Online Banking – Safety Tips

Keep your password confidential: Your password is your key to your web bank account. Sharing the password means that crooks can also access your online account. In addition, make your password as impersonal as possible. Do not use your date of birth, phone number, or your identity card number as your password. Change your password every four months and do not store it in your computer or other personal devices.

Beware of questionable e-mails: Crooks may also send you emails asking for your personal information such as a password or pin. As we noted earlier, as time goes by, they get smarter and smarter. They have designed fake bank logos and use them when sending you an email, you may be easily lured to give personal information. You can detect fake emails from these crooks because their emails usually direct you to questionable internet sites. In addition, you will notice that they do not address you as you are used to being called by your bank. The emails may also contain poor grammar.

Make use of anti-virus protection software: You should get the best quality antivirus protection available for your internet banking experience. They protect your personal information in your computer from being lost due to a virus. Search for the services of a computer expert to enable you to get the top rated services available.

If you discover you did submit private detail to these con artists, inform your bank immediately: Make sure you give your bank your current contact information so that they can get in touch with you with any questions or any other matters that require your attention.

Ensure you have strong computer expertise to improve the safety of your personal information: Otherwise, avoid shared computers.

If you notice that some money is missing in your internet bank account, notify the bank immediately: The more time that passes the more money can be stolen from you.

As use of the Internet continues to expand exponentially, banks and other financial institutions have increased their use of the Internet to deliver products and enhanced financial services, or simply to improve communications with consumers. The Internet offers the potential for safe, convenient, and new ways to shop for financial services and conduct banking business 24/7.

While it's true that the Internet has the "potential" for safe and secure financial transactions, safe banking online relies on you making good choices and decisions that will help you avoid costly surprises, or carefully crafted scams and phishing schemes. Despite all the hype concerning system security, we have learned that no such impenetrable systems exist. The inescapable fact remains; you are your own best protection while conducting financial transactions on the Internet. So it's important that you learn about, and take advantage of, **security features offered by your financial institution.**

Some examples are:

Encryption is the process of scrambling private information to prevent unauthorized access. To remind you that your transmission is encrypted, most Internet browsers display a small icon on your screen that looks like a lock or a key, when you conduct secure transactions online. Avoid sending sensitive information, such as account numbers, through unsecured e-mail.

Passwords, or personal identification numbers, should be used when accessing an account online. Your password should be unique to you, and this is extremely important, you should change it regularly. Do not use birth dates or other numbers or words that may be easy for others to guess.
Always carefully control to whom you give your password. For example, if you use a financial company that requires your passwords in order to gather your financial data from various sources, make sure that you are aware of the company's privacy and security practices.

General security over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers, or Internet service provider, to ensure you have the latest in security updates.

Tips on safe computing practices when conducting your online banking at home, or at a public computer:

- Never leave your computer unattended once you have signed in to online banking.

- After completing your transactions, ensure that you sign out of online banking, clear your cache, and close your browser. Often, it is easy to forget to sign out of an online banking session.

- Keep your password and card number safe. This seems like a no-brainer, but surprisingly many users do forget this critical step in the process.

- Do not share, disclose, or provide your bank card number, or password, to another party or website other than your bank. Most banks will not send you an email requesting this information. If your bank practices this very unsafe routine; you should change banks.
- Do not save your bank card number, or password, on a publicly accessed computer.
- If you do use a public access computer such as at an Internet cafe or public library, to be

safe change your password after completing your session by calling your bank's telephone banking number.

- When selecting a password, choose a series of characters that cannot be easily guessed by anyone else. The best passwords are made up of an alpha-numeric combination that's more than four characters long and a combination of capital and lower case letters.

For more information about safe internet banking visit the FDIC’s website. Our website also contains links to other websites providing information about Identity Theft and Tips to avoid scams.