequences if the victim doesn't respond immediately. It downloads malware on the phone or includes a link to a fraudulent website designed to look like the legitimate organization's site. When victims reach that site they are tricked into entering their personal information.

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

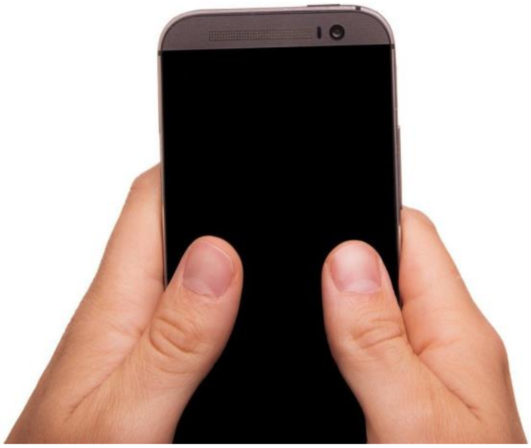
Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on Page 2



What is Smishing vs. Vishing?

Smishing and vishing are both phishing tactics targeting mobile users. Smishing uses deceptive SMS text messages to trick victims into revealing sensitive information. Vishing, on the other hand, uses voice calls or voice mails for the same fraudulent purpose.

It’s essential to never share personal information in response to unsolicited messages, whether received via email, phone, or text message, and to independently verify the request through known, trusted channels.

7 Types of Smishing

Smishing attacks can take several forms, each with its own approach but all ultimately aiming to trick victims into divulging sensitive information or performing actions beneficial to the attacker. Here are some of the most common types of smishing attacks:

1. ***Impersonation Scams***: The attacker pretends to be a known organization or individual. The attack could be via a message pretending to be from a bank, government agency or a reputable company.
2. ***Tech Support Scams***: Attackers pose as representatives from tech companies, claiming that the victim’s device or account has been compromised and that they need sensitive data to fix the problem.
3. ***Account Suspension Scams***: These messages claim that an account (bank account, social media or any other service) has been suspended and prompt the victim to verify their identity by providing sensitive information.
4. ***Missed Delivery Scams***: Attackers send messages claiming that the victim has missed a package delivery, and they need to provide personal details or a fee to reschedule the delivery.
5. ***Prize or Lottery Scams***: Messages claiming that the victim has won a prize or a lottery, and they need to provide personal details or make a payment to claim the winnings.
6. ***Charity Scams***: In these attacks, scammers impersonate a charitable organization, asking for donations, usually following a large-scale disaster or during holiday seasons.
7. ***Malware Link Scams***: Messages containing a link, which when clicked, installs malware on the victim’s device, allowing the attacker to steal information or gain control over the device.

Attackers are constantly innovating and finding new ways to exploit human trust, so it’s crucial to be skeptical of any unsolicited or unexpected message that asks for sensitive information or prompts to click a link.

How To Protect Against Smishing

Protecting against smishing attacks involves a combination of awareness, vigilance and adopting certain precautionary measures. Here are some steps you can take:

1. ***Be Suspicious***: Always be wary of unsolicited messages that request personal information or urge you to take immediate action.
2. ***Don’t Click on Links***: Avoid clicking on links in unexpected or unsolicited text messages. If you believe the message could be legitimate, independently look up the company’s contact information and reach out to them directly for verification.
3. ***Verify the Sender***: Be cautious of messages from unknown numbers or numbers that don’t look like phone numbers. Scammers often use email-to-text technologies to anonymize their true phone numbers.
4. ***Install Security Software***: Keep your mobile device secure by using trusted security software, and ensure that all your devices have the latest updates and patches.
5. ***Educate Yourself and Others***: Awareness is a powerful tool against smishing. Understand the tactics scammers use and share this knowledge with friends and family.
6. ***Use Two-Factor Authentication***: Implement two-factor authentication on your accounts when possible. This adds an extra layer of security, making it harder for scammers to access your accounts, even if they get your login details.
7. ***Don’t Respond***: If you receive a smishing text, don’t respond, even if the message gives you an option to “opt out” of future messages. Responding can confirm to the scammer that your number is active.
8. ***Report Smishing Attempts***: Forward smishing texts to 7726 (or “SPAM”) on most carriers. This helps your carrier identify and block spammers. You can also report the scam to the Federal Trade Commission (FTC) in the United States.

Remember, the most important rule is to never share your personal information in response to an unsolicited message. If in doubt, contact the company or organization directly using contact details you know are legitimate.

