2024 GUIDE TO

Personal Cybersecurity

OnPoint
COMMUNITY CREDIT UNION

Table of contents

Introduction

The digital age has brought great conveniences but also certain risks. Artificial intelligence and automation has led to increasingly sophisticated and convincing frauds and scams targeting our bank accounts and our personal information. Every time we open an online account to try a new game or service, participate in social media, or even, in some cases, swipe our debit or credit cards, we increase the risk of exposure.

Millions of Americans are the victims of identity theft and fraud each year, and those numbers are rising. Nationally, U.S. consumers reported losing $10.3 billion related to fraud complaints last year, up 17% from 2022's total of $8.8 billion. Oregon and Washington ranked first and second respectively in impostor scam complaints in 2023. While massive data breaches frequently make headlines, even the most careful consumers are open to individual attacks, with youth/teens and senior citizens particularly vulnerable. It's important to educate yourself on the basics of cybersecurity as well as the current trends and tricks.

Fraud or Scam?

The terms “fraud” and “scam” are often used interchangeably, but there are key differences, particularly with your level of protection against financial loss.

Fraud involves unauthorized access to personal information without the victim’s knowledge or consent.

> For example, credit card fraud entails someone making unauthorized transactions using your stolen card information—they may have hacked a merchant’s website or used a card skimmer at a gas station to get your card details.

Scams attempt to manipulate the victim into willingly providing money or personal information, usually relying on strong emotions such as panic or fear.

> In contrast to fraud, scams like “phishing” may deceive you into revealing sensitive information such as your card number through fake emails and websites.

In cases of fraud, you will typically be protected against loss as long as you report unauthorized activity to your financial institution in a timely manner to allow for a dispute. If you are victimized by a scam, however, your financial institution will have fewer options, and you will likely be liable for the loss.

You can protect yourself by learning cybersecurity basics and understanding the red flags of scams and identity theft attempts. OnPoint has many online articles and educational resources available for you.

Who are the targets?

Everyone is at risk. However, youth/young adults (ages 13-25) and seniors (ages 60+) are the most vulnerable targets.

YOUTH & YOUNG ADULTS (AGES 13–25):

Young adults, teenagers, and even younger children are growing up with online gaming and mobile devices. Early exposure to digital technology can provide a valuable comfort level, but it also puts them at risk from social engineering tactics, and they may overlook password security and privacy settings.

- In 2022, security researchers detected seven million attacks relating to popular children's games, resulting in a 57% increase in attempted attacks compared to 2021.
- Young people, particularly children, often have clean credit histories that are not closely monitored, making them attractive targets for identity thieves.
- Chat features in online games give scammers a platform to convince young people to reveal personal information, transfer money, or click on malicious links (such as a supposed update or mod to a popular game).
- The rise of Fintech solutions for young people is a temptation for scammers.

By learning the basics of cybersecurity young people are better equipped to explore the positive side of the digital world with less risk of being exploited.

SENIORS (AGES 60+):

People aged 60 and older can be especially vulnerable to phishing, fraud, and identity theft. A high percentage of romance—or sweetheart—scams are driven by a need for connection or loneliness in seniors, and evolving AI-driven phone and email fraud can be hard to detect.

- Elder fraud complaints to the FBI's Internet Crime Complaint Center (or IC3) increased by 14% in 2023, and associated losses increased by about 11%.
- Scammers may target older individuals because they assume they possess significant assets.
- Tech support scams, confidence and romance scams, non-payment or non-delivery scams, investment scams, and personal data breaches, were the top five types of elder scams and fraud reported in 2023.

Seniors, and caregivers alike, should familiarize themselves with the evolving tactics criminals use to run scams or commit fraud.

Latest trends in Cybercrime

Identity theft is an ever-evolving phenomenon. While developing good cybersecurity habits is still the best course of action you can take, it's also important to be aware of the new trends.

- **Deepfake phishing.** AI and advanced technology are leading to more sophisticated scams, such as deepfake phishing, where bad actors can recreate a loved one's voice to add weight to their manipulative communications. Just because it looks or sounds like someone you know, be wary, especially if there are other red flags present.
- **Credential stuffing.** Technology improvements have made "credential stuffing" easier. Someone with stolen login credentials (username and password) from one website will test the same combination on other websites, and automation makes this a faster process.
- **Diversified targets.** Cyber-attackers target a range of groups and organizations, including small businesses, schools, and individuals, which often have less robust network defenses.
- **Smart Devices.** A growing number of "smart" appliances, cars, and systems are connected to the internet, creating more potential access points for cyber-attacks. Preventive steps include changing your router name and password from the default settings, using a guest network for smart devices, and adding multi-factor authentication requirements to access administrative control of your primary network.

How to spot and avoid common internet scams and fraud.

Fortunately, you can protect your personal information with a proactive approach to cybersecurity. Vigilance can prevent you from falling victim to cybercrime, but you should be ready to act quickly if your information is stolen. We're here to help—our comprehensive guide to personal cybersecurity can prepare you to protect yourself against or recover from scams and fraud.

