Privacy and Security: Staying Safe on the Internet

We are committed to protecting your privacy and safeguarding your personal and financial information.

Online banking makes managing your finances easy and convenient. However, there are some simple measures you should take whenever you go online to access your accounts.

Because your online security is our priority, we have compiled information and suggestions to keep your personal and financial information safe and secure.

SECURITY GUARANTEE

Our online banking system is safeguarded with the best security available in a commercial environment, ensuring that your information is protected while data is transmitted between your computer and our banking server.

Encryption

Internet encryption protects your information while it is in transit between your computer and our systems. Encryption ensures that data cannot be read or altered because the information is scrambled.

Our online banking website uses a 128 bit SSL, encrypting both request and response transactions, through a secure connection.

To establish a secure connection, make sure that the prefix of our website address in your browser reads 'https' (and not simply 'http'). All the browsers we support meet this requirement. If yours doesn't, please download the appropriate encryption support from your browser's supplier.

SAFE BROWSING

When visiting a branch, you can feel confident that your money is safe and secure. We are keeping you just as safe when you bank online but once your information reaches your computer, you have a responsibility to protect it.

Personal Access Codes (PAC): Keep Them Safe

Online credentials can be numerous as they are needed for email accounts, social networking sites, online newspapers and shopping websites.

That's a lot of usernames and passwords - and it can be tempting to use the same combination for everything. But this makes it far too easy for hackers because once they have one password, they can access all your sites.

Login credentials are the keys to your accounts so don't leave those keys around for anyone to find. For online banking, the key is your Personal Access Code (PAC). We recommend you:

- Choose a PAC that is easy for you to remember but difficult for others to guess. Avoid using current phone numbers, dates of birth, or social insurance numbers.
- Be smart and don't save a list of your credentials on your PC. If you have to write them down, keep these details locked away somewhere only you can access or consider using password-management software, which secures and encrypts usernames and passwords and allows you to use a single master password.
- Do not share your PAC with anyone, especially online. Employees of our financial institution will never call, email, write or ask you to provide your online banking credentials. Ever.

- Don't authorize browsers to memorize your credentials. Saving these on your computer allows anyone using your PC to gain access to your login-protected sites.
- Consider changing your PAC every 90 days for optimum security.

Monitoring Your Accounts

Make sure you review your account statements (whether online or on paper) on a regular basis.

Frequently reviewing your paper and/or electronic account statements ensures that you spot any incorrect or fraudulent transactions as soon as they occur.

If your card has been skimmed (when the card's magnetic stripe and PIN are fraudulently copied by embedded devices at ATMs or point-of-sale devices) or unauthorized transactions have been made, you will want to catch this as soon as possible.

Personal Details

When you move, it is important to notify us of your change of address. If your mailing information isn't up-to-date, statements or letters that contain personal information will continue to be sent to your former address.

Logging In and Out

When you are finished with your banking session, always log out by clicking the "Log Out" button, as opposed to simply closing the browser window. To help protect your information, your online banking session will end automatically if there has been no activity for a period of time.

If your session has timed out, no further transactions can be made until you log in again. This time-out feature helps protect your accounts from unauthorized access.

Clearing Cookies and Cache

When you spend time on the Internet, your browser stores information, such as the websites you visit, the images and files you view, and your personal information, including passwords and login details. This data is held on your computer's hard drive and is known as 'cache.'

Even though you may have logged out and closed your browser, this information may remain accessible. You can protect your data by clearing your browsing history regularly.

Learn how to clear the history in every browser you use.

Private Browsing

Some web browsers have a feature that allows you to browse the Internet without the browser storing information, such as the sites you visit, the images you see and videos you watch. This feature is sometimes used by people who share the same computer.

Private browsing is a temporary option and must be selected in order for it to be activated. Private browsing, however, does not give you immunity to spyware or make you anonymous. It is still possible for your Internet service provider, employer or the websites you visit to track your online activity.

INTERNET SCAMS

While pickpockets can only target a few people each day, Internet fraudsters cast their nets much wider, using the anonymity and reach of mass emails and fake websites. You can protect yourself from these situations by knowing how to identify and avoid these scams.

Phishing

A common way for Internet scammers to obtain your personal information is through a method called phishing. Usernames, passwords, banking information and credit card details are phished through email or instant messaging. Phishing works by sending communications, which appear to be from your financial institution, but they are not.

