SECURITY FINANCIAL BANK

CYBERSECURITY

Security Financial Bank

www.sfbank.com • customerservice@sfbank.com

SFB Fraud Center: 800-237-8990

SFB Customer Service: 888-254-0615

Member FDIC

INTRODUCTION

Established in 1934, Security Financial Bank (SFB) is a locally owned community bank with $850 million in assets. Serving western Wisconsin with a focus on financial services for business and agricultural clients, SFB strives to provide products and services that exceed its clients' needs and guidance that enables them to succeed.

At SFB, we believe in doing everything we can to help our customers avoid cybersecurity threats. This helpful guide provides valuable insights into avoiding online threats and gives tips to protect yourself and your confidential information.

If you have any questions about your SFB account, please call **888-254-0615** or visit an SFB office near you.

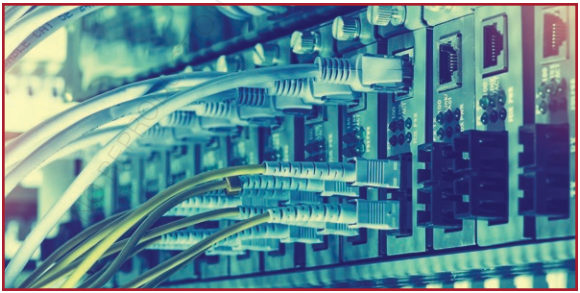
WHAT IS CYBERSECURITY?

The economic vitality and national security of the United States rely on interdependent and critical networks, systems, services and resources, also known as cyberspace. Cyberspace has transformed the way we communicate, travel, power our homes, run our economy and obtain government services.

A staggering amount of our personal information is stored in computers and therefore at risk of a cyberattack. Cybercriminals exploit our dependence on cyberspace and present dangerous risks to our economy and national security.

Cyberintrusions and cyberattacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations and hurting our economy. Cybersecurity involves protecting the information on which our nation relies by preventing, detecting and responding to attacks.

This guide outlines the types of threats most commonly found in cyberspace and ways to protect your computer system and personal information. It provides detailed information on the safe use of the internet, social networks, online shopping sites and mobile technology.



MALWARE

Malware are harmful computer programs that are transmitted through the internet, email or standard software installation. They are designed to take over infected computer systems and execute unauthorized tasks, including:

+ Displaying unwanted advertisements.
+ Accessing unwanted websites.
+ Tracking online activity.
+ Stealing passwords and personal information.
+ Compromising personal accounts.
+ Crashing computer systems.

The most common type of malware is called “spyware” or “adware.” Spyware can monitor nearly any activity or information on an infected computer. This includes temporary system data as well as files on the hard drive. Commonly targeted information includes the following:

Email Addresses

Email addresses can be extracted from an infected computer and used in spam mailing lists.

Keyboard Events

Key loggers record keystroke data before it is sent to the intended application.

Clipboard Content

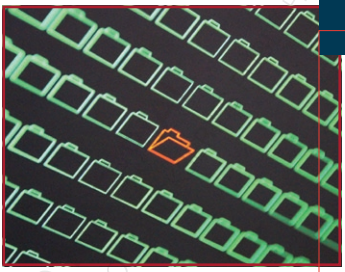
The system clipboard often contains sensitive information, including registration codes, data from recently modified documents and personal information that could be used in identity theft.

Network Traffic

Entire files can be extracted and reconstructed from this data, including usernames, passwords, emails and web content.

Many viruses act primarily as spyware, while others contain spyware features within them. Common examples are listed below.

Autonomous Spyware



Autonomous spyware operates as a separate process or injects itself into other processes on a computer system. It can be designed to perform almost any type of function, from monitoring emails to giving cybercriminals remote access to a computer.

Bot

A bot is a remote control agent that gives cybercriminals access to the infected computer as part of a bot network (botnet). Botnets can scan networks for vulnerabilities, install further malware and extract personal information, such as passwords, Social Security numbers and banking data.

False Antispyware Tool

Applications available online are often advertised as spyware detection/removal tools when, in fact, they themselves are spyware.

Hijacking Virus

Hijacking viruses modify browser settings so that users are directed to unwanted websites.

Web Bug

This type of malware uses standard web cookies that store authentication, preferences and other types of user information in order to track browsing habits and build individual profiles.