Account hijacking.

Account hijacking occurs when an identity thief obtains someone's login credentials for a social media, email, or online banking account. Among other possible consequences, the attacker might use the stolen account to make the victim look bad, steal their money, or impersonate the victim to scam someone else with a higher-value account.

The previous decade has been punctuated with high-profile data breaches:

- In 2023, T-Mobile experienced two data breaches affecting 37 million customers.
- From 2019 through 2023, Facebook exposed more than 540 million user records.
- A 2022 student loan servicer Nelnet Servicing experienced an information leak affecting 2.5 million users.

In other words, it is quite likely that some of your personal information has been exposed. It's important to take precautions to prevent someone from getting enough additional information about you to access your accounts.

How to spot it:

- Someone you know contacts you about a too-good-to-be-true offer.
- Someone you know contacts you via a strange phone number.
- Someone you know starts posting strange offers on social media.

How to avoid it:

Regularly update your passwords, use two-factor authentication, and protect your web traffic with a Virtual Private Network (VPN). Additionally, ensure that all of your passwords—or even better, passphrases—are unique across your various accounts. Automation has made it easier for criminals to test login credentials at different sites, so if you repeat passwords, once one account is compromised, others could be as well.

If you suspect one of your accounts has been accessed without your permission, contact the organization's customer service department immediately and file a complaint with the Federal Trade Commission.

Impostor scams.

A scammer pretends to be someone you know, a government representative, or an employee of a company you might do business with. They attempt to manipulate you into sending money or sharing personal information. They can spoof phone numbers or email addresses to appear legitimate. They might try to get control of your computer by sending a malicious link or ask you to send them money via gift card or wire transfer, which is like giving the scammer cash—if you're a victim of this scam, you likely will not recover your funds.

How to spot it:

- They claim to be from tech support calling about a problem on your computer. You need to pay them or click on a link they send.
- They claim you owe money to the IRS or another government agency.
- You just won a prize for a contest you don't remember entering, but you have to pay fees to get the prize.
- A friend is in trouble and needs your help.
- You got a check for too much money and need to send a refund.

How to avoid it:

- Do not send gift cards or wire transfers to people you do not know.
- Never send money without first verifying who contacted you, even if you feel like you know the person or they say they are a friend or relative.
- Do not give out your personal information to people you do not know.
- Do not give access to your computer to people you do not know.
- The IRS and other government agencies will not contact you by phone, nor take payment by gift card or similar methods.

Children and teenagers are particularly susceptible to accepting links from, sharing personal information with, or sending money to scammers through online games or on social media.

Sweetheart scam.

A sweetheart scam is a trick in which a scammer uses emotional manipulation to gain the trust of their target. Using online dating apps and similar tools, the scammer convinces their target to send money or share personal information.

Also be wary of what's known as the "pig-butchering" variant. It usually starts with a text message under the guise of accidentally reaching a wrong number or trying to re-establish a connection with an old friend. Scammers attempt to keep the target talking to build a rapport (this is referred to as 'fattening the pig') before introducing the prospect of a lucrative investment opportunity, often through cryptocurrency.

How to spot it:

- An online acquaintance professes strong feelings, even though you have never met.
- Someone you meet online requests a check, money order, or wire transfer.
- Someone contacts you through a dating site but claims to live in another city or country.
- A stranger needs urgent help and/or offers a financial incentive.

How to avoid it:

Be extra cautious about requests from someone you've never met, especially if you have no mutual connections. These scammers prey on our desire to be valued and our willingness to help—it's an extremely effective scam and requires a high level of situational awareness.

- Never send money to a stranger you meet online.
- Recognize that sweetheart scammers will attempt to manipulate you emotionally.
- They'll claim to fall in love with you, and then request money for a purpose that plays on your sympathy.
- Their goal is to get as much of your money as possible, either over time or all at once.

Seniors can be especially at risk for sweetheart scams. Scammers assume seniors have more assets than others and may be less familiar with cybersecurity best practices and online scams.

Phishing, vishing, smishing.

Phishing is a form of social engineering where scammers use an email to impersonate a business or reputable person to trick or intimidate people into providing passwords, credit card numbers, and other identifying information, or sending money. Phishing messages are often sent to large numbers of people at once. A more-focused variant is called spear phishing, where the scammer uses social engineering and spoofed messaging to target one or more individuals in a specific organization. For example, they might simulate a message from the target's employer asking them to provide critical information or conduct a financial transaction that bypasses normal procedures.

When a scammer uses phone calls, it's known as voice phishing, or vishing. Similarly, smishing tactics use SMS messages. In all forms, phishing attacks mimic communications from brands, businesses, and people you trust.

How to spot it:

- You receive an unexpected message requesting sensitive information.
- You receive a message from someone you know but from an unknown or strange email address or phone number.
- The message sender doesn't use your name (however, they may use your name if it is a spear phishing scam).