You can prevent smishing by staying vigilant. You should avoid clicking links in unexpected texts, never share personal information in response to unsolicited messages, use security software, update devices regularly, implement two-factor authentication and report suspected smishing attempts to your service provider.

Sources/Credit:
Article:
Forbes Advisor, What Is Smishing? Definition, Examples & Protection, By Shweta, Kelly Main, Contributor, Editor, August 1, 2023
Images:
Telephone, Mobile, Call image. Free for use., By: niekverlaan,
Smartphone, Phone, Typing image. Free for use.; By: niekverlaan; Attribution: Pixabay; Pixabay Content License Summary

2023 Business Email Compromise Statistics

BEC attacks are more common than ever

In 2023, the volume of nefarious emails impersonating enterprises reached a staggering crescendo, with attacks such as BEC making up 99% of reported threats. Historically, most of the threats reported in user inboxes have been BEC attacks, but 99% represents by far the highest share since Fortra began tracking this data point.

Considering this intelligence, organizations must implement a security awareness training program to ensure their staff are well placed to identify and flag potential BEC attacks. The unprecedented prevalence of BEC attacks means that, essentially, they are not a risk but an inevitability. Organizations must provide their employees with the necessary skills and information to recognize and alert security teams to the warning signs of a potential BEC scam.

Cybercriminals are innovating BEC tactics

Traditionally, BEC scams impersonate an organization's CEO or high-level executive to fool victims into facilitating a major financial transaction. However, threat actors have begun to change their tactics, expanding their target list to include vendors associated with the intended victim. By compromising a third-party or business partner, cybercriminals can target larger organizations with realistic emails containing key insider information, significantly increasing the legitimacy of an attack and the likelihood of success. Similarly, cybercriminals have begun to utilize generative AI to craft well-written, mistake-free emails that are more likely to fool victims.

Interestingly, while wire transfers made up only 4% of the preferred cash-out methods, in Q1, cybercriminals moved away from asking for a specific payment. Instead, attackers ask the victim to provide "the outstanding balance" or "owed amount", attempting to redirect payment of an unpaid invoice that has been partially or fully approved by internal stakeholders.

These developments are yet another example of how important regular security awareness training is. It is not enough to provide security awareness training upon hiring an employee or once a year; organizations must administer training regularly to reflect the current threat landscape.

Hybrid vishing is on the rise

Hybrid vishing attacks, which use phone numbers and the stolen intellectual property of trusted brands to evade gateways and convince users of their legitimacy, make up for 45% of all reported Response-Based threat types. These attacks primarily impersonated online financial services brands such as PayPal and digital security software such as Norton or McAfee products. If the victim calls the phone number, the criminal will attempt to monetize the attack through identity theft, credit card fraud, or a malware implant.

Again, organizations must empower their employees to identify and thwart hybrid vishing attacks with cybersecurity awareness training. Hybrid vishing is a relatively new attack technique, and it is likely that an organization's staff will be neither aware of it nor how to thwart it.

Credential theft is making a comeback

Despite falling in the second half of 2022, credential theft led all email impersonation threat types in Q1 2023. The Microsoft O365 phish drove this increase, experiencing the largest quarter-over-quarter jump in share (10%) since Fortra began reporting this datapoint, making up nearly 41% of all credential theft phishes. Most modern organizations use the Microsoft Suite in some capacity, meaning users are pre-conditioned to trust emails from Microsoft, helping cybercriminals obfuscate their attacks.

Although it's difficult to convey, organizations must impress upon their staff that the brands they trust the most are inherently the least trustworthy. Again, this can only be achieved through effective security awareness training.

Fortra's 2023 BEC Trends, Targets, and Changes in Techniques Report reveals the alarming surge in Business Email Compromise (BEC) attacks, constituting 99% of reported threats. Cybercriminals are innovating tactics by targeting vendors and utilizing generative AI. Hybrid vishing and credential theft are also on the rise. Organizations must prioritize regular security awareness training to empower their staff to identify and thwart these evolving threats. The report serves as a crucial reminder that knowledge and proactive measures are paramount in safeguarding against cybersecurity risks in today's increasingly perilous digital landscape.

Sources/Credit:

Article:
2023 Business Email Compromise Statistics, Josh Breaker-Rolfe, August 15, 2023

Image:
Scam Phishing Fraud royalty-free stock illustration. Free for use & download, Image by Mohamed_hassan; **Attribution: Pixabay;** *Pixabay Content License Summary*

UNION BANK

October 2023

Expect the Unexpected: The Keys to Business Continuity Planning for Financial Institutions

From raging wildfires to hurricanes to a worldwide pandemic, there is no shortage of reminders to the financial services industry of the importance of maintaining a business continuity plan (BCP).

