**Cyber Security Basics**

**What is Cyber Security?**

Did you know that 95% of all cyber security incidents involve human error? Cybersecurity, also referred to as computer security or IT security, involves the methods of protecting computer systems, data, and networks from access to and attacks by unauthorized users. These attacks typically have a malicious intent, and frequently involve accessing and possibly stealing data or personal information, extorting money, or disrupting business operations.

In this handout, we will address some major concerns that young adults are being met with in the online world. Topics include:

* Passwords
* Social Networks
* Phishing
* Ransomware

For more information, visit our webpage at: [https://www.brandonu.ca/indigenous-cybersecurity/](https://exchange.brandonu.ca/owa/redir.aspx?C=0ehojr-CkQU7JTelCULhC8Ci70OYt8TdyjrFbQW_X76Kh3Ez96vXCA..&URL=https%3a%2f%2fwww.brandonu.ca%2findigenous-cybersecurity%2f)

**Passwords**

Passwords are keys to your accounts that protect your data and prevent illegitimate access to systems. You use passwords for many online services such as:

* Email
* Bank Accounts
* Netflix
* Facebook and other Social sites (Instagram, Twitter, TikTok)

When someone has your passwords they can:

* Impersonate you to request information
* Transfer your bank balance to their account
* Read your email for sensitive information
* Access healthcare details
* Use your email to send phishing mail
* Download your pictures

Always create strong passwords!! You can also use a password manager to store passwords. Here are some rules:

* Long and complex
  + At least 8 characters (longer is better)
  + Mix of upper and lower case characters
  + Include numbers and special characters
* Unique (not used for other services)
* Does not use personal references (pet names, birthdates, etc.)
* Does not follow a pattern or sequence

**What is multi-factor authentication?**

Multi-factor authentication involves not only using a password, but also a second form to authenticate your identity like a text message code, or an application request on a mobile. Some services now offer two-step authentication (may be opt-in): When you log in, you may:

* Receive a text message with a code to enter
* Receive an automated phone call (press a button to confirm)
* Get a application pop-up on your mobile device where the app was provided by the service

**Social Networks**

Lots of web sites, apps and programs (Facebook, Twitter, Snapchat, Instagram, TikTok, and many others) that many people use to connect with friends and family, often sharing very personal information. Someone can access social network sites in many ways, including, PC, Tablet, Mobile Phone. It is important that what you post is only seen by who you want to see it. Unless you specify, all social media posts are PUBLIC to anyone that has an account on that social network. This can be harmful for future jobs, unwanted private messaging, catfishing, and a variety of other problems. Every social network has privacy settings. Make sure your settings for each social network account you are on, are set properly.

**What are the risks?**

* Your personal information could be stolen by a cyber criminal, putting your identity and accounts at risk.
* The personal information you share could give cyber criminals enough to get your email address and password.
* Cyber criminals could gain access to any account that has a password recovery service and use any saved information to make purchases.
* Links in messages from cyber criminals posing as someone you know could be a part of a phishing attack trying to trick you into sharing personal information or contain malware that infects your computer.
* Geotagged photos are photos that have geographical information, like your current location, added to them – and today, most smartphones and digital cameras have a function that automatically geotags all your photos unless you turn it off. Geotags can expose where you live, when you're traveling and even what car you drive, which could make you a target for robbery.
* When you update your status with your whereabouts on a regular basis, you could tip someone off to your routine, and invite real-life threats like robberies, break-ins or stalking.
* If you add "friends" you don't know, you could become the victim of a scam.
* Apps deleted from your account may not be fully deleted – the creator may still have access to your information.
* If you don't have a strong password, others could gain access to your profile and pose as you – and potentially send out spam or fake posts that are damaging to you.
* Potential employers could search social networking sites to get a sense of your character. If you've uploaded damaging or embarrassing photos or posts to your social network account, you could hurt your reputation and your chances of employment.

Three of the easiest things you can do to be sure of your privacy on social networking sites are:

* Choose a strong password
* Take the time to set your privacy setting to control who can see what
* Always think carefully about any information you choose to share online