How to avoid it:

The goal is to convince you to give up your personal or confidential information by creating a false sense of urgency or desire. These scammers often use fear, false authority, or other emotional manipulations to get you to let down your guard. If you have doubts about a message:

- Never trust a request for your password—your password is only for you. A legitimate source will not need your password, a PIN, nor your debit/credit card number to access your account information.
- Call the organization directly, don't follow any links in the message.
- Research the company that sent the communication.
- Report it to the Federal Trade Commission.

The rise of AI technology has allowed for greater sophistication in phishing attacks. From more natural-sounding language to simulating the voices and images of people you know, it can be harder to detect a scam at a glance. It's important to trust your instincts if anything about a request seems odd.

Quick money, unexpected windfalls, and too-good-to-be-true offers.

These too-good-to-be-true messages promise unexpected money, often in exchange for a fee or tax. The most well-known variation involves a prince in crisis requesting help to transfer funds out of his country. However, scammers may also claim to represent cash prize contests, rebate programs, or the estate of wealthy relatives.

Some modern iterations involve listings at online exchange sites such as Zillow or Facebook Marketplace, including:

- A seller offers items for much less than they are worth.
- A potential buyer offers to overpay in exchange for a promise to refund them that difference.
- A rental listing where the 'owner' insists they need a wire transfer for a deposit before meeting or visiting the home.

How to spot it:

- Someone offers you money unexpectedly.
- You get a message from someone you know from an unknown email address or phone number.
- Someone asks you to deposit a check on their behalf and offers you a portion of the cash.
- An online posting doesn't want to meet first and requires a deposit.
- An online seller wants to "verify" your identity with a code sent through Google Voice.

How to avoid it:

You should always be suspicious if a lawyer, bank, or company contacts you offering any sum of money—even if the offer includes official-looking documents. If you are contacted don't send money or attempt to deposit unverified funds, especially if you've never met the sender. A check might be a fake, or a cash app transfer could prove fraudulent. The funds may initially be made available by your financial institution, but if the funds from the deposit are removed from your account, you would lose any portion of the deposit you had withdrawn or spent. Seek the advice of a lawyer or financial consultant if you're suspicious of a communication.

Question everything. The scammers can produce convincing emails, spoofing a digital payment service like PayPal or Venmo to explain the need for an overpayment. They will often combine these offers with social engineering attempts to make you act with urgency.

Fake approval messages.

A common example of this scam is when attackers send fake approval notices to consumers claiming the target has been "pre-approved" for a line of credit, mortgage, or personal loan. The goal is to convince the target to provide personal or financial account information in order to accept the offer.

Recent college graduates are often the target of fraudulent credit card offers. Homebuyers are vulnerable to housing scams. Similarly, attackers may claim to be insurance companies offering federal tax relief after a natural disaster. Impostor scams are the most common complaint to the Social Security Administration.

How to spot it:

- You get approved for an offer you don't remember applying for.
- You're offered an insurance payout for coverage you don't have.

How to avoid it:

Always be cautious of lenders that:

- Promise to negotiate a loan modification to avoid foreclosure.
- Guarantee credit if you can pay a fee in advance.
- Offer a suspiciously low or extremely high interest rate; or credit offers that don't mention an interest rate.

Likewise, if you don't remember applying for credit from a lender that contacts you, it's best to seek credit elsewhere. You may also want to check your credit report for unusual activity. You can obtain one free copy of your credit report from each of the major bureaus, once per year, at annualcreditreport.com.

How to spot and avoid common offline schemes.

Consumers aren't exposed to security risks only on home computers or mobile devices. Debit and credit card transactions made in public can be vulnerable. Cards equipped with an EMV chip have some protection through data encryption, but physical purchases are still susceptible to skimming devices. For example, a criminal might place a false chip reader over a legitimate point-of-sale device to siphon card data. In certain circumstances, fraudsters might use a portable RFID scanner to read card chips from a target's wallet, purse, or bag, but this requires extremely close proximity and is relatively low risk—just be wary of anyone getting too close to you.

Other offline scams to watch out for:

Social Security scam: Scammers often target seniors, threatening a suspension of Social Security benefits or even arrest, and demanding the target's Social Security number.

Health care scams: Scammers may attempt to solicit fees for services not rendered.

Secret shopper scams: Mystery shoppers are independent contractors posing as customers who report back to market research companies, among others, about the brand experience. However, deceitful mystery shopping schemes demand shoppers to pay for goods upfront, or for a worthless certification.

SIM card swapping.

Fraudsters don't need physical access to your phone to steal your phone number. They can trick your phone carrier's customer service into thinking that you're attempting to activate your SIM card on another device. Then they can use your number to access your texts, phone calls, data, and any accounts associated with your phone number. This includes receiving secure access codes sent to your phone number.

How to spot it:

- Your phone suddenly stops receiving calls and messages.
- You get an alert saying your phone number has been successfully transferred to another SIM card.

How to avoid it:

The only way to protect yourself is never to consider your phone number to be fully secure. You can strengthen the security of your phone account by requesting that your carrier place an additional passcode on it.