PROTECT YOURSELF

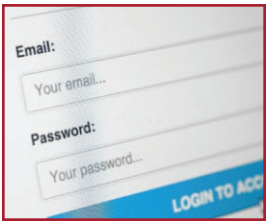
Follow these tips to protect yourself from viruses and spyware:

Keep a clean machine.
Having the latest security software, web browser and operating system are the best defenses against malware and other online threats. Make sure to keep all your software up to date and to install the latest patches to your operating system, especially those related to network and internet activity.

Protect all devices that connect to the internet.
Install trusted antivirus tools, and keep them up to date. Computers, tablets, smartphones, gaming consoles and other devices connected to the web all need protection from malware.

Plug and scan.
Universal Serial Bus (USB) keys and other external devices can be infected by malware, so always use your security software to scan them.

Configure your browser and email settings.
Configure your browser to block active content like ActiveX, Java, scripting, pop-ups and other potentially harmful content. You can also set your email program to send and display email using plain text instead of HTML. This greatly reduces the risks of infection through embedded script, web bugs and other HTML-based techniques. Many email clients (e.g., Microsoft Outlook, Apple Mail, Thunderbird) now offer the option to disable scripting and block images until the user authorizes their display.



Be mindful of what you download.
Hackers often use social engineering to trick people into installing malware, so exercise caution when downloading anything from public websites or newsgroups. Be especially wary of sites featuring pop-up windows or requests to install browser components and other applications.

Pay attention when installing applications.
If you decide to install an application from the internet, make sure you read and understand all license and privacy agreements. Information about monitoring functionality and additional software is often included in these documents. During the installation, make sure to read every instruction and look out for default options prompting your computer to install additional software. Remember that you are ultimately responsible for what you install on your computer or mobile device.

When in doubt, throw it out.
Links in emails, tweets, posts and online advertising are often used to compromise your computer. Regardless of whether you know the source, if it looks suspicious, delete the message or mark it as junk mail.

SPAM AND EMAIL SCAMS

Unsolicited commercial email, or spam, is the starting point for many email scams. The wide reach, convenience and anonymity of emails allow scammers to work in volume, as they only need to fool a small percentage of the millions of people they contact. Common scams include the following:

Trojan Horse Email

Trojan horse emails entice you with attachments that might interest you, such as jokes, photographs or patches for a software vulnerability. When opened, however, the attachment may:

+ Create a security vulnerability on your computer.
+ Give hackers access to your computer and files.
+ Install malware that monitors your online activities.
+ Turn your computer into a bot to send spam or spread the virus to other computers.

False Business or Investment Opportunities

These email messages present the opportunity to make easy money but provide very little detail about the nature of the business. These opportunities usually amount to little more than pyramid schemes encouraging you to recruit more people into the scam or attempts to get you to browse an unsafe website.

Health and Diet Scams

Health and diet scams lure consumers with promises of quick fixes and amazing results for common ailments. The products typically don't work and often serve as an excuse to get you to browse an unsafe website and leave your credit card information.

Online Con Games

Like traditional con games, these scams start with an initial bait, such as an email with a personal introduction and a call for an urgent response, and then progress with a series of forged documents and carefully crafted communications asking for money to pay made-up fees or bribes. The purpose of online con games is to trick the victims into transferring funds to the cybercriminal and divulging their personal banking information.

Phishing Email

Phishing email messages are crafted to look as if they've been sent from a legitimate organization. They often urge you to act quickly because your account has been compromised or your order cannot be fulfilled. Their purpose is to fool you into visiting unsafe, yet believable, websites so that you either download malware or reveal sensitive information, such as your account number, address, banking username and password, etc.

If you are unsure whether an email request is legitimate, contact the company directly. Use the information provided on an account statement or another official document; do not use the information in the email. Most institutions have policies against asking for personal account information by email, so you should be skeptical of any message that requests for your sensitive information.

PROTECT YOURSELF

Follow these tips to reduce spam:

Enable filters on your email programs.
Most email clients offer spam filters as well as ways to mark emails as spam so that similar messages are no longer delivered to your inbox.

Protect your privacy.
Hide your email address from online profiles and social networking sites, and only allow certain people to view your personal information.

