

Tips for Secure Online Banking

How can you make your password more secure?

Your online banking password is the key to your personal and financial information. If criminals know your password, they can use it to steal from you or pose as you in online transactions. This newsletter will provide you with some simple tips to make your online banking experience safer.

Criminals will always gravitate towards the easiest money. The more barriers that you can put into place, the more likely the criminal will go elsewhere. The reason all financial institutions implemented new login procedures (known as multifactor authentication) a few years ago was to add a layer of security and deter criminals from your online account. Criminals adjust and so should you. Here are some easy Do's and Don'ts that you can use to steer criminals elsewhere:

Do's

Install a reputable antivirus software program on all computers and keep them current. This is **the single most important thing** you can do to protect yourself. While we do not endorse or recommend a particular product, some good solutions are Internet Security packages available from makers such as: Norton, McAfee, or Kaspersky.

Make your password as long and complex as possible. Our online banking system will permit you to create a password up to 8 characters long.

Make it easy to remember, but hard to guess. Use a combination of letters and numbers that you know, but that wouldn't make sense to others. Combine initials and important numbers and, if you are feeling particularly adventurous, a special character such as @ or # or \$ or & or *. A good password could be 17dg*wm4. How can you make a similar combination work for you?

Use more than one password. Use a generic password for low-risk situations such as a newspaper website where there is little risk to you if someone figures it out. Not every website warrants the same level of protection as your online banking website. To make your ever-growing list of passwords more manageable, consider using a general-purpose password for websites that do not contain personal or financial information, and creating a unique, secure password for each website that does, such as online banking.

Use trustworthy computers. Shared public computers like those in airport lounges, Internet cafes, public libraries, and hotel lobbies could be connected to keystroke loggers or infected with password-stealing viruses. Don't use them to access online banking or other websites containing confidential information about you.

Don'ts

Never e-mail your password or respond to an e-mailed request for your password or other confidential information. **We will never ask you to submit confidential information in an e-mail.** E-mail travels the Internet in much the same way as a postcard travels through the U.S. Mail. There is no "envelope" to protect the contents from prying eyes. There is no reason for anyone but you to know your password ever. Requests for your passwords via e-mail are most assuredly scams.

Do not include your login name in your password. Similarly, any part of your login name is a poor choice for a password.

Avoid predictable sequences of characters, such as "1234" or "abcd", in your password. Automated password crackers often start by guessing predictable sequences such as these.

Avoid dictionary words or names Words in any language can be determined by automated password crackers that also contain multi-lingual dictionaries. Similarly, password crackers also contain lists of names used as possible passwords. No one else may remember the name of your high school sweetheart, but if his or her name is on the list, your password may be vulnerable.