You can prevent damage caused by a SIM swap fraud by never linking other accounts, like your social media profiles, to your real phone number. Instead, you can use a VoIP service such as a Google Voice number. These types of phone numbers aren't associated with SIM cards, so there's no way for a hacker to take them over.

ATM fraud.

ATMs are tempting targets for fraudsters. The machines are filled with cash and consumers regularly expose their card information and PINs. Fraud schemes range from stealing card data to spying on unknowing consumers.

How to spot it:

- Always evaluate an ATM before you use it, even if it's a machine you frequent.
- Check for new buttons, unfamiliar keypads, or attachments that might conceal a pinhole camera.
- Pull on the card reader to check for devices that can capture your card data, known as skimmers. If it's loose or comes off in your hand, do not trust the machine. Likewise, if the keypad feels loose, it may have been altered.
- Holes or cracks appear in the ATM shell.

How to avoid it:

Try to avoid ATMs in areas with low foot traffic or low light, and make sure no one is standing near you when you use the machine.

You can watch for unusual activity with your ATM/debit card, and turn the card off if necessary, through OnPoint's Card Manager app.

Know the common signs of identity theft.

Vigilance will reduce your chances of becoming a victim of identity theft, but there are no guarantees. If you are the target of fraud, it's vital to take action as soon as possible.

Never ignore suspicious activity related to your financial accounts. Identity thieves often check to see if their targets are paying attention by making small charges on accounts. Even if an unidentifiable charge only amounts to a dollar, you should investigate. You can obtain a free copy of your credit report from each of the three credit bureaus at www.annualcreditreport.com.

Clues that your identity has been compromised include:

- You stop receiving calls and texts or can no longer connect with your wireless cellular network.
- A notice from an organization with which you do business states you were impacted by a data breach.
- Unexpected withdrawals from your accounts.
- Your mail stops unexpectedly.
- You're notified of a tax return that you did not submit.
- Your checks are refused by merchants.
- Your health insurance provider says you've reached your benefits limit when you haven't been to the doctor.
- You receive medical bills for procedures and services you didn't use.
- Unfamiliar accounts appear on your credit report.

Children have limited and clean credit history, which makes their social security numbers particularly attractive to identity thieves. A social security number is really all that's needed to begin a scheme of synthetic identity theft, especially because parents and children are unlikely to check on credit activity. You can request a copy of your child's credit report as a special situation.

What to do if you've been scammed or think you might be vulnerable.

If you have a reason to believe your personal information was stolen, if you do business with a company that recently experienced a data breach, or if your wallet was stolen, take action immediately.

Seeing fraudulent activity on your credit card bill, credit report or background check is never fun, but you shouldn't panic. There were 5.7 million accounts of reported fraud which amounted to $6.1 billion in losses in 2021, yet there are many resources available.

It's important to take these steps, even if you're not certain that identity theft has occurred. Scammers often hold onto information to wait until the target has dropped their guard:

- Contact your financial institutions to check for unauthorized activity and replace any compromised cards.
- Change the passphrases on all affected accounts—and unaffected accounts using similar login credentials or verification methods.
- Place fraud alerts with any one of the three major credit reporting bureaus: Experian, TransUnion, or Equifax—the chosen agency will notify to the others.
- Freeze your credit.
- Contact and get reports from your debt collectors, creditors, and your financial institutions.
- File a report with local law enforcement or the FTC.
- Consider a credit monitoring service for added protection.
- Check out OnPoint's identity theft resources for more information.

Unsure if your accounts were impacted by a data breach?

The site Have I Been Pwned? can help determine if your accounts have been compromised.

Tips for talking to your children about online safety.

Preferring vulnerable targets who may not have much knowledge about financial scams, identity thieves often target children. What looks like a fun online game may be a trap designed to capture their parent's credit card information. Scammers may also pose as children online to solicit personal information from young targets.

Some key ways to protect minors from scams include:

- **Education:** Teach children about threats they are likely to encounter online, such as malicious links, viruses, spam, and online predators.
- **Device permissions:** Newer models of smartphones often provide child-safety controls, allowing parents to limit user access to an approved app list, block offensive content and limit screen time.
- **Oversight:** Parents can promote good digital habits by playing an active role in the online interactions of their children. Playing an online game together can be a fun teaching moment.

Teaching kids about cybersecurity.

The best way to teach children about cybersecurity is to talk with them and engage them at a level they can understand. Try to connect cybersecurity to the advice you give your children about real-life interactions. For instance, taking a gift from a stranger in the street is similar to accepting a friend request from a stranger online.

Important security topics for kids include:

- **Making strong passphrases:** Create passphrases by following best practices, including a unique passphrase that contains a random combination of 10 or more upper- and lowercase letters, numbers, and symbols. For example, consider an easy to remember passphrase that also reinforces good habits, like: I@lwaysEATmyVegg!s15
- **Keeping devices safe:** Establish rules about who is allowed to touch your children's devices. Practice saying "No" to strangers.
- **Identifying secure Wi-Fi networks:** Use flashcards to practice spotting the symbols that represent secure and unsecured networks.
- **Maintaining the privacy of social media:** Explain who can see social media profiles and practice finding and updating privacy settings online and in video games.

