

# Your password: The key to your personal information.

Think of your password as a guard that stands between your personal information and potential online risks. Given the best protective armour, the chances of anything getting through are greatly minimized.

When you create passwords with combinations of letters and numbers that are unique for every one of your online accounts, you'll make it more difficult to unlock your identity – keeping your information safe and secure. You should password-protect all your devices: computer, laptop, tablet, smartphone, etc.

## WHAT MAKES A STRONG PASSWORD

Many people choose a password that's easy to remember – like an address, pet's name or special date – and use it over and over again. The thing is, attackers try these first because they're pieces of information that are easy to obtain.

**To protect your passwords online, follow these tips:**

- Use a combination of upper and lower case letters and at least one number.
- Include at least one character that isn't a letter or number.
- Be creative. Use the first letter of each word of a memorable sentence or phrase, then make it even tougher by changing some of the letters to numbers (e.g. use a "3" to replace an "e").
- Try a mix of your pet's name, your favourite numbers, the street you grew up on or other combinations.

## OTHER TIPS TO KEEP YOU PROTECTED

- Never use your name, birthday, driver's license or passport number.
- Commit your passwords to memory and don't store them on your computer or in your mobile phone.
- If a website or browser asks to keep you signed in, unclick that option and take the time to re-enter your password each time.
- Clear your browsing history or cache after online banking and shopping.
- If you get an email that includes a password you've just set up, delete it.
- Make sure sites are secure before you enter your password.
- Avoid using a single dictionary word.
- Stay away from things like words spelled backwards, misspelled words, and abbreviations that are easy to figure out.
- Don't repeat numbers (5555) and letters (bbbb), include simple sequences (abcdefg or 56789) or use letters that appear in a row on your keyboard (qwerty).
- Make sure that you change your smartphone's original default password.
- Change your passwords after implementing a fix or following being compromised.
- Use different passwords for different online accounts, especially those dealing with sensitive or financial information (banking online).

Keep in mind you don't have to have malicious software on your computer for your passwords to be compromised. If you log into a site without a secure connection (not an HTTPS site) through a public Wi-Fi network, your information may be wide open to anyone and everyone. It's impossible to know how many cyber criminals or threats are out there. But when you've done everything you can to protect yourself, you can feel a lot more confident about going online and enjoying all of the great things the Internet has to offer.