

General Security Tips

Passwords

Do not use your real name or your Social Security number as part of your username or password. Set a reminder to change your password on a regular basis, such as every 3 months. When creating a new password, use combinations of letters (Uppercase and lower case), numbers, and special characters such as #, & and @. Avoid using single words in a common language.

How do I create a strong password? One technique is to transform a phrase. For example:
Yankee doodle went to town: would be: YDW2town
Chicago is my kind of town: would be: CizmKot2
I dislike broccoli: would be: eyeH8brocolee

Another technique is to combine a word or phrase with letters and numbers:
Five barbequed chickens: would be: 5BbkewChicknz
Formative years: would be 4mativeYEARZ

The strongest passwords feature a combination of nonsensical letters, numbers and special characters. For example:

#1 – 5pN!!X99732\$
#2 – 78HK&302mmz

What passwords should be avoided?

- a correctly spelled dictionary word
- your, child or spouse's name
- sequential alphabetic/numeric strings
- phone numbers, licenses plate numbers
- street name

(Do not use any of the examples above for your password.)

Remember: Don't write down your password where they can be found. Do not share your password with anyone.

When selecting security questions, provide answers that are easy for you to remember, but hard for others to guess. Do not write down your security questions or answers or share them with anyone.

Other Security Hints

When you use a web browser like Internet Explorer or Firefox, it saves the password in memory as long as it is running, so remember to quit the browser when you are finished. This will assist in preventing any potential unauthorized access to your account information.

When using the web for transaction websites and shopping, be sure to shop with merchants you know and trust. Look for “secure transaction” symbols like a lock symbol in the lower right-hand corner of your web browser window, or “https://...” in the address bar of the website. The “s” indicates "secured" and means the web page uses encryption.

Always be careful when using public Wi-Fi spots, as they are not secure.

Keep your computer updated with the most recent web browser and operating system updates. Load anti-virus software on your computer. Some of these also include a firewall for further protection.