Follow these tips to avoid falling victim to an email scam:

When in doubt, throw it out.
Don't trust any email sent to you by an unknown individual or organization, and never open an attachment in an unsolicited email, even if it seems to come from someone you know. Most importantly, never click on a link sent to you by unsolicited email. Instead, delete the email or mark it as junk mail.

Configure your email client for security.
There are a number of ways to configure your email client to minimize the risk of email scams. For example, viewing email as "text only" protects you from scams that use HTML.

Activate your firewall.
A firewall will not prevent scam email from reaching your mailbox, but it can protect your computer if you inadvertently open a virus-bearing attachment. Make sure your antivirus software includes an email-scanning feature and keep it up to date.

Make your passwords long and strong.
Set a different password for every account. When creating passwords, use both capital and lowercase letters, as well as numbers and symbols.

Use a password vault.
When using a password for each unique account, it's possible to end up with many different passwords that are hard to remember. Using a software-based password vault can help you securely store and update unique passwords.

Verify the website before sending sensitive information.
Always contact the company directly, using information provided on an account statement or another official document, not the email. Also, check the website's URL. Malicious web locations may look identical to the legitimate website, but their URLs usually have subtle variations in spelling or different domains (.com versus .net).

Follow these tips if you think you may be the victim of an email scam:

Report the incident.
If applicable, contact the network administrators so they can look for any suspicious activity. Consider reporting the incident to your local police department and filing a report with the Federal Trade Commission or the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center at: **www.ic3.gov**

Change your financial accounts.
If you believe your financial accounts may be compromised, contact your financial institution immediately to block any fraudulent transaction. Close any online account that may have been compromised.

Monitor your financial accounts.
Watch for any unauthorized charges to your financial accounts. Report any suspicious activity immediately. You may have to file a police report as well.

SOCIAL NETWORKS

Social networking sites such as Facebook and Twitter are a great way to stay connected with others, but you should be wary about how much personal information you post. Threats commonly found on social networking sites include the following:

Spam and Online Scams

Every email scam has its equivalent on social networking sites. What's more, some sites allow users to hide the URL when posting a link, forcing you to click on it to find out if it's a legitimate address.

Fraudulent Profiles

Cybercriminals may create a fraudulent profile to impersonate an official organization or someone you know to trick you into divulging personal information.

Data Collection

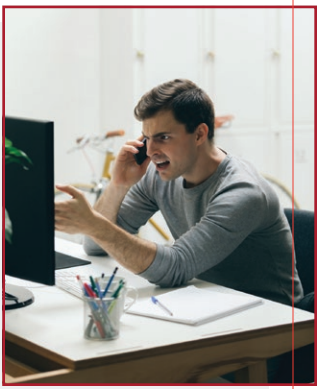
In some cases, cybercriminals don't even need to trick you. All the information they need to steal your identity, access your data or stalk you can be collected from your posts and those of your friends. Be aware of your privacy and security settings before you make a post.

Hacked Account

Cybercriminals can gain access to your account if you do not guard your username and password carefully. This information can also be stolen from the service provider or from your computer or mobile device through malware such as key loggers. Once they have control of your account, cybercriminals can:

+ Steal any confidential data associated with the account.
+ Send out spam and phishing messages to all your contacts.
+ View any personal information posted by your contacts.
+ Use your name to scam people you know and trick them into divulging personal information.

The following are signs that your social network account has been hacked:



+ There are posts you never made on your page. These posts often encourage your friends to click on a link or download an application.
+ A friend, family member or colleague reports getting messages from you that you never sent.
+ Your information was lost by way of a data breach, a malware infection or a lost or stolen device.

PROTECT YOURSELF

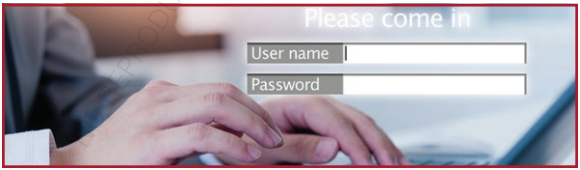
Follow these tips to keep your information private on social networking sites:

Familiarize yourself with the different settings.
Use the privacy and security settings on social networks. They allow you to control who sees what you post and manage the information broadcast about you. Make sure you read and understand the sites' privacy policies.