Most institutions follow the FFIEC's recommended BCP process, which includes a business impact analysis (BIA), risk assessment, risk management and risk monitoring/testing. A tested, effective BCP ensures your organization is ready for the unexpected.

What is a Business Continuity Plan?

A BCP document includes critical information an institution needs to operate during an unplanned situation, helping to minimize financial loss and ensure continued service to customers or members. Effective business continuity planning provides a strategy for financial institutions to maintain and recover business operations and processes when they experience an unexpected disruption, such as a natural disaster, technology outage or terrorism.

According to the FFIEC, a BCP helps mitigate the adverse effects of disruption on an institution's strategic plans, reputation, operations, liquidity and compliance. A BCP should be specific to your institution and provide employees with operational instructions for addressing and working through a disruptive event. As such, your BCP should define what constitutes an event, individual roles and specific responsibilities and your response to an event.

Even though your response should be defined, it's impossible to know if the predetermined response will be completely effective. That's why your plan should be flexible, and your institution should have defined leadership roles that are authorized to deviate from the plan if needed.

Business Continuity Plan vs. Disaster Recovery Plan

Since financial institutions are a key part of U.S. infrastructure and economy, it is critical that business operations remain resilient, effects of disruptive events are minimized, and data remains accessible and secure. That's where both business continuity planning and disaster recovery come into play, though important distinctions exist between the two.

Business continuity relates to ensuring an institution's operations continue functioning with minimal downtime during an unexpected event, whereas disaster recovery involves restoring access to data or IT infrastructure after a disaster. Disaster recovery is a component of an institution's larger BCP. A disaster recovery plan (DRP) within the overall BCP helps institutions plan for protecting and accessing customer or member data in the event of a disaster or unexpected event. Both are critical to avoiding any negative reputational, financial or operational consequences.

A DRP varies depending on the severity of the incident and the unique nature of business process-

Continued on Page 2

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

es or technology being restored. As a result, a DRP is comprised of individual processes and procedures designed to provide a temporary process/procedure until normal operations are resumed, as well as insight and guidance on how normal operations are expected to be restored. Since disaster events vary widely, processes or procedures within a DRP may be general and instruct the entire institution or more specific and instruct individual branches, lines of business or departments.

Why Should Institutions Have an Up-to-Date Plan for Business Continuity?

The financial sector has prioritized digital channels, making managing data fundamental from both a customer experience and compliance perspective. Financial institutions of every size must prioritize and plan for efficient, rapid disaster recovery to meet compliance requirements, minimize downtime and—most importantly—meet the expectations of customers or members during and after a disaster or disruptive event. Business continuity plans bolster institutional resilience and ensure that institutions can continue operating in the event of a system outage following a disaster or cyberattack.

Business Continuity Plan Examples: How to Develop a BCP

While threats of physical loss or disruption caused by pandemics and natural disasters pose risks, other threats to a business continuity plan include disruptive data loss, breach or corruption. These threats could affect any geographic region at any point in time.

To protect your institution from the impact of data being lost, breached or corrupted, include the following elements in your BCP:

Risk Impact Analysis: The RIA assesses the probabilities and consequences of risk events if they occur. The results of the RIA are used to prioritize risks by establishing a criticality ranking. This helps determine what events or risks are more probable and require consideration.

Business Impact Analysis: A modern BCP must account for the critical role of data in today's banking environment, beginning with your BIA, which assesses and prioritizes all business functions and processes. A BIA is a systematic process to determine and evaluate the potential effects of an interruption to your institution's critical business operations because of a disaster, accident or emergency. This analysis is critical in establishing the priority of restoration for services and systems. The BIA process also helps senior leadership evaluate disruptive events' potential operational, financial and reputational effects.

Data Flow Diagram: This diagram visually represents your data and shows how information flows throughout your institution or within a specific line of business. This includes the origination of the data, intake of the data, data processing or manipulation, how various business units and internal systems interact with the data, how the data is shared with third parties and the final disposition of the data. The diagram is vital to your BCP and should be revised every few years or when introducing new business processes or lines of business.

Data flow diagrams help you understand how data flows and resides within your institution, facilitating the identification of risk and interdependencies within business processes that rely on data for fulfillment. These diagrams can also jump start your efforts to map processes and identify areas of possible unnecessary redundancy and automation.