You are asked, supposedly by your financial institution, to log in to your online banking to verify account information. Often some type of security concern is cited as the issue. The fake email instructs you to click on a link that takes you to a non-legitimate version of your online banking site - one that is largely indistinguishable from the legitimate site - and you'll be asked to enter your credentials.

Phishing emails may include:

- Warnings about account closures
- Requests to update your information
- Offers to register for a new service
- Offers for pre-approved credit cards
- Free virus-protection programs

Once you click on the link, which directs you to a phishing website, you'll be prompted to enter personal or banking information. Phishing scams seek personal details, such as your address, social security number or mother's maiden name. The details obtained will then be used for identity theft.

Never provide personal details or any account details in an email. Electronic messaging is not a secure form of communication. If you receive a message that you are unsure about, please contact us.

Pharming

Another way for hackers to get their hands on your personals details is by pharming them. Pharming occurs when hackers use a malicious code on your PC, which compromises your computer's host file and redirects you to fake websites. The malware hides the fraudulent URL, cloaking it in the legitimate one that appears in your browser.

With pharming, the dishonest redirection of URLs happens even when you type correct URLs directly into your browser, making you think that you're on the correct website when you are not. Once there, you are asked to enter your online banking credentials or account information, which hackers take and use for criminal activity.

How to Avoid Phishing and Pharming Scams

We will never send you emails or communications asking you to verify or provide your online banking details. The best way to protect yourself is to never use a link provided in an email to access your online banking (because we don't send those; scammers do). Do not open emails or email attachments from unknown sources. Scan email through your anti-virus software.

Always type your financial institution's website address directly into your browser and remember to look for confirmation that you are browsing securely. The letter "s" in 'https' indicates you are navigating in a secure site, in comparison to the open and unprotected 'http' URLs. Look for the 'https' when online shopping, too.

Don't believe emails warning that your account has been compromised or that you'll miss out on a great deal if you fail to act immediately. If you are concerned, call or visit one of our customer service representatives.

Anti-Virus Software

Install anti-virus software on your computer to protect your information, money and privacy. Such software detects viruses and cleans your computer so that harmful viruses do not spread. Set up your anti-virus to run frequent scans and update the software as soon as it is required. Ensure you have real-time scanning of every email and every file you download.

Malware

Malicious software (malware), spyware, worms and Trojans are the same class of destructive viruses; just with different names. Nobody wants a computer virus. They can steal your personal information, take over your PC and use your computer to attack other people's computers. Your PC can become infected through email attachments, downloading infected content or visiting harmful websites.

Spyware

Spyware is exactly what it sounds like - tracking software that is downloaded to your computer (without your knowledge) when you visit certain Internet sites. Secretly, it gathers information about you and your browsing habits. This information can be trivial or it can include passwords and personal data that you wouldn't want criminals to get their hands on. It can also interfere with user controls and disable legitimate anti-virus programs.

The best way to protect your computer against spyware is smart browsing. Stay away from sites that look unsafe and avoid streaming or downloading content from untrustworthy sources. Many anti-virus products offer targeted spyware solutions that inspect your operating system, installed programs, downloads and files.

Scareware

One of the most common viruses to watch out for is known as scareware. These scams pop-up on your screen and display alarmist warnings, telling you a virus has invaded your computer. Scareware prompts you to download (and often pay for) fake anti-virus software to remove the non-existent viruses. Scareware is a scam that tries to trick you into paying money in exchange for nothing.

You can protect against scareware by keeping your anti-virus software up-to-date and by being judicious about what you choose to download to your computer. You should also familiarize yourself with the interface of your legitimate anti-virus program, so you won't be fooled if one of these pop-ups appears.

COMPUTERS & SMARTPHONES

We have created secure channel to communicate with our customers but you need to do your part by making sure your computer is virus-free and the operating system is kept updated.

Operating Systems

Your computer's operating system needs to be up-to-date in order to defend itself from viruses and malicious software (malware). If one part of your operating system develops a virus, it leaves holes in your PC's security defences and compromises the safety of the information contained in your computer.

Keeping your software up-to-date is one of the most important ways of staying safe online because it is much harder for viruses to infect an updated operating system and software. Hackers are targeting operating systems with new viruses all the time and software companies combat these efforts with security patches. You should always download the latest security patch as soon as it becomes available.