Keep your personal information private.
Be cautious about how much personal information you provide on social networking sites, and let your friends know if they are posting information about you that you would rather not share. If you have a lot of friends or followers, use the tools available to limit the information to which different groups have access.

Make your passwords long and strong.
Set a different password for every account. For more secure passwords, combine capital and lowercase letters with numbers and symbols.

When in doubt, throw it out.
As with email, never trust a message requesting your personal information or click on a link from an unsolicited message. If someone is harassing you, block him or her from your friends list and report the situation to the site administrator.



Follow these tips if you believe your account has been compromised or hacked:

Change the passwords to all of your related accounts.
It is crucial that you change your passwords immediately. Remember to set a different password for every account, and combine capital and lowercase letters with numbers and symbols to create a more secure password.

QuickTip

If you cannot access your account because the password has been changed, contact the web service immediately and follow all of their instructions to recover an account.

Alert your contacts.
Notify all of your contacts that they may receive spam that will appear to come from your account. Tell them to not open messages or click on any links from this account, and warn them of the potential for malware.

Scan your computer for malware.
If you believe your computer or mobile device is infected with malware, make sure your security software is up to date and scan your system with an antivirus program.

ONLINE SHOPPING

Online shopping is convenient, quick and easy, but it's important to protect your banking or credit card information when making a purchase. Common threats when shopping online include the following:

Malicious Websites

Some cybercriminals try to trick you by creating malicious websites that appear legitimate but really serve to steal your personal information or install malware on your computer.

Unreliable Sellers

Without a physical location for you to track, it is easy for less reputable sellers to take your money without living up to their end of the transaction. Some may even sell the personal information you provided during the purchase to marketing firms or cybercriminals.

Phishing

Cybercriminals sometimes attempt to gather information by sending emails requesting that you confirm your purchase or account information.

PROTECT YOURSELF

Follow these tips to protect your information when shopping online:

Keep a clean machine.
Before you add items to your cart, make sure your computer or mobile device is up to date with the latest security software.

Check out the sellers.
Research thoroughly before you supply any information to a seller with whom you have never done business before. Look for merchant reviews on independent sites, and note the phone number and physical address of the seller in case there's a problem with your transaction or bill.

Protect your personal information.
Before providing personal information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

Make your passwords long and strong.
Set a different password for every account. Always combine uppercase and lowercase letters with numbers and symbols to create secure passwords.

Make sure the transaction is secure.
Look for indicators such as the closed padlock on your browser's address bar and a URL that begins with "s-http" or "https." These indicate that the transaction is encrypted and secured. Never use an unsecured wireless network to make an online purchase.

Keep a paper trail.
Print and save records of all your online transactions, and review your credit card statements for discrepancies. If you find any unauthorized charge, report it immediately to your financial institution.

When in doubt, throw it out.
Never trust a message requesting your personal or financial information. Legitimate businesses will not solicit this type of information through email. Contact the seller directly if you are alerted to a problem. Use the contact information found on your account statement, not in the email.

HOME NETWORKS

Most households now run wireless networks of devices linked to the internet. This means that every device is connected to a wireless access point controlled by an internet router. Devices that may connect to a router include the following:

- Smartphones
- Tablets
- Computers
- Laptops
- Televisions
- Gaming consoles

To protect these devices and your home from cybercriminals, you must ensure that your wireless network is secure. Common threats to home networks include the following:

Piggybacking

Piggybacking occurs when cybercriminals in your area connect to your wireless network. This can lead to bandwidth shortages and illegal activity through your internet connection. That means any crime the hackers commit will be traced back to you.

Unauthorized Computer Access

If your wireless network is not secured, cybercriminals may access files on your computer, install malware or even take control of your computer. They may also monitor your internet activity to steal passwords and other sensitive information.

PROTECT YOURSELF

Follow these tips to secure your wireless home network:

Make your wireless network invisible.
Identifier broadcasting allows wireless devices to detect your home network as a potential access point. To disable this default option and make your network invisible to others, consult your router's user manual.

Change the router's name and password.
Change your router's default service set identifier (SSID) to a name that cannot be easily guessed. Create a strong password for your router (use a mix of numbers, letters and symbols).

QuickTip

Some routers allow for guests to use the network through a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.

Encrypt your network traffic.
Review your security options and choose the highest level of encryption available. Wi-Fi Protected Access (WPA) and WPA2 are more secure than Wired Equivalent Privacy (WEP).