In addition to these three components, your BCP should have a data classification policy to identify and classify all data based on its sensitivity and criticality levels. At a minimum, your institution must understand what data you have, what data is critical, where it is stored, how it is protected and how it can be recovered. Your BCP should also reference your network segmentation policy, which limits the access and movement of your data. Further, your BCP should also reference your data backup policy to eliminate any unnecessary connections into or out of your backup storage site, especially crucial in a ransomware attack.

Testing Your Business Continuity Plan

Testing your plan is the last phase of the BCP process and should not be overlooked, as it is integral to ensuring preparedness. In the past, many institutions conducted one large-scale BCP test at annual or semi-annual intervals. However, this approach makes it difficult to manage the testing process and discern the results. Modern planning narrows the scope of testing while increasing its frequency. Consider conducting small, function-specific tests or simulations monthly or quarterly, starting with the most critical functions.

By accumulating these tests over time, your institution will have a more accurate picture of your BCP's overall effectiveness. The increased flexibility and resiliency that testing provides, coupled with a robust infrastructure, goes a long way in weathering or avoiding many issues. Additionally, your institution should review and update its plan to ensure optimal effectiveness.

Enhance Your Preparedness with an Effective Business Continuity Plan

Past disasters demonstrate that business disruptions can occur quickly and without much warning. Having an up-to-date BCP helps institutions prepare for unforeseen circumstances while minimizing effects to customers and members.

Sources/Credit:
Article:
CSI Web, Steven Ward, Strategic Business Consulting Team, CSI Advisory Services, July 1, 2023
Images:
Hurricane, Devastation, Charley, Image by WikiImages from Pixabay,
Storm, Thunderstorm, Tree, Image by Jan Mallander from Pixabay;
Attribution: Pixabay; Pixabay Content License Summary

Best Practices for Social Media Security

In this era of a dynamic digital world, all of us have a favorite place on social media where we go to find comfort, fun and connection. These virtual venues, like quaint coffee shops or busy city parks, have become an essential part of our daily lives, where we exchange tales, make friends and keep in touch with loved ones around the world.

And it's quite similar for businesses as well. Social media is where all their customers come together and talk about the things that matter to them, be it the experience they had at an amusement park or how they felt about a product or service. So, it goes without saying that social media is the place for organizations to connect with customers, including the potential ones.

But the Internet can certainly be a dangerous place, filled with lurking cyber threats that are ready to feast on unsuspecting explorers. So, we must all be vigilant guardians of our online environments and take steps to ensure our safety and privacy in the real world.

You're not alone if you've ever had second thoughts about your online safety or hesitated to press the "Post" button, whether it's as a business or an individual. We all have the instinctive need to protect the things that are important to us. This includes protecting our online profiles on social media and the data of our customers from cybercriminals and other malicious actors who take advantage of vulnerabilities to steal sensitive data, spread false information and carry out other fraudulent actions.

What is social media security?

Social media security involves a set of policies and procedures used to safeguard user information, privacy and accounts on various social networking sites. It provides security against online harassment, unauthorized access, phishing attacks, malware, data breaches and identity theft. By implementing the right security measures, users can significantly lower their chance of being a target of cyberattacks and ensure a safer online experience.

Best practices for social media security and privacy

Develop a strong password policy

Organizations should create a strong password policy and instruct employees to use it when logging into their social media accounts. Passwords should include intricate combinations of uppercase, lowercase, digits and special characters. They should also be updated regularly, and the same passwords shouldn't be used on different platforms. Avoid using common passwords or information that could be guessed, such as birthdates or pet names.

Enable two-factor authentication

Two-factor authentication amplifies security by requiring users to submit a second form of verification, such as a special code sent to their mobile device, in addition to their password. This approach substantially reduces the risk of unauthorized access, even if the initial credentials have been compromised.

Educate employees on security awareness

Security breaches can be avoided with regular training and updates on new security risks. Organizations should regularly hold training sessions to inform employees of the potential hazards of social media and how to identify and react to potential threats. Employees should be taught how to spot phishing efforts, suspicious sites and social engineering tactics. Organizations should also implement guidelines for using social media, managing passwords and handling data.

Limit access privileges

Organizations should limit access rights by allowing only authorized staff access to social media profiles. Ensure that only those employees who need access to certain accounts and functionalities for their jobs are granted administrator rights. To retain control over account security, access rights should be verified and updated regularly.