Learn more about how to protect your family from cybersecurity threats.

Small business cybersecurity.

Small businesses (less than 500 employees) are common targets for cybercriminals. Small and Midsize Businesses (SMBs) saw an increase in fraud of 13.6% from 2022 to 2023, and the trend is expected to continue. SMBs are vulnerable because they often lack dedicated IT staff—smaller school districts and healthcare organizations are also being targeted for this reason. Common threats small businesses face include social engineering attacks and ransomware, with generative AI and deepfake messaging adding greater sophistication that can be hard to detect.

SMB owners can protect their assets by implementing policies limiting their risk exposure. For example, the decision to allow staff to access sensitive materials from mobile devices should be weighed against potential risks, such as malware infection. Before working with any IT vendors, SMB owners should ask for references and check online reviews. A trustworthy IT partner can audit the business's current technology and make recommendations to reduce the risk of a costly data breach.

Basic cybersecurity protocols to follow include:

- Keeping all software up to date.
- Installing firewalls on all company devices.
- Making secure backups of all business-critical data.
- Teaching employees about evolving cybersecurity threats and what they should do to stay secure whether working at the office or from home.
- Emphasizing the dangers of phishing emails and malicious links.

Securing your accounts.

When thinking about cyberattacks, you might envision hackers creating viruses to access personal accounts and business networks. However, the vast majority (98%) of cyberattacks rely on social engineering. Social engineering and confidence schemes are designed to trick you into revealing personal information that will compromise your account security.

In most cases, cybercriminals deceive their targets into thinking they are interacting with someone trustworthy—a government official or bank representative for example. Scammers use emotional appeals, pressure, urgency, and limited information to trick people into providing the additional information necessary to access and gain control of the target's account or network. Generative AI makes a scammer's message even more convincing; they can even imitate images and voices of known individuals.

Take the time to ensure that you contact the business or organization via their official channels. Don't trust links and phone numbers sent to you unexpectedly. For example, a representative from your financial institution will never initiate contact and ask you for sensitive information such as your credit/debit card PIN, three-digit code, online banking password, or secure access code to verify your identity on a call or email.

Learn more about confidence schemes and how to protect yourself.

Protect yourself from cybercrime.

Dealing with identity theft can be incredibly stressful and may cost significant amounts of time and money. A proactive approach to identity security can save you from substantial disruption.

Password management best practices:

- **Use different logins, passwords, and login recovery methods for accounts with sensitive information.** If you use the same username and/or password for multiple sites, an attacker may be able to use information obtained from a breached site to access other sites across the internet. Automation makes this far easier and faster to test usernames and passwords across many sites.
- **Implement long, complex passphrases.** Phrases like "Ialwayseat2pizzas" are hard to guess, but easy to remember.
- **Use a password manager.** These are apps and browser plug-ins that make it easy to use complex passwords. There are paid options, but do your research and choose what works best for you. Avoid saving your information to a free password auto-fill site. A paid third party could be more secure and help you remember your passwords for every site.
- **Make secure backups of your data.** Create a file containing your passwords and store it in an encrypted folder on your computer. Never store your passwords as plain text. If you store your passwords on a physical piece of paper, place them under lock and key.

Use two-factor authentication (2FA) when possible:

- **Get a secure access code sent via SMS text or use a secure phone app that generates a one-time code.** In each case, you'll be required to use your password plus a secure code to access the account.
- **Consider using biometric sign-in capabilities if available.** Instead of managing different passwords and login information, biometrics offer a more complex and secure option that's more difficult to duplicate or hack.
- **When logging into your OnPoint account from an unregistered device,** you will always be asked to provide a second form of authentication in the form of a secure access code sent to a phone number on your account.

Strong password checklist.

(🔒 Password | 👤 Username)

WE ARE HERE TO HELP KEEP YOUR ACCOUNTS SAFE

At OnPoint, we take your account security seriously. Please be aware, OnPoint will never ask for sensitive information via phone, email or text. This includes requests for passwords, secure access codes, PIN or credit/debit card 3-digit codes. For more information, please visit onpointcu.com/security.

🔒👤 □ **Memorable.** Practice your username and passwords and commit them to memory so you're able to recall your credentials when you need them. Consider using a passphrase with symbols swapped for some characters. For example: "eYeL1kEf00+B@ll" is complex, relatively easy to remember and significantly more secure than "ilikefootball".

🔒👤 □ **Private.** Do not share your username or password with anyone—shared passwords increase risk of fraud.

🔒👤 □ **Unique.** Use a different username and password for each account—reusing or repeating credentials increases the risk of a fraudster obtaining your information. If an online retailer has a data breach, the credentials obtained from the breach may be used by a hacker to attempt to gain access to other accounts using the same information.