Activate your firewall.
Most operating systems come with a pre-installed firewall. Make sure to turn it on to block cyberciminal activity.

Use file-sharing with caution.
If you don't need to share files on your network, disable file-sharing on all your computers. Otherwise, create a single dedicated directory for file-sharing and set a strong password for it. Never open your entire hard drive for file-sharing.

MOBILE DEVICES

Today's mobile devices are just as powerful as any personal computer, so it's important that you take the same online safety precautions with your smartphone and tablet as you do with your computer.

If you're using wireless technology outside of your home, you should know about the security threats you may encounter when using a public access point.

Evil Twin Attack

An evil twin attack consists of impersonating an access point to steal data from devices that connect to it. Cybercriminals who use this technique can steal a wide range of confidential information, including credit card numbers, addresses, usernames and passwords.

Wireless Sniffing

If your device is connected to an unsecure public access point, cybercriminals can use wireless sniffing tools to retrieve personal information such as your passwords, bank account numbers and credit card numbers.

Shoulder Surfing

Remember that, in public areas, criminals don't need a computer to steal your sensitive information. If close enough, they can simply glance over your shoulder as you type.

Malware specific to mobile devices also pose many threats. Known pitfalls include the following:

Smartphone Worms

These malware programs allow cybercriminals to hack smartphones from their own mobile devices anywhere in the world. The hackers are then able to:

+ Forward financial data stored on your smartphone.
+ Coordinate infected smartphones as part of a bot network (botnet).
+ Access your smartphone remotely and change the root password.
+ Configure your smartphone to install applications that are not officially distributed or approved by the manufacturer.

Spy Software

Once installed on the target device, spy software allows cybercriminals to:

+ Listen to phone calls as they happen.
+ Secretly read text messages, call logs and emails.
+ View the device global positioning system (GPS) location.
+ Forward emails to another inbox.
+ Remotely control all device functions through text messaging.

Cross-Platform Malware

Keep in mind that any threat affecting your personal computer may have a counterpart for mobile devices. This includes autonomous spyware, bots, hijacking viruses and web bugs.

PROTECT YOURSELF

Follow these tips to protect yourself when using a public wireless access point for your mobile device:

Keep a clean machine.
As with your personal computer, you should install the latest protections on all your mobile devices. Before downloading any new application, make sure that you understand its privacy policy and what data it can access.

Protect your personal information.
Only give out your cell phone number to people you know and trust, and never give anyone else's number out without his or her permission. You should also disable the geotagging feature on your device so as to keep your usual whereabouts private if you lose your device.

Lock your devices.
Cell phones and other mobile devices often contain a tremendous amount of personal data, and lost or stolen devices can be used to gather information about you and your contacts. Use a strong password to lock your devices.

Consider whether you really need to connect to the internet.
Disable wireless networking when you are not planning to connect to the internet.

When possible, connect using a VPN.
Many organizations offer a virtual private network (VPN) that allows employees to connect securely when away from the office. A VPN encrypts your connection and keeps out any unencrypted traffic.

Be careful of what you do online.
When choosing your online activities, keep in mind that most public access points offer unsecured, unencrypted network connections. If you can't connect securely using a VPN, consider avoiding the following activities:

+ Online banking
+ Online shopping
+ Sending emails
+ Typing passwords or credit card numbers

Disable file-sharing.
To prevent cybercriminals from gaining access to your confidential files, you should disable file-sharing when connecting to a public access point.

Be mindful of your surroundings.
When using a public access point, keep an eye on what's going on around you. Check if others can view your screen.

When in doubt, don't respond.
As with email, never respond to a text, phone call or voice mail requesting your personal information. With caller ID, you can block or reject calls from specific phone numbers or caller names.

CYBERBULLYING

Cyberbullying is the repeated use of information technology to deliberately harass, threaten or intimidate others. Cyberbullying can take many forms, and a single incident may fit into several categories. The following are the most common types of cyberbullying:

Cyberstalking

Harassing someone by repeatedly sending him or her insulting or threatening messages.

"Dissing"

Denigrating someone by sending or posting deliberate lies about him or her to intentionally damage the person's reputation and friendships.

Flaming

Participating in an online fight using electronic messages that are deliberately insulting and vulgar. Flaming can occur in either a private or public online group.

