IT Services Newsletter - May 2020

May 7, 2020

Security

Physical Computer Security

The internet is not the only way for somebody to steal your information. Locking your devices while you are away from them will create an extra layer of protection between your information and the people wishing to steal it. Avoid allowing your browsers to save account credentials. If somebody breaks into your computer, they will be able to log into any account that has saved credentials.

Quiz

You should share your passwords with:	**You should never:**
1. Trusted co-workers 2. Your boss 3. Nobody 4. Your friends Answer: 3 ***Why?*** *Treat each password like the key to your house – every time you share the password, it's like making a copy of that key.*	1. Leave a computer unlocked. 2. Write down passwords at your desk. 3. Use the same password for all accounts. 4. All of the above. Answer: 4 ***Why?*** *Locking your devices with both a physical and password lock is like locking a bike with two different types of locks – the added protection will reduce your chance of becoming the target of theft.*

If you believe that your computer has been accessed in your absence, contact **IT Services** immediately at **itshelp@selkirk.ca or 1-844-304-6500 EXT.55255**

5 Steps to Securely Work From Home

Some of you have been working from home for over a month now and are settling in to a new routine. Below are five simple steps to working securely and creating a cyber-secure home for your family.

Attackers have learned that the easiest way to get what they want is to target you, rather than your computer or other devices. If they want your password, work data or control of your computer, they'll attempt to trick you into giving it to them, often by creating a sense of urgency. The most common indicators of a social engineering attack include:

- **Urgency: Someone creating a sense of urgency, often through fear, a crisis or an important deadline. Cyber attackers are good at creating convincing messages that appear to come from trusted organizations, such as banks, government or international organizations.**
- **Policies**: Pressure to bypass or ignore security policies or procedures, or an offer too good to be true.
- **Contacts**: A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

Home Network: Almost every home network starts with a wireless (often called Wi-Fi) network which enables all of your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. Both work in the same way: by broadcasting wireless signals to which home devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

- **Change the default administrator password:** The administrator account is what allows you to configure the settings for your wireless network. An attacker can easily discover the default password that the manufacturer has provided.
- **Allow only people that you trust:** Do this by enabling strong security so that only people you trust can connect to your wireless network. Strong security will require a password for anyone to connect to your wireless network. It will encrypt their activity once they are connected.
- **Make passwords strong:** The passwords people use to connect to your wireless network must be strong and different from the administrator password. Remember, you only need to enter the password once for each of your devices, as they store and remember the password.

Not sure how to do these steps? Ask your Internet Service Provider, check their website, check the documentation that came with your wireless access point, or refer to the vendor's website.

When a site asks you to create a password: create a strong password, the more characters it has, the stronger it is. Using a passphrase is one of the simplest ways to ensure that you have a strong password. A passphrase is a password made up of multiple words, such as "*bee honey bourbon.*" Using a unique passphrase means using a different one for each device or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app that generates the code for you. Two-step verification is probably the most important step you can take to protect your online accounts and it's much easier than you may think.

Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software. Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to exploit them and hack into the devices you are using. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including not only your work devices but Internet-connected TV's, baby monitors, security cameras, home routers, gaming consoles or even your car.

Kids / Guests: Something you most likely don't have to worry about at the office is children, guests or other family members using your work laptop or other work devices. Make sure family and friends understand they cannot use your work devices, as they can accidentally erase or modify information, or, even worse, accidentally infect the device.

Security SuperStar!

May's Security Star winner is **Kyle Beres**. Congratulations and thank you for reporting your suspicious email to itsecurity@selkirk.ca Phishing emails today rarely begin with, *"Salutations from the son of the deposed Prince of Nigeria..."* and it's becoming increasingly difficult to distinguish a fake email from a legitimate one. Keep up the great work!

Other News

Zoom 5.0 Is Here!

Zoom Desktop Client has released its latest version 5.0 with enhanced security features. To update your Zoom to the latest version, click here.

Note: Beginning May 30th, all Zoom users must have the latest version in order to continue joining meetings.

Once you update your Zoom to the latest version, check out the new Zoom backgrounds that the Marketing & Communications Team have made available You will find a beautiful selection of Selkirk College campus' and Kootenay images as well as simple instructions on how to download them.

Working Remotely:

If you are requiring additional resources to make the shift to successfully work from home, please submit an IT helpdesk ticket with your request and supervisors authorization. We will do our best to help you in a timely manner.

Thanks for reading! Stay safe, stay healthy.