Staying Safe Online –
Tips to help prevent identity theft and cybercrime

Charter Bank is committed to ensuring the highest standard of security for our customers that use Charterbanker.com. Our security controls include multi-factor authentication and layers of security software and hardware.

While Charter Bank is dedicated to the highest standard of security for our systems, you as the end-user also play an important role in ensuring that you are adequately protected when you use the Internet. If you have any questions about your online experience at charterbanker.com, please contact your local branch so that we may further assist you.

To help you stay safe on the Internet, we recommend the following security tips and best practices.

Things You Should Do

Protect your password

Your password is as important as your Social Security number. The best passwords are ones that are difficult to guess. Try using a password that consists of a combination of numbers, letters (both upper and lower case), punctuation, and special characters. You should change your password regularly and use a different password for each of your accounts. Never share your password with others, and never reply to phishing e-mails with your password or other sensitive information. If you need to write down your password, store it along with any security tokens in a secure, private place. Charter Bank will NEVER ask you for your password or PIN.

Boost your computer security

Install anti-virus, anti-spyware and other Internet security software on your PC. Use it regularly and keep it up-to-date. Make sure the computer you are using has the latest security patches and take advantage of your PC's security features. Take the time to look at the program files and make sure there aren't unknown programs running on your machine.

If you have a wireless network at home, make sure to take the necessary steps to make it secure—such as not broadcasting your network name, requiring a password to connect and changing the default password on your wireless router.

Log out completely

Closing or minimizing your browser or typing in a new web address when you're finished using your online account may not be enough to prevent others from gaining access to your account information. Instead, click on the "log out" button to terminate your online session. In addition, you shouldn't permit your browser to "remember" your username and password information.

Use your own computer

It's generally safer to access your account from your own computer. Unfamiliar computers could contain viruses or spyware. **Before you use another computer**, make sure you will be able to delete all of the "Temporary Internet Files" and clear all of your "History" after you are finished.

Things to Remember

Watch for suspicious activity in your accounts

Have a plan in place to report suspicious activity to the appropriate parties. Follow your instincts—if it doesn't feel or look right, it probably isn't.

Be mindful that laptops and desktops aren't the only device receiving phishing e-mails

Cyber criminals are using cell and smart phones, social media sites and other digital and electronic devices to send phishing e-mails riddled with computer malware. Responding to suspicious phone messages or personal messages to your social media account could also compromise your information and security.

Don't respond to e-mails requesting personal information

More often than not, these are phishing e-mails that try to persuade you to give up your personal information and take immediate action! Legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as e-mail. If you have reason to believe that your financial institution actually does need personal information from you, pick up the phone and call the company yourself.

Understand social engineering

A social engineer is someone who poses as someone else in an effort to gain confidential information—an account number, Social Security number, password, computer credentials or bank account. Always know who you are talking to or doing business with on the Internet or the phone.

Understand the dangers of e-mail attachments

Attachments are the easiest method for a hacker to install a computer virus on your machine. Often the attachment is included in an unsolicited e-mail, but it's always a good idea to question the sender of the attachment and know what you are opening. The same goes for an embedded link in the e-mail that you are instructed to click on. Clicking on a link and entering confidential information could result in your information being compromised or stolen.

Understand what you download

When you download a program or file from an unknown source, you risk loading malicious software programs onto your computer or mobile device. Fraudsters often hide these programs within seemingly benign applications. Think twice before you click on a pop-up advertisement or download a "free" game or gadget.

Be mindful of working on an open wireless connection

Wireless networks may not provide as much security as wired Internet connections. In fact, many "hotspots"—wireless networks in public areas like airports, hotels and restaurants—reduce their security so it's easier for individuals to access and use these wireless networks. Unless you use a security token, you may decide that accessing your online accounts through a wireless connection isn't worth the security risk.

Refer to the **FAQ** section for additional questions.

Staying safe on the Internet and following the above best practices is paramount in helping you to protect your valuable assets. Security controls are continually implemented to protect customer and sensitive information. Sadly, the bad guys are just as diligent in hacking these controls, which makes our responsibility to follow safe online practices all that more important.

Frequently Asked Questions

1. **How can I avoid identity theft?**

   Never release personal or account information to unsolicited e-mails, telephone calls or text messages. Be cautious of who you give personal or account information.

2. **What should I do if I receive an e-mail, text or SMS message asking me to verify or provide my account or personal information?**

   Do not click on or select any embedded links in unsolicited e-mails or text messages as they could contain viruses or Trojan horses.

3. **What should I do if I receive a phone call, e-mail or text message telling me my account will be blocked, locked or closed if I don't respond immediately?**

   Do not respond directly to the solicitation or contact. Respond by calling or e-mailing the customer service number your financial service provider lists on your account statement or on the back of your credit or debit card.