Outing

Distributing confidential, private or embarrassing information online. For example, a cyberbully may forward email messages or images meant for private viewing.

Because most cell phones have cameras now, many people are sharing private photographs and videos via email and text messaging and posting them on sites like YouTube, Vimeo and Facebook. These images and videos may involve unsuspecting victims in compromised situations.

PROTECT YOURSELF

Follow these tips if you or your children are being cyberbullied:

Don't add fuel to the fire.
Do not respond if someone sends you or your children a threatening message. If the behavior continues, ask the person to stop, but only once. Then block the person from contacting you or your family.

Preserve the evidence.
Save every message from the cyberbully as evidence that you or your children are being harassed. Also keep your message requesting the person to stop.

Contact the appropriate authorities.
If the harassment was by email, notify the online service provider. If it took place in a chat room, tell the organization that runs the server. Instant messaging and similar services all have harassment policies and provide information about what to do and who to contact if you're having problems with another user.

You may need to contact the police if the cyberbullying involves dangerous criminal acts, such as:

+ Threats of violence.
+ Child pornography and sexually explicit messages or photos.
+ Invasion of privacy, such as taking a picture of you or your children where privacy would be expected.
+ Harassment, stalking and hate crimes.
+ Obscene phone calls and text messages.
+ Extortion.

IDENTITY THEFT

Identity theft is when someone steals your personal information and uses it to commit fraud under your name. This serious crime can wreak havoc on your finances, credit history and reputation. There are several types of identity theft:

Tax-Related Identity Theft

An identity thief may use your Social Security number to:

+ Get a job.
+ Apply for government benefits.
+ Take your tax refund.

If you receive a notice that you were paid by an employer you don't know or that more than one tax return was filed in your name, visit the Internal Revenue Service (IRS) website at: **www.irs.gov/individuals/identity-protection** or contact them at: **800-829-1040** (individuals) / **800-829-4933** (businesses)

Financial Identity Theft

An identity thief may use your information to:

+ Open bank or credit card accounts.
+ Apply for loans or utility services.
+ Rent a place to live.

Check your credit report to see if your information is being misused: **www.usa.gov/credit-reports**

Medical Identity Theft

An identity thief may use your health insurance information to:

+ See a doctor.
+ Get prescription drugs.
+ File claims with your insurance provider.

PROTECT YOURSELF

Follow these tips if you believe that you are the victim of identity theft:

Change all of your passwords.
Set a different password for every account. Use capital and lowercase letters, numbers and symbols to make it secure.

Contact all affected organizations.
This includes any financial institution as well as government organizations. For example, if your Social Security number and driver's license have been compromised, contact the Social Security Administration (SSA) and your state Department of Motor Vehicles (DMV).

Close or freeze all compromised accounts.
Inform your bank and other financial institutions that someone may be using your identity, and review all recent transactions. Cancel any new account or charge that you did not authorize, and obtain new cards with new account numbers.

Contact the authorities.
File a report with your local law enforcement agency. Even if local police don't have jurisdiction over the crime, you will need to provide a copy of the report to your banks, creditors and other businesses. If funds have been stolen, contact one of the three credit bureaus so that they place a fraud alert on your file and prevent any further criminal activity.

QuickContact

+ Equifax **800-525-6285**
+ Experian **888-397-3742**
+ TransUnion **800-680-7289**

REPORTING A CYBERCRIME

We encourage Wisconsin citizens to report cyber incidents to the Wisconsin Statewide Intelligence Center (WSIC) by emailing **cybercrimes@doj.state.wi.us** or by calling toll-free at **888-324-9742** or locally at **608-242-5393**.

If you are the victim of a cybercrime, you should report the situation as soon as you find out about it. In addition to the WSIC, there are several resources available to you:

Local Law Enforcement

Regardless of whether the cybercrime takes place over multiple jurisdictions, your local police department must make a formal report and refer the case to other agencies, when appropriate. Some local agencies have departments that focus specifically on cybercrime.

Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center. IC3 reviews complaints related to cybercrime and refers them to the appropriate agencies. You can file a complaint online at: **www.ic3.gov**

Better Business Bureau

The Better Business Bureau investigates disagreements between businesses and customers. File a complaint online at: **www.bbb.org/consumer-complaints/file-a-complaint/get-started**

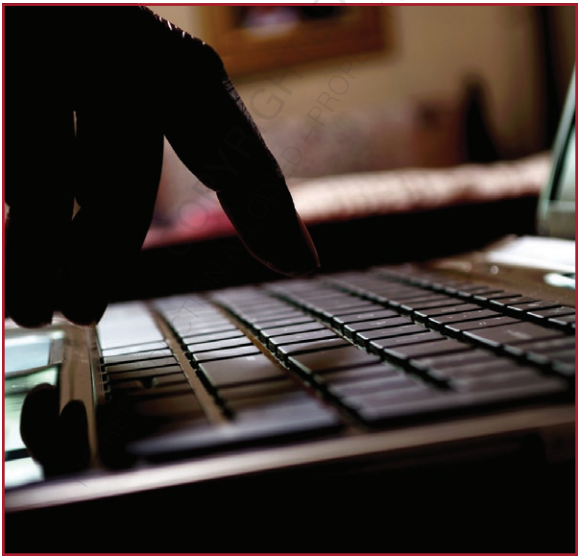
U.S. Postal Inspection Service

The U.S. Postal Inspection Service investigates fraudulent online auctions and other cases involving the mail. You can file a complaint online at: **https://postalinspectors.uspis.gov/contactus/filecomplaint.aspx**

Federal Trade Commission

The Federal Trade Commission (FTC) operates the Consumer Sentinel, a secure online database used by civil and law enforcement agencies worldwide to expose patterns of cybercrime. You can file a complaint online at: **www.ftccomplaintassistant.gov**

In cases of identity theft, call the FTC hotline at **877-IDTHEFT** or visit: **www.ftc.gov/idtheft**



COLLECTING EVIDENCE

Though evidence isn't always needed when reporting a cybercrime, it is important to keep all records relating to your complaint. Items that should be preserved include the following:

- Canceled checks
- Certified mail receipts and envelopes
- Money order receipts
- Wire receipts
- Chat room and newsgroup texts
- Credit card receipts
- Facsimiles
- Log files with the date, time and time zone
- Messages from Facebook, Twitter and other social networking sites
- Pamphlets and brochures
- Phone bills
- Printed or electronic copies of emails with full header information
- Printed or electronic copies of web pages

SECURING YOUR DATA

The first step to securing your information is to password-protect your different accounts.

Follow these tips when selecting a password:

+ Set a different password for every account.
+ Make each password difficult to guess and unique to you.
+ Choose at least eight characters, combining uppercase and lowercase letters with numbers and symbols.
+ Write down your passwords and store them in a safe place away from the computer.
+ Don't share your passwords with others.
+ Change your passwords several times a year.

Many account providers offer additional ways to verify your identity, such as code phrases or user-specific questions. Ask your financial institution and online service providers if they offer multifactor authentication or other supplementary security measures.

BACKING UP YOUR FILES

You should also protect yourself against data loss by making electronic copies of important files. Follow these steps to back up your electronic data:

Keep paper copies of all important documents.
Print out all electronic receipts and other important documents, and file them in a safe place that would likely survive a natural disaster.

Use your backup software.
Many computers come with a software program that allows you to make copies of every file and program on your computer. Other software programs are available for purchase if your system does not have a backup program or if you're seeking other features.

Make sure you run your backup program at least once before first connecting to the internet, and update your backup files at least once per week.

Select a reliable device to store your data.

+ **Cloud backup service:** This service is best to store an unlimited amount of backup data. When data is backed up to a reliable online provider, it can be accessible anytime it's needed and can be updated frequently.
+ **External hard drives:** These are best if your computer contains large files or serves as a library for many image, music and video files.

Safely store your backup device.
Keep your backup device somewhere safe away from the computer. Store it in a place that would likely survive a natural disaster or any other hazard.

QUICK TIPS

Since online technology is constantly evolving, the extent, nature and risks of a cyberattack are impossible to predict. Therefore, it is important that you always take precautions when connecting to the internet, whether you are at home, at work or in a public place, such as a school or library.