🔒👤 □ **Secured.** If you need to store your credentials, they must be stored securely. If you have a physical copy, keep it in a safe place—if possible, write down hints instead of the usernames and passwords. For digital storage, use an encryption device or storage service and commit a single strong username and password combination to memory.
If you use security questions, make sure that the answers cannot be found easily through social media or public records. Many people choose a random answer for security questions not actually based on personal information.

🔒 □ **Variety.** Make use of all available characters in your password, including lowercase letters, uppercase letters, numbers and symbols.

🔒 □ **Authentication.** If your password is guessed or stolen, two-factor authentication can create an additional layer of security. Often in the form of a short code sent via call or text to your phone number, dual authentication requires that a fraudster have access to your phone in addition to your username and password.

🔒 □ **Random.** A randomized password makes it harder for criminals to use computer software or knowledge of your personal information to guess your password.

🔒 □ **Updated.** Changing your passwords every three months can help secure your accounts, especially those holding some of your most sensitive information.

DOES NOT CONTAIN:

🔒👤 □ Birthdate, Social Security number, phone number

🔒👤 □ Names of friends, family, pets, favorite sports teams, etc.

🔒 □ Common terms or phrases (i.e., quotes, clichés, etc.)

🔒 □ Words from the dictionary

🔒👤 □ Adjacent keyboard combinations (i.e., qwerty, 456789, fghjkl)

🔒👤 □ Less than 10 total characters (letters, numbers, symbols)

How to protect your data online.

One of the most important cybersecurity considerations is deciding how and when to share your personal information online. Complacency or disregard for the value of your information could lead to falling victim to a scam. In some instances, willingly providing your information or credentials could leave you liable for financial loss.

For added security, you may want to consider adding identity theft insurance. Insuring your identity can help restore your finances and credit profile if you're ever a victim of identity theft. Discover whether identity theft insurance is right for you.

- Social media best practices
- VPN, Wi-Fi, home networks and browsers
- Spoofed accounts and bots
- Malware and viruses

Social media cybersecurity best practices.

Social media and email have opened up new opportunities for scammers. By posing as friends, relatives and businesses, they can trick their targets into giving away personal information.

☑ Consider privacy on social media:

- Personal information commonly used for security questions and contact info is frequently shared on social media. Minimize risk by updating privacy settings, deleting unused social media profiles, and strongly considering which details to share about yourself online.
- Don't post about your vacation on social media until you're home. Sharing your vacation photos at the moment might be fun, but it's also a message to criminals that your home is empty.

☑ Control how your data is shared with third parties:

- Whenever you sign up for a new online account, check the settings for an option to opt out of data sharing—the more companies that have your info, the greater your risk of exposure.

☑ Unsubscribe from unwanted or unnecessary marketing emails:

- Under federal law, anyone sending commercial emails is required to provide an easy method for opting out of future communications. Emails you receive without an unsubscribe option may violate the law.
- Major email clients like Gmail automatically generate unsubscribe buttons on marketing emails.

☑ Enroll in e-statements:

- Signing up for online billing statements from your creditors, financial institutions and utility companies can reduce your exposure to mail fraud.

☑ Offline, protect physical documents:

- Reduce your risk of mail fraud by installing a lock and surveillance on your mailbox, shredding your old documents, and using a secure mail receptacle.

VPN, Wi-Fi, home networks and browsers.

Cybersecurity considerations go beyond the personal information you share and use on the Internet. They extend to the very networks, browsers, and devices you use to connect to the Internet in the first place.

☑ Avoid open Wi-Fi connections:

- Unprotected Wi-Fi networks could make your web traffic and personal information vulnerable.
- Only sign into your online banking account over a secured network—a home or office network is best. Public networks can unintentionally put a user at risk because they are missing that added password sign-in layer of security.

☑ Update your home network and browser:

- Always keep device software and security patches up to date and consider adding browser extensions for enhanced security. Additionally, almost any router can do web filtering by using one of many different free or pay-for DNS services. You can also configure your router to use one of many DNS services to protect your entire home, usually for free.
- Don't forget about those smart devices. Technology has connected our appliances, cars, everything, to our home network. These smart devices can create vulnerabilities that let fraudsters access your home network.

☑ Browse the web through a virtual private network (VPN)

- A VPN anonymizes your web traffic by routing it through one or more servers across the globe. Since sites won't remember your information, you'll need to re-enter login credentials.
- Using a VPN can make some digital activities less convenient. For instance, as an OnPoint member, you can establish your devices as "registered". Registered devices can bypass the need for an additional secure access code to log in to Digital Banking. When using a VPN, you are unable to register your device and need to enter a secure access code each time you log in.
- Additionally, using a VPN may result in some financial institutions flagging your account under "suspicious activity," especially if the VPN routes you through other countries. To avoid your VPN creating a barrier to your financial accounts, we recommend establishing a VPN with a U.S. address.

Spoofed accounts and bots.

Scammers may pretend to be a person or organization you trust by pretending to call, text, or email you from an official source. These spoofed contacts can even appear legitimate through caller ID, SMS, or email.