Monitor and evaluate account activity

Social media accounts should be frequently monitored to identify any unauthorized access or questionable behavior. Organizations should create a procedure for content approval and review before the content is published. Keep a record of logins, posting schedules and account configuration alterations. And make sure that you respond immediately to any security or unauthorized access problems.

Use third-party applications with caution

Carefully examine the security procedures and reputation of third-party apps before integrating them into your social media accounts. Pay attention to the permissions given to these applications because they could give access to private information that they shouldn't be privy to. Regularly check permissions and revoke them for unnecessary applications.

Protect mobile devices

With the increasing usage of mobile devices for social media management, it's necessary to take precautions for the safe usage of these devices. Ensure that these devices have activated biometric or secure password authentication. The data that's saved on your devices should be encrypted, and operating systems and software should be updated often to fix security flaws.

Update and patch software regularly

Attackers may take advantage of outdated software, jeopardizing the security of your social media accounts. All social media management applications and platforms should be updated with the most recent security patches and upgrades. Organizations should perform frequent scans for vulnerabilities and promptly implement any pending patches.

Sources/Credit:

Article:
Sprinklr, Umme Sutarwala, Guest Contributor, Freelance, August 22, 2023

Image:
Media, Social Media, Apps, Image by Pixelkult from Pixabay;
Attribution: Pixabay; *Pixabay Content License Summary*

Mobile Banking App is HERE!

UNION BANK

November 2023

Cybersecurity Awareness Month

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

Since 2004, the President of the United States and Congress have declared the month of October to be Cybersecurity Awareness Month, a dedicated month for the public and private sectors to work together to raise awareness about the importance of cybersecurity.

This is the 20th Cybersecurity Awareness Month and it has grown into a collaborative effort between government and industry to enhance cybersecurity awareness, encourage actions by the public to reduce online risk and generated discussion on cyber threats on a national and global scale.

Secure Our World: 2023 and Beyond

In recognition of the 20th year, CISA announced a new enduring cybersecurity awareness program, Secure Our World. Secure Our World reflects a new enduring message to be integrated across the Cybersecurity and Infrastructure Security Agency's (CISA) awareness campaigns and programs, and encourages all of us to take action each day to protect ourselves when online or using connected devices.

The program promotes behavioral change across the Nation, with a particular focus on how individuals, families and small to medium-sized businesses can Secure Our World by focusing on the four critical actions below. Secure Our World is the theme for this year's Cybersecurity Awareness Month and will remain the enduring theme for future awareness month campaigns.

Four Easy Ways to Stay Safe Online

We can all collaborate to build a safer, more trusted digital world! By learning the four simple steps we can take to stay safe online at home, work and school, and sharing these tips with our community, we can all become significantly safer online.

Below are the simple actions we should all take not only during October, but every day throughout the year.

Staying Safe Online Is Easy With These Four Steps

Use Strong Passwords

Strong passwords are long, random, unique and include all four character types (uppercase,

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on Page 2

lowercase, numbers and symbols). Password managers are a powerful tool to help you create strong passwords for each of your accounts.

Turn On MFA

You need more than a password to protect your online accounts and enabling MFA makes you significantly less likely to get hacked. Enable MFA on all your online accounts that offer it, especially email, social media and financial accounts.

Recognize & Report Phishing

Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the message.

Update Software

Ensuring your software is up to date is the best way to make sure you have the latest security patches and updates on your devices. Regularly check for updates if automatic updates are not available.

Own a business? Learn more business-related online safety advice at **Secure Your Business**.

Cybersecurity Awareness Month 2023 Resources and Partner Toolkit

CISA and the National Cybersecurity Alliance (NCA) have partnered to create resources and messaging for organizations to use when they talk with their employees, customers and memberships about staying safe online. Available resources include:

- A PDF guide to Cybersecurity Awareness Month
- A sample email to promote Cybersecurity Awareness Month to your employees
- A sample press release to announce your participation in the 20th Cybersecurity Awareness Month
- Sample social media posts and graphics. Don't forget to use #CybersecurityAwarenessMonth and/or #SecureOurWorld in all your Cybersecurity Awareness Month related posts!
- A branded video background you can use during conference calls
- A branded email signature graphic
- An infographic to educate you and your community on the 4 simple steps to stay safe online
- A 101 presentation you can use to educate your colleagues, employees, and customers about Cybersecurity Awareness Month
- A branded PPT template you can use to create your own presentations

Download the toolkit here and here.