Your operating system lets you know when updates are available by notifying you there are new security features to download. You can also upgrade your operating system to the latest version available from the manufacturer; however, you should ensure your computer has sufficient hardware capacity to support an upgrade.

Remember to back up your data. To fully eliminate a virus that has infected your machine, the re-installation of your operating system may be required. Protect yourself against the permanent loss of important data by frequently backing up your files on an external hard drive so you'll have the data should you ever have a problem with your operating system.

Browsers

Web browsers are the gateways to the Internet. Similar to having an up-to-date operating system, upgraded browsers provide more features, stability and security.

The latest versions of web browsers have security features that can identify and block harmful and fake websites and pop-ups, and warn you if a site is flagged as unsafe. Some browsers also have a 'Private Browsing' feature, which conceals your browsing history from others.

Whether you use Internet Explorer, Firefox, Safari, Chrome or something else, stay safe online by using the latest version available.

Firewalls

A firewall protects your computer and home network from harmful websites and hackers. It sits between your computer and the Internet, scanning information that is being transmitted. It allows for safe browsing, while blocking unauthorized intrusions. Firewalls also stop your computer from being used by hackers to send malicious software to other computers.

Most computers now come with a firewall as part of the standard operating system. However, you can get the maximum protection for your computer by installing additional firewalls and ensuring they are kept up-to-date.

Protecting Your Smartphone

Browsing the web has never been easier - it's all at your fingertips. Smartphones let you surf, shop or bank wherever you are. Make sure your information stays secure while you're on the move by following these smartphone-safe browsing tips:

- Activate your phone's password feature, which locks the screen and prevents anyone but you from accessing your phone. Set up the password feature on your phone with a code that only you know.
- Don't connect to unknown networks through Wi-Fi hotspots to make financial transactions.
- Beware of smishing - that's phishing on phones through text messages. Never download media or images, or click on text-message links that come from unrecognizable people or phone numbers. Never provide personal details or any account details using any form of electronic messaging because this is not a secure form of communication. If you are unsure, please contact us.
- Download apps exclusively from the official source for your smartphone's platform, such as the Android, Apple or BlackBerry stores.
- Install anti-virus software for your smartphone when available and update it frequently.
- Install location finding applications, which work with your phone's built-in GPS. These applications allow you to locate and/or remotely erase (or "wipe") data in your phone if it is lost or stolen.
- Update your smartphone's operating system as soon as newer versions are available.

WI-FI & E-SHOPPING

These days, everyone is on the go and it's not uncommon to access Wi-Fi at coffee shops, hotels, restaurants or airports. Using wireless networks to access information is convenient, but not risk-free. Be smart when you surf. Protect yourself from threats by:

- Using only a trusted computer to access your online banking. Don't use shared library or cafe computers.
- Managing your online banking only from secure networks. We recommend that you don't use unsecured public networks for anything sensitive.
- Connecting only to password-protected networks. If there are several networks available, ask employees of the organization which network they operate.
- Never leaving your computer unattended, especially if you are logged into your online banking.
- Using different PACs and security questions as login credentials. If someone obtains your credentials for one site, such as a social networking site, you don't want them to be able to access your other ones.
- Ensuring you log out before you close your browsers.

Shopping Online

Online shopping is the epitome of convenience. There are no lines and no crowds, but it can also be a haven for fraudsters. Consider the following tips when using your credit cards online to ensure your information stays secure:

- Make sure that you are shopping at a trusted retailer when you enter your credit card details online.
- Provide retailers with only the necessary details to complete the transaction. These include your credit card number, expiry date, the security code on the back of the credit card and the card's billing address. Never provide your social insurance number, account details or your mother's maiden name. For shopping sites that require you to register with a username and password, don't use your online banking PAC.

- Use your credit cards only on e-commerce websites that use secure browsing technology on the screens where you enter your card information. Ensure the web address begins with 'https' (as opposed to 'http') and has a closed padlock icon on the screen.
- Ensure that smaller retailers requesting credit card details have reputable contact details, a physical address and you feel comfortable with providing them your card information.
- Never give your account or credit card details to anyone on eBay or Craigslist.

Our Privacy and Security Policy

For more information on the specific policies and practices that we use to safeguard your personal and financial information, please click here to view our Privacy Statement.