Identify spoofed accounts or bots pretending to be people:

- **Check email addresses,** not just display names. For example, a message may claim to be from a company's customer service department, but the address will be something like "customerservice@intel.nowhere.xyz".
- **Check the email header** by clicking the drop-down option under the subject line. Look for suspicious addresses in the "return" and "sent from" paths.
- When in doubt, contact the supposed sender through a trusted channel to verify if the message is legitimate.

Malware and viruses.

Malware, also called a virus, is a malicious program that can make changes to your computer, access your accounts, or lock you out of your computer.

Common malware types include:

- **Trojan horse:** A program that appears normal at first, but then takes over your computer.
- **Spyware:** Programs that watch your activity and steal your passwords.
- **Ransomware:** A virus that locks up your computer until you pay a ransom.

Not all viruses make themselves known immediately. A malicious program might sit in your computer for a long time before accessing your information. That's why it's important to regularly scan your computer for malware.

Use a trustworthy security program to monitor your computer for suspicious programs. New viruses emerge all the time, so it's important to keep your security software up to date at all times.

Likewise, it's a good idea to keep your operating system and programs updated. As hackers find new vulnerabilities, software vendors create security patches to improve protections.

Stay vigilant and protect your data.

Criminals have an easier time stealing personal information online, but their illicit activity isn't limited to the web. Here are ways you can stay vigilant and protect your data.

✓ **Consider credit monitoring services.**

- There are many services available that monitor internet traffic for personal information posted on the "dark web," which includes web pages not indexed in search engines.
- These services also look for abnormal charges to your credit accounts.
- Note that these services can't prevent fraud and they won't correct mistakes on your credit report.

✓ **Place alerts on your financial accounts.**

- Set up text or email alerts to automatically monitor transactions and account balances.
- If you notice suspicious activity, take action immediately by contacting the financial institution.

✓ **Limit physical access to your devices.**

- Never leave your devices unattended.
- Set up passwords, PINs, and biometric authentication (e.g., fingerprints, facial recognition) on any device with access to your personal information.
- Ensure that your device is set to lock automatically after a short period of inactivity.

Stay vigilant and protect your data.

(continued)

☑ **Keep your login information private.**

- Never share your login data with anyone. Many people share media accounts for entertainment purposes, and although our recommendation is to never share login credentials, that's not always practical. If you decide to share your login credentials for entertainment sites, ensure that all passwords and usernames are unique from those that you use for your financial accounts.
- Don't store your passwords in unencrypted files (e.g., text files, spreadsheets).

☑ **Check for card skimmers.**

- Criminals can place skimming devices over ATMs, POS systems, and gas station pumps.
- Before inserting your card, check for loose pieces, hidden cameras, and fake keypads.

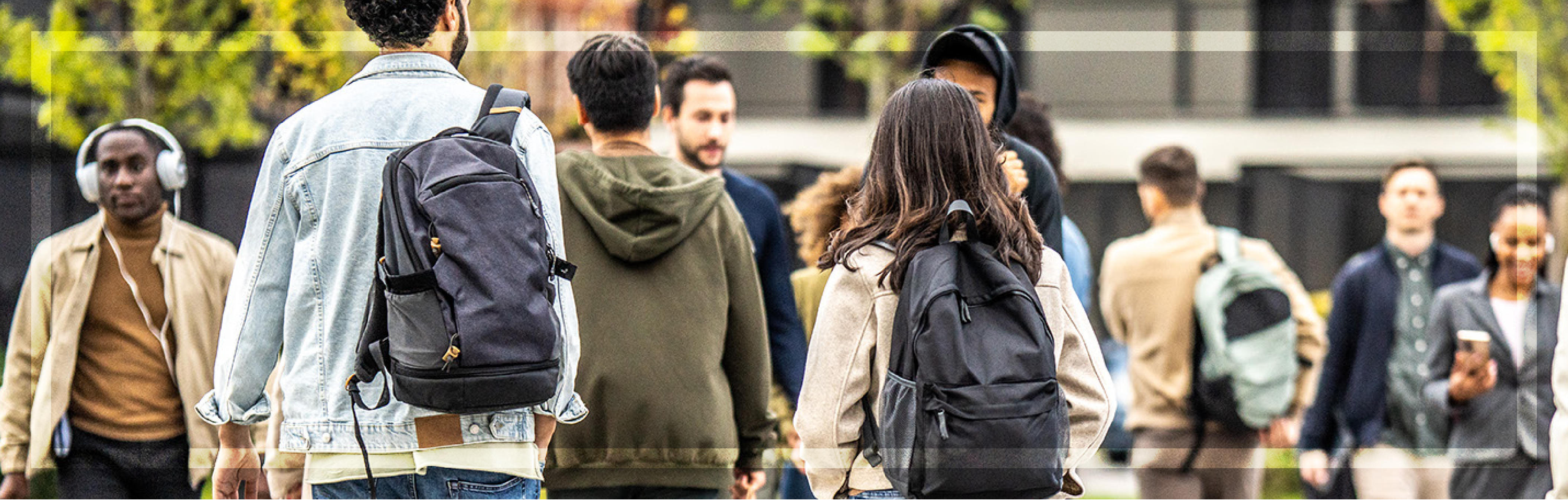
☑ **Monitor your credit report for unusual activity.**

- Regularly reviewing your credit reports can help you spot fraudulent activity before it takes a toll on your finances—get your credit report for free once per year from annualcreditreport.com.
- A child's social security number is vulnerable to identity thieves. Request a credit report for your child at annualcreditreport.com/requestingReportsInSpecialSituations.action
- Download our free credit eBook to learn how to easily understand your credit report.