More Resources:

Secure Our World

Simple ways to protect yourself, your family and your business from online threats.

Tip Sheets

Learn more about the Four Easy Ways to Stay Safe Online by downloading the Secure Our World Tip Sheets.

Animated Videos

Learn more about the Four Easy Ways to Stay Safe Online by watching our short, animated YouTube videos.

Sources/Credit:
Article:
CISA
Images:
Image by Pete Linforth from Pixabay,
Image by Cliff Hang from Pixabay,
Image by cristianrodri17 from Pixabay;
Attribution: Pixabay, Pixabay Content License Summary

Tips to Keep Your Hybrid Workforce Secure

As the world transitions into a more permanent hybrid workforce, the flexibility brings both newfound benefits and challenges for employers and workers. Whether your team is working in the office, remotely, or something in-between, you don’t need to compromise your security for more flexibility. Here is a list of five simple tips to maintain your hybrid workforce culture while securing your workers and company assets.

Securing a new world of hybrid work: What to know and what to do

The cybersecurity landscape has fundamentally changed, as evidenced by large-scale, complex attacks like Nobelium, Hafnium, and more recently last week’s Colonial Pipeline attack, which signals that human-operated ransomware is on the rise.

Hackers launch an average of 50 million password attacks every day—579 per second. Phishing attacks have increased. Firmware attacks are on the rise, and ransomware has become incredibly problematic.

People are working on corporate networks and home networks and moving fluidly between business and personal activity online thanks to technologies intertwined with both aspects of our daily routines. The network is changing with employees’ home networks and devices are now part of the corporate network. What this means for organizations is that the network is suddenly without firm borders.

What is hybrid workplace cybersecurity?

Hybrid workplace cybersecurity refers to security protocols and measures an organization uses to protect its data and technology assets when operations include both in-office and remote work. These measures include access controls, firewalls, data backup and recovery, encryption, and regular security assessments and training.

Under the hybrid work model, an “owner” is responsible for specific tasks, such as identifying team members, managing folder structures, and maintaining the confidentiality of sensitive information. Since the model includes firm governance flexibility to collaborate and communicate, employees can continue working securely regardless of their location.

What is the biggest cybersecurity challenge with the hybrid workforce?

The biggest security challenge with the hybrid workspace is maintaining a secure and cohesive IT environment despite the added complexity of multiple locations, devices, and network integrations.

Here are some tips to keep your hybrid workplace secure

1. Educate your workforce to embrace secure work practices

Workers expect technology will follow them wherever they go—but having flexible locations exposes them (and your organization) to threats in new ways. That is why IT and security teams need to ensure the hybrid experience is secure at every endpoint by educating users about safe practices and potential hazards.

2. Verify the person is who they say they are

Multi-factor authentication (MFA) is a simple, first layer of security all businesses need before they can grant access to company assets. Think of MFA as something you know (your username/password) and something you have (your phone) to verify your identity and device health.

3. Enable secure access from anywhere

VPN provides a safe tunnel between users and applications so workers can stay productive and connected when they are on the road or working from home. It helps ensure only approved users get in by providing the right level of security without compromising the user experience.

4. Defend against security threats at any entry point

Most security breaches target endpoint users, requiring a first line of defense at the DNS layer and a last line for threats that slip through. The first layer blocks domains associated with malicious behavior before they get into your network or contains malware if it is already inside, while the last layer protects against more advanced threats.

Sources/Credit:

Articles:
CISCO, Microsoft Security, RiskOptics

Image:
Image by Eduardo • Subscribe to my YT Channel from Pixabay;
Attribution: Pixabay, Pixabay Content License Summary

Mobile Banking App is HERE!

UNION BANK

December 2023

Top Cybersecurity Trends to Watch Out for in 2024

With the Digital revolution around all businesses, small or large, corporates, organizations and even governments are relying on computerized systems to manage their day-to-day activities and thus making cybersecurity a primary goal to safeguard data from various online attacks or any unauthorized access. Continuous change in technologies also implies a parallel shift in cybersecurity trends as news of data breach, ransomware and hacks become the norms.

1. Rise of Automotive Hacking

Modern vehicles nowadays come packed with automated software creating seamless connectivity for drivers in cruise control, engine timing, door lock, airbags and advanced systems for driver assistance. These vehicles use Bluetooth and WiFi technologies to communicate that also opens them to several vulnerabilities or threats from hackers. Gaining control of the vehicle or using microphones for eavesdropping is expected to rise in 2023 with more use of automated vehicles. Self-driving or autonomous vehicles use an even further complex mechanism that requires strict cybersecurity measures.