Follow these quick tips if you think you are the victim of a cybercrime:

- If you are at work and have access to an information technology (IT) department, contact the appropriate staff immediately.
- Verify that the software on all of your systems is up to date. If it isn't, install all appropriate patches to fix known vulnerabilities.
- Disconnect your device from the internet to prevent cybercriminals from accessing your system.
- Update your antivirus program and perform a full scan of your system. If you find an infection, perform a full system restore.
- If you believe sensitive information may have been compromised, notify the appropriate authorities, including your network administrators, if applicable.
- To report a cyber incident, contact the Wisconsin Statewide Intelligence Center at: **cybercrimes@doj.state.wi.us** or by calling **888-324-9742** (toll-free) or **608-242-5393** (local).
- File a report with your local police department so that there is an official record of the incident.
- Report any online fraud to the Internet Crime Complaint Center (IC3) at: **www.ic3.gov**
- Report any case of identity theft or consumer fraud to the Federal Trade Commission (FTC) at: **www.ftccomplaintassistant.gov**

RESOURCES

As online technology continues to evolve, it is important to stay informed of the latest threats. For more information on cybersecurity, consult the resources below.

Wisconsin Statewide Intelligence Center (WSIC)

WSIC serves as the state's primary focal point for threat information sharing among law enforcement, emergency management, fire service, public health, corrections, military and private sector partners. To learn more, visit:
www.wifusion.org / **cybercrimes@doj.state.wi.us**
24/7 Incident Reporting:
Toll-free: **888-DCI-WSIC (324-9742)**
Local: **608-242-5393**

Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is a coalition of private, law enforcement and government organizations focused on unifying the global response to cybercrime. Visit the APWG online at: **www.antiphishing.org**

Better Business Bureau

The Better Business Bureau investigates disagreements between businesses and customers. File a complaint online at: **www.bbb.org/consumer-complaints/file-a-complaint/get-started**

Federal Trade Commission

The Federal Trade Commission (FTC) operates the Consumer Sentinel, a secure online database used by civil and law enforcement agencies worldwide to expose patterns of cybercrime. You can file a complaint online at: **www.ftccomplaintassistant.gov**

In cases of identity theft, call the FTC hotline at **877-IDTHEFT** or visit: **www.ftc.gov/idtheft**

Financial Fraud Enforcement Task Force

The Financial Fraud Enforcement Task Force aims to improve efforts across the government to investigate and prosecute significant financial crimes and recover proceeds for victims. For more information, visit: **www.stopfraud.gov**

Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) reviews complaints related to cybercrime and refers them to the appropriate agencies. For more information, visit: **www.ic3.gov**

National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) educates and empowers the online community, promoting the safe and secure use of digital assets both at home and in public. For more information, visit: **www.staysafeonline.org**

Stop. Think. Connect.

Stop. Think. Connect. is a coordinated initiative of the APWG and NCSA. Its goal is to promote safer online habits in both the public and private sectors. For more information, visit: **www.stopthinkconnect.com**

U.S. Computer Emergency Readiness Team

The U.S. Computer Emergency Readiness Team (US-CERT) improves the Nation's cybersecurity, coordinates the sharing of information related to cybercrime and proactively manages risks to our infrastructure in regard to new technology. For more information, visit: **www.us-cert.gov**

U.S. Department of Homeland Security

The U.S. Department of Homeland Security (DHS) plays a key role in securing our online networks by partnering with operators of critical infrastructure systems and educating the public on how to stay safe online. For more information, visit: **www.dhs.gov/topic/cybersecurity**

SECURITY FINANCIAL BANK

CYBERSECURITY

As our web habits evolve, so have the strategies of cybercriminals. This guide highlights the security risks and threats that you need to know to use the internet and mobile technology safely, both at home and in public.

- Malware
- Spam and email scams
- Identity theft
- Threats to home networks and mobile devices
- Securing your information

Security Financial Bank

www.sfbank.com • customerservice@sfbank.com
SFB Fraud Center: 800-237-8990
SFB Customer Service: 888-254-0615

Member FDIC

The information in this guide is derived from recommendations from the Wisconsin Statewide Intelligence Center (WSIC), the Wisconsin Department of Justice: Division of Criminal Investigation (DCI), the Department of Homeland Security (DHS) and other U.S. Governmental agencies.

if you SEE | SAY something | something™

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

1-800-361-4653 | www.quickseries.com

01-0549-110-01 | 0549-015
ISBN 978-1-68423-956-6 | Printed in Canada