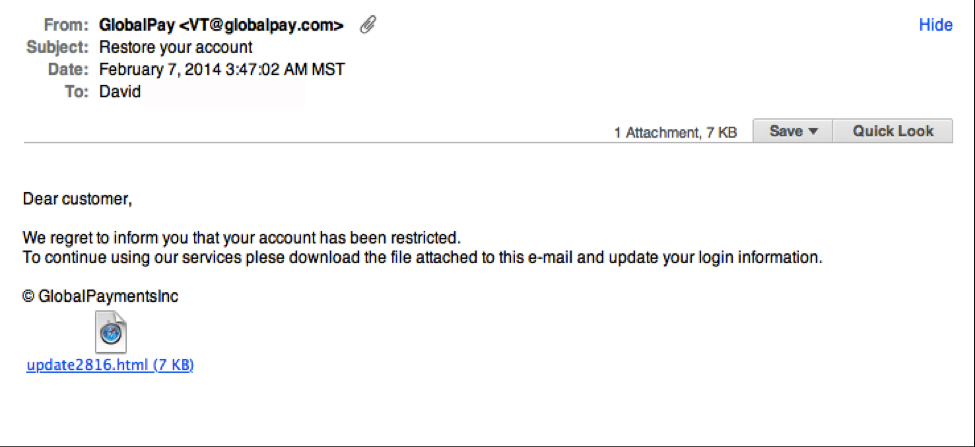
For more info, visit

<https://www.trustedreviews.com/news/facebook-privacy-settings-2939307>

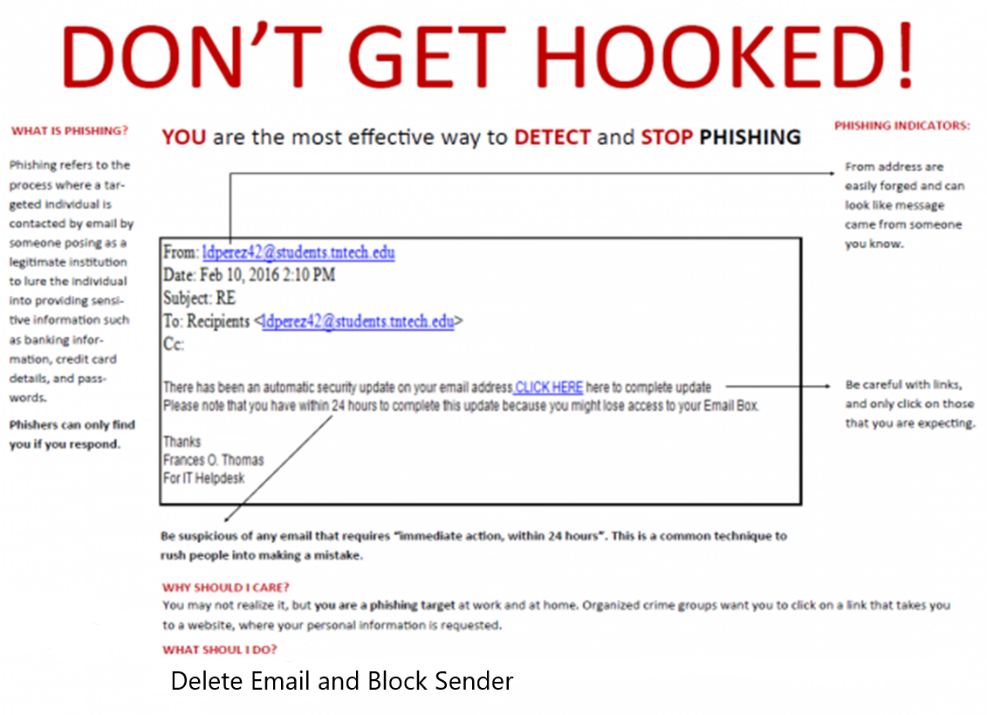


**Phishing – What is it?**

The process where a targeted individual is contacted by email by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details, and passwords



Messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or website with a broad membership base.

This technique has raised e-scams to a new level and has lately become the go-to choice for many attacks threatening individuals and businesses. Phishers can only find you if you respond. Please note that you are the most effective way to detect and stop phishing. Remember, if something looks too good to be true, it probably is. Legitimate organizations will not ask you for your personal information.

If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your school administrator immediately or tell your parents. Take this IQ Test!!

<https://www.sonicwall.com/phishing/>

**Malware**

Malware – malicious software – is any code or application that damages or secretly takes control of a computer system, device, or network. Malware is used to steal private information, disrupt businesses, and extort payments. Malware is a genuine threat to your website, to your business, and to your customers. Malware leads to:

* Website traffic loss – New customers are warned about your site and loyal customers stop coming back.
* Brand tarnishing – Your company's reputation – not just your website – is damaged.
* Consumer distrust – Consumers will not trust your website, business, or products and services.

Instead of overt internet vandalism and mayhem, today’s malware criminals stealthily infiltrate websites and home computers for illegal profit.

Their mission: Put malware on your site and spread the malware to your visitors for fraud and theft.

Your mission: Keep malware off your site and keep customers on your site!

**How is malware used?**

For illegal profit, consumer deception, website vandalism, and other criminal activities.

* Adware shows pop-up ads on infected computers and the attackers collect payment based on the number of times the ads appear.
* Spam is the bulk junk mail that everyone gets in their Inbox. Spam can be sent from malware-infected computers. The attackers collect payment based on the number of emails sent or on responses to the sales or information requests in the emails.
* Identity Theft and Info stealing capture private information, such as usernames and passwords, credit card and banking information, or social security numbers. The attackers can use the stolen data directly to impersonate the theft victim, or sell lists of stolen data within their crime network.

**How do I prevent a malware infection?**

Keep your computer clean, and backed up.

* Maintain an up-to-date backup of all your important files (USB thumbdrive)
* Keep up to date Malware/Anti-Virus protection of your computer.

Here is a good free option for malware protection:

<https://www.avira.com/en/free-antivirus-windows>