2. Potential of Artificial Intelligence (AI)

With AI being introduced in all market segments, this technology with a combination of machine learning has brought tremendous changes in cybersecurity. AI has been paramount in building automated security systems, natural language processing, face detection, and automatic threat detection. Although, it is also being used to develop smart malware and attacks to bypass the latest security protocols in controlling data. AI-enabled threat detection systems can predict new attacks and notify admins of any data breach instantly.

3. Mobile is the New Target

Cybersecurity trends provide a considerable increase (50 percent) for mobile banking malware or attacks in 2019, making our handheld devices a potential prospect for hackers. All our photos, financial transactions, emails, and messages possess more threats to individuals. Smartphone viruses or malware may capture the attention of cybersecurity trends in 2023.

4. Cloud is Also Potentially Vulnerable

With more and more organizations now established on clouds, security measures need to be continuously monitored and updated to safeguard the data from leaks. Although cloud applications such as Google or Microsoft are well equipped with security from their end still, it's the user end that acts as a significant source for erroneous errors, malicious software, and phishing attacks.

5. Data Breaches: Prime Target

Data will continue to be a leading concern for organizations around the world. Whether it be for an individual or organization, safeguarding digital data is the primary goal now. Any minor flaw or bug in your system browser or software is a potential vulnerability for hackers to access personal information. New strict

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

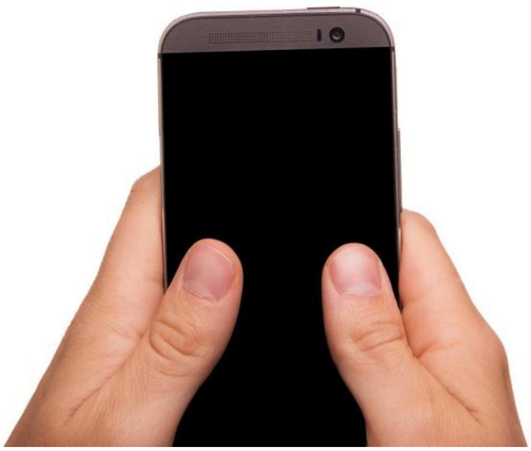
Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
740-374-0010
By Appointment Only

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Continued on Page 2



measures General Data Protection Regulation (GDPR) was enforced from May 25th, 2018 onwards, offering data protection and privacy for individuals in the European Union (EU). Similarly, the California Consumer Privacy Act (CCPA) was applied after January 1st, 2020, for safeguarding consumer rights in the California area.

6. IoT With 5G Network: The New Era of Technology and Risks

With the advent and growth of 5G networks, a new era of interconnectivity will become a reality with the Internet of Things (IoT). Read about What Is the Internet of Things (IoT) and Why It Matters? This communication between multiple devices also opens them to vulnerabilities from outside influence, attacks or an unknown software bug. Even the world's most used browser supported by Google, Chrome was found to have serious bugs. 5G architecture is comparatively new in the industry and requires a lot of research to find loopholes to make the system secure from external attack. Every step of the 5G network might bring a plethora of network attacks that we might not be aware of. Here manufacturers need to be very strict in building sophisticated 5G hardware and software to control data breaches.

7. Automation and Integration

With the size of data multiplying every day, it is eminent that automation is integrated to give more sophisticated control over the information. Modern hectic work demand also pressurizes professionals and engineers to deliver quick and proficient solutions, making automation more valuable than ever. Security measurements are incorporated during the agile process to build more secure software in every aspect. Large and complex web applications are further hard to safeguard making automation as well as cyber security to be a key concept of the software development process.

8. Targeted Ransomware

Another important cybersecurity trend that we can't seem to ignore is targeted ransomware. Especially in the developed nations' industries rely heavily on specific software to run their daily activities. These ransomware targets are more focused such as the Wanna Cry attack on the National Health Service hospitals in England Scotland corrupted more than 70,000 medical devices. Though generally, ransomware asks to threaten to publish the victim's data unless a ransom is paid still it can affect the large organization or in case of nations too.

9. State-Sponsored Cyber Warfare

There won't be any stoppage between the western and eastern powers in attempts to find superiority. The tension between the US and Iran or Chinese hackers often creates worldwide news though the attacks are few; they have a significant impact on an event such as elections. And with more than 70 elections bound to be held this year, criminal activities during this time will surge. Expect high-profile data breaches, political and industrial secrets to top cybersecurity trends for 2023.