Digital protection checklist

Considering how many ways there are for identity thieves to target consumers online, it's essential to make sure you have all your bases covered.

- ✓ Invest in a reliable password manager
- ✓ Use PINs and passwords on all of your mobile devices
- ✓ Set up two-factor authentication on sensitive accounts
- ✓ Create a safe word for family and work to protect against deepfake scams
- ✓ Review shared entertainment accounts and consider separate login credentials
- ✓ Sign up for e-statements from financial institutions, utility companies, and creditors
- ✓ Unsubscribe from irrelevant marketing emails
- ✓ Be wary of unexpected requests for urgent action, such as demands for payment or account details
- ✓ Review your data-sharing agreements with all organizations and social media sites with which you do business
- ✓ Sign up for a trusted credit monitoring service
- ✓ Learn how to identify account spoofing
- ✓ Keep your computer operating system and software up-to-date
- ✓ Keep your anti-virus software up to date
- ✓ Consider using a secure VPN connection
- ✓ Add physical security to your mailbox
- ✓ Make a habit of checking for card skimmers



Resources

Education is the first defense against identity theft, but help is always available. If you suspect you are a target for fraud or identity theft, follow the steps provided in this guide or notify your financial institutions and the credit bureaus of the suspicious activity.

Resources to prevent becoming a victim of identity theft

- The OnPoint Security Center
- Select a top-rated password manager
- Get your free credit reports
- USPS Informed Delivery Service
- How to choose a VPN

Resources if you suspect your information has been compromised

- Have I been Pwned?
- File a complaint with the FTC
- Oregon identity theft resources
- Washington State identity theft resources
- TransUnion credit freeze information
- Experian credit freeze information
- Equifax credit freeze information

Conclusion

Preventing identity theft and other forms of online fraud protects your finances and can give you peace of mind. Practicing good habits online can save you time and money in the long run.

Nevertheless, even people with the best cybersecurity plans are vulnerable to new and unexpected attacks. Knowing how to respond if you suspect fraud can reduce stress and help you resolve your issue quickly.

OnPoint Community Credit Union is dedicated to providing reliable and trustworthy banking services in person and online. We follow a clear set of guidelines each time we contact you about your accounts or share your information with our affiliates.

Stay up to date on the latest security news, review tips, and learn more about how to protect your information at the OnPoint Security Center.

OnPoint®
COMMUNITY CREDIT UNION

onpointcu.com

800.527.3932 | 503.228.7077

https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts
https://www.t-mobile.com/news/business/customer-information
https://firewalltimes.com/facebook-data-breach-timeline/
https://news.bloomberglaw.com/litigation/lawsuits-over-nelnet-data-breach-combined-into-single-proceeding
https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts
https://www.consumervoice.org/top-password-managers
https://reportfraud.ftc.gov/#/
https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing
https://www.ssa.gov/scam/
https://www.annualcreditreport.com/index.action
https://www.onpointcu.com/card-manager/
https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021
https://www.onpointcu.com/security/identifying-and-reporting-fraud/
https://haveibeenpwned.com/
https://www.onpointcu.com/blog/how-scammers-target-kids-online/
https://www.onpointcu.com/blog/the-biggest-cybersecurity-questions-for-parents/
https://risk.lexisnexis.com/about-us/press-room/press-release/20230305-small-and-midsize-business-lending-fraud-on-the-rise
https://www.onpointcu.com/blog/how-small-business-owners-can-teach-their-employees-about-cybersecurity/
https://www.onpointcu.com/blog/how-to-prevent-peer-to-peer-payment-fraud/
https://www.kaspersky.com/resource-center/preemptive-safety/how-to-choose-a-password-manager
https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity
https://www.nerdwallet.com/article/insurance/identity-theft-insurance
https://www.rightinbox.com/blog/security-chrome-extensions
https://www.comparitech.com/net-admin/network-monitoring-tools/
https://www.onpointcu.com/security/
https://usa.kaspersky.com/blog/cybersecurity-threats-for-kids-2024/29630/
https://www.fbi.gov/news/stories/elder-fraud-in-focus
https://www.ncoa.org/article/what-are-the-top-online-scams-targeting-older-adults/
https://www.forbes.com/councils/forbestechcouncil/2024/01/23/deepfake-phishing-the-dangerous-new-face-of-cybercrime/
https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network
https://www.experian.com/blogs/ask-experian/what-is-synthetic-identity-fraud-theft/
https://www.cisa.gov/news-events/news/protecting-against-ransomware
https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network