TELUS Keeping Your Devices and Accounts Safe PINs and Passwords

[TELUS Wise online basics 9. Keeping your devices and accounts safe: PINs and passwords]

[Female Narrator] The most important step you can take to protect yourself from identity theft is to make sure that only you can use your devices and your accounts. Phones, tablets, and some computers can be locked using a pin or password. A pin is usually a string of numbers. Whereas the password is a mix of letters, numbers, and special characters, like dollar signs, exclamation marks and question marks.

Setting up a pin or password should be one of the first things you do when you get a new device.

[Let's get started]

Otherwise anyone who picks it up can gain access to everything that's on it.

[Choose a personal identification number]

Once set up, you'll have to enter your PIN or password to use the device. On Apple devices like iPhones, tap settings, and then Touch ID and passcode. Passcode is their word for pin. It'll ask you to set a pin with six numbers, but you can also choose to make it shorter or use letters. On Android devices tap "Settings" and then scroll down to "Lock screen". Then tap "Screen lock type" and pick the type of lock you want. A pin, a password, or a pattern that you draw on the screen. It doesn't matter which one of these you choose, as long as you are able to lock your device in some way.

You will also need to choose a password when setting up an online account, like you do for email or social media accounts. Often people use passwords that are simple to remember, and they use the same ones across different accounts.

[Sign up]

Some of the most common passwords people use are things like "123456", "QWERTY" (that's the first six keys on the top row of your keyboard), "1111", the word "password", or a common phrase like, "I love my dog". Password such as these are not recommended, as they are easy for other people to guess. Other times people use passwords that anyone they know could guess, like their pet's name or their date of birth for example.

Here are three tips for setting strong passwords.

[1. Use a mix of letters, numbers and special characters]

First use a mix of letters, numbers and special characters. Most hackers, or people who break into other people's systems or accounts, use programs that try different passwords, including the most common ones. Because they're computer programs they can do this quickly and easily. Having a mixture of letters numbers and other symbols, like punctuation marks, can make this process more difficult. You can start with a regular word and replace some of the letters with numbers or other characters as shown here.

[b4n4n4$]

Use upper and lowercase letters, but don't always put the capital letter at the beginning.

[2. Longer passwords are stronger]

Second, make it long. Don't just use a single word. Programs that try to guess passwords often run through the whole dictionary. So even if you've changed a few letters into numbers or characters, they can still guess it. To prevent this, expand your word into a phrase. For example, turn bananas into

bananas are yellow or I like bananas. Most passwords don't allow spaces, so you can run the words together like this

[bananasareyellow]

then replace some letters in the new words with numbers or other characters.

[3. Use different passwords for different accounts]

Finally, use different passwords for different accounts and websites. Often sites and companies themselves get hacked rather than individual accounts. In these cases, when large amounts of data are stolen hackers can gain access to users' personal data, including passwords.

[Email Hacked Social Media Hacked Bank Hacked]

If you use the same password across multiple sites, it makes it possible for hackers to then access your other accounts. Remembering different passwords for different sites can be challenging.

One easy solution is to simply add the first and last letter of the site to the password, for example, for your Facebook account, you'd put an F before the password and K after

[Fb4N4N4$@reYe110w!k]

or you can change it around. For Amazon you could put an N before the password and an A at the end. You don't have to use this method exactly. You can put the letters in the middle or reverse them or do whatever you like. As long as it's a pattern you'll remember.

You can use this method for every password except for your email. Because you use your email address to sign up for most of your other accounts., it's the one that is the most important to keep private. You can use the same method to come up with a password, but make sure it's a totally different one from all your other accounts. Now, you only need to remember two passwords; the one that you use for your email address and the other one that you change slightly for each of your other accounts.

[Facebook Amazon Bank]

Another option is to use a password manager.

[Password Manager]

This is a program that handles passwords for different accounts. It creates a different, almost unbreakable, password for each account, and then remembers and manages each of your account logins automatically.

One, popular password manager that has a free basic version is LastPass.

[LastPass Simplify your life.]

Some internet browsers, like Chrome, also have password managers built in.

[Password Manager]

Password managers can be useful, but they can only solve the problem of having different passwords for different accounts. You still need to make sure you have a strong password for the password manager, because anyone who can log into it can log into all of your accounts.

[TELUS Wise]

For more information on online basics, check out the other videos in this series. Visit our website at telus.com/WiseOnlineBasics