10. Insider Threats

Human error is still one of the primary reasons for the data breach. Any bad day or intentional loophole can bring down a whole organization with millions of stolen data. Report by Verizon in data breach gives strategic insights on cybersecurity trends that 34 percent of total attacks were directly or indirectly made by the employees. So make sure you create more awareness within premises to safeguard data in every way possible.

11. Remote Working Cybersecurity

The pandemic has forced many companies to move to remote working, introducing a new set of cybersecurity challenges. Remote workers may be more vulnerable to cyberattacks as they often have less secure networks and devices. As such, organizations must ensure adequate security measures to protect their remote workers, such as multi-factor authentication, secure VPNs, and automated patching.

12. Social Engineering Attacks

Social engineering attacks are on the rise, as attackers use techniques such as phishing, spear phishing, and identity theft to gain access to sensitive data. Organizations must ensure that their employees are trained to recognize and report any suspicious activity and have measures in place to protect against these types of attacks.

13. Multi-Factor Authentication

Multi-factor authentication (MFA) is a security measure that requires users to provide more than one form of authentication before they can access an account. This additional layer of security helps to protect against cyberattacks, as attackers must have access to multiple pieces of information in order to gain access. Organizations should ensure that all accounts are secured with MFA to reduce the risk of unauthorized access. Automation is becoming increasingly important in cybersecurity. Automated security processes can help reduce the time it takes to detect and respond to threats and improve the accuracy of threat detection. Automation can also reduce the reliance on manual processes, which can be time-consuming and prone to human error.

14. International State-Sponsored Attackers

State-sponsored attackers have become increasingly sophisticated, and organizations need to be aware that these types of attackers may target them. They must ensure adequate security measures to protect against these types of attacks, such as multi-factor authentication and real-time monitoring.

15. Identity and Access Management

Identity and access management (IAM) is a security measure that helps organizations control and monitor who has access to sensitive data and networks. They should ensure adequate IAM measures, such as user authentication, authorization policies, and access control lists.

Sources/Credit:
Article:
Nikita Duggal, SimpliLearn
Images:
Image by Pete Linforth from Pixabay,
Image by Cliff Hang from Pixabay,
Attribution: Pixabay, Pixabay Content License Summary

Top Cyber Scams of 2023

Scams are a part of the digital ecosystem, and knowing how to protect yourself is only half the battle. A key part of practicing proper cybersecurity is being aware of the most common cyber scams. With roughly half of 2023 behind us, here are the scams I have seen the most this year and how you can avoid them.

1. Fake Financial Websites

In this type of cyber scam, scammers create a fake website that mimics your bank's website to trick you into entering sensitive information, like your login information or bank account number. You may click on a link from an email, text, or online ad that brings you to a fake site.

Here are ways you can avoid fake bank websites:

- Use your bank's mobile app to access your accounts.
- Bookmark your bank's website.
- Always check that the URL or web address is correct.

2. Mortgage Loan Modification Scam

In a mortgage loan modification scam, the scammer will contact you over email, text, or by using a fake website, and offer mortgage modification services.

When you try to receive these services, they will either try to collect money for the service before performing it or try to get you to transfer the deed to them. If you transfer the deed to the scammers, they will not perform the mortgage modifications and may sell your property without your consent.

Follow these tips to avoid a mortgage loan modification scam:

First contact your trusted mortgage servicer or lender for mortgage modifications.

- Never pay money for services until you receive them.
- Avoid transferring the deed to a property if you are not prepared to lose ownership of it.

3. Student Loan Forgiveness Scam

With previously proposed legislation regarding student loan forgiveness, scammers have found a new scheme to steal information from you.

A scammer may email you saying they are part of the student loan forgiveness program, and they need you to enter sensitive information to process the loan forgiveness. The scammer may also ask you to pay upfront for loan forgiveness assistance by providing a payment option in their email.

Stay safe from this scam with these tips:

- Verify a service is an official Federal Student Aid Servicer .
- Do not pay anyone for student loan forgiveness help until you receive the service.
- Identify phishing emails with typos or obvious misspellings or urgent requests.
- Check the email address, even if the contact's name seems real.
- Never send payment information through email.

Sources/Credit:
Articles:
Raghu Valipireddy, LinkedIn
Image:
Image by Eduardo • Subscribe to my YT Channel from Pixabay;
Attribution: Pixabay, Pixabay Content License Summary