IT Services Newsletter - June 2020

June 15, 2020

Mobile Security

Smartphones have become popular relatively quickly, and mobile security has yet to catch up.

- **Stay Alert: When downloading applications, be aware of the access and permissions being granted to these applications to avoid sharing private information.**
- **Stay Updated: Make sure that all apps are regularly updated to prevent hackers from taking advantage of vulnerabilities present in older versions of the app.**
- **Stay Secure: When connecting to corporate networks remotely, use a VPN to help protect the information being shared between you and the company.**

If you believe that your mobile device has become compromised, contact IT Services immediately at itshelp@selkirk.ca or 1-844-304-6500 EXT.55255

Quiz	
Mobile devices should be: ***a) Locked with a password.*** ***b) Updated when updates become available.*** ***c) Use a trusted anti-virus app.*** ***d) All of the above.***	**ANSWER: D** ***Why? You want to protect both the outside and inside of your mobile device. On the outside, protect it with a password to prevent unauthorized access. On the inside, make sure that all updates are installed when they become available in order to prevent hackers from using bugs found in older versions to break into your device.***

Common Questions of the Month?

How do I update Zoom?

Either submit an IT Help ticket or join one of the IT Virtual Drop-In Zoom sessions. Links are found at https://go.selkirk.ca/ For more Zoom information, go to: Zoom for Staff and Students

Does IT supply webcams and headsets?

No, IT Services does not supply these items. You can contact the Castlegar Campus bookstore to inquire if they have any in stock. Alternatively, you can purchase one on your own from a local business or online.

How do I find my pay stub or request an absence?

Click the link below for detailed instructions:

Employee Resources - Absence Module

Review Your Unit4 Payslip

⚠ Your password for Unit4 may not be the same as your Novell password.

Where do I submit an IT Help Ticket?

Go to go.selkirk.ca and click "SUBMIT A TICKET" or click this link: Submit a Ticket

Case Studies You Can Relate To

Business Email Compromise [xxxii]

One type of wire fraud currently targeting businesses is the Business Executive Scam (BES), which is a type of phishing. The potential victim receives an email that appears to come from their employer's human resources or technical support department. Fraudsters create email addresses that mimic that of the real departments. An email message will be sent to the accounting department advising that the "executive" is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The "executive" instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses are typically in excess of $100,000.

IT Services is actively working on the migration from Novell and Groupwise to Microsoft 365.

As part of this migration ITS have temporarily enabled Microsoft OneDrive for staff and will continue enabling services as they are configured.

The projected service release dates (TBD) are as follows:

- Student O365 email and OneDrive access in September 2020
- Staff and student Office online access in September 2020
- Staff O365 email access in February 2021
- Microsoft Teams access in March 2021 (TBD)

Further release announcements, training and instructions will be made available at https://go.selkirk.ca/

Other News & Security Star Winner

Case Study - Remote Access Hacks - June 2014

Attacks involving remote access tools have gained attention since the massive 2013 data breach at Target, in which attackers broke into Target's point of sale (PoS) systems via a remote access account belonging to a Heating, Ventilation and Air Conditioning (HVAC) company.

Bluejeans is coming to an end!

As of July 1, 2020, IT Services will no longer be supporting Bluejeans as a video conferencing tool.

recently, hackers broke into payment systems at several northwestern U.S. restaurant od service companies via a remote access account belonging to a provider of PoS systems. In that incident, a LogMeIn account used by the vendor to remotely support and manage customer networks was breached and then used to plant data-stealing software on PoS systems belonging to the vendor's customers.

Security Star winner of the month is Jayme Jones!

Congratulations and thank you for reporting your suspicious email to itsecurity@selkirk.ca

Cybersecurity is a shared responsibility – people, processes, tools, and technologies work together to protect an organization's assets.

Quote of the Month	***A day without laughter, is a day wasted. "Charlie Chaplin"***

Thanks for reading! Stay safe, stay healthy.