PASSWORDS

Your password is the key to your accounts! With your password, someone could gain access to your accounts, transfer funds, and steal your money. Hackers have developed a whole range of tools to get at your personal data. And the main impediment standing between your information remaining safe, or leaking out, is the password you choose**.** Knowing how to make a strong and secure password can keep strangers out of your accounts! This short tutorial can teach you how to create a password that is easy to remember, yet complicated enough to foil most security attacks.

Did you know? Your confidential information is probably not safe unless you use at least an 8-digit complex password. If you use less than 8 characters, and you restrict your characters to only alphabetic letters, it can be cracked in minutes.

How to create strong passwords

A strong password **should:**

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~ ! @ # $ % ^ & * ( ) - _ + =)

A strong password **should not:**

- Spell a word or series of words that can be found in a standard dictionary (e.g. angrybirds, mypassword, daisymae)
- Spell a word with a number added to the beginning and/or the end (e.g. johnsmith1, password123, daisy8703)
- Be based on any personal information such as user id, family name, pet, birthday, etc. (e.g. johnsmith, mydogrover, 10311978)
- Be based on a keyboard pattern (e.g. qwerty) or duplicate characters (e.g. asdfgh, aabbccdd, 456789)

Create a password that's easy to remember:

Rather than trying to remember a password created using various character types which is also not a word from the dictionary, you can use a passphrase. Think up a sentence or a line from a song or poem that you like and create a password using the first letter from each word.

A passphrase could be a lyric from a song or a favorite quote. An example of a strong passphrase is "Superman is $uper str0ng!". A nonsensical word can built using the first letter from each word in a phrase (e.g. C$200wpG., represents "Collect $200 when passing Go."). These typically have additional benefits such as being longer and easier to remember.

Each system or application may have different password restrictions or requirements. Unfortunately, some systems don't allow the use of special characters (e.g. ~ ! @ # $ % ^ & * ( ) - _ + =), so when you're confined to letters and numbers, you'll need to make extra sure the password you create is complex enough.

Check the strength of your password

It's a good idea to check the strength of the password you've created. Try using Microsoft's password checker: https://www.microsoft.com/security/pc-security/password-checker.aspx

You have an obligation to protect your online accounts and the information stored on your computer from unauthorized access. Creating good, strong passwords that are difficult or impossible to be discovered, and keeping them private, are important elements of computer security.

Your financial institution has taken strong measures to ensure the security and safety of your account and its overall online banking system. By staying alert to potential security threats and keeping in mind the suggestions listed above, you can help us keep online banking extremely safe and secure. Follow the good practices and use the knowledge we've provided here, and you will be much more prepared to enjoy the conveniences of online services with peace of mind!

These helpful tips are provided by www.infosightinc.com, a computer security company working with your bank as a responsible member of the community to help insure the privacy and security of your financial information.

KEEP YOUR PASSWORDS SAFE

Without a strong password, someone could gain access to your accounts, transfer funds, and steal your money. A strong password can protect your online accounts as well as the information stored on your computer. It's also important to know how to safely handle your passwords.

Whether you're online or offline, guard your password as you would guard the key to your house. We suggest you review the following password tips:

- Don't share your password with anyone, including supervisors, personal assistants, or IT personnel. Your password is yours alone.
- Never speak your password aloud. Others might hear you.
- Watch for shoulder surfers. Someone looking over your shoulder can discover a password.
- Don't keep a copy of your password in a desk drawer, on a monitor, or under a keyboard.
- Do not email your password to a co-worker, or offer anyone hints about what your password might be.
- Never write down your password. You wouldn't write down your PIN number for your ATM card, would you?

Be careful with shared computers

Cybercafe's offer a convenient way to use a shared public computer when you are away from home or office. But be careful. Public computers are okay for casual web browsing, but they are NOT okay for connecting to your email, which may contain personal information; to any secure system, like the office network or, bank or credit union; or for shopping online. If you must use a shared computer to log into a password-protected site, log out as soon as you're done, erase the browser history, clear the cookies and close the browser window. Make sure you leave the "remember me" box un-ticked when you log in, too.

Be careful with public WiFi connections

Even if you're using your own computer, your information can still be hacked at a WiFi hot spot. Use caution when doing any kind of online banking or shopping or activity that would require you to exchange sensitive data over the airwaves. The best way to protect sensitive information is to use a Virtual Private Network (VPN), which encrypts the data moving to and from your laptop.

Avoid shoulder surfers & phishing

Protect yourself against social engineers (unscrupulous people looking to harvest passwords) by never sharing your password or login information with anyone. A legitimate company will never ask for your password over the phone or via email, nor will they provide a link within an email directing you to the login page of their website.

What should you do if you think your password has been compromised?

Here are a few simple steps you can take to protect yourself if you think your password has been compromised.

- Change your password: do this for every other account that uses the same password
- Contact the affected companies: Call the company to notify them and keep a record of the call.
- Inform your email contacts: Criminals might harvest your contacts so they can use phishing techniques to send your unsuspecting friends and family malware-infected links or scams.
- Monitor your accounts: Review activity on your accounts and consider ordering a free credit report.

Taking these simple steps can help ensure that your password remains safe.

These helpful tips are provided by www.infosightinc.com, a computer security company working with your bank as a responsible member of the community to help insure the privacy and security of your financial information.