Information Security Branch

OCIO | Office of the Chief Information Officer

Information Security for Students

As a student you'll find that you are introduced to new technologies and social media platforms through your classes and your friends. There is a whole world of information out there to access and learn from, but you need to make sure you are safe first.

Keep your Accounts Secure

As school starts, you'll likely be swamped with different accounts for emails, learning systems and social media. Follow these simple tips to keep those accounts secure.

- **Keep different passwords for each account**. If one of your accounts is breached, you don't want someone getting access to the rest of your accounts.
- **Create strong passwords for each account.** Simple words and a couple numbers just doesn't cut it. Make sure to mix it up with symbols in the place of letters, and uncommon words. Don't use anything based on personal details that might be on your social media account.
- **Use password memory tricks.** If you are feeling overwhelmed with remembering all your passwords, based them on a common theme. That could be an idea, a story or anything. Just make sure that each password changes it up a bit.
- **Don't share your passwords.** It might seem like a simple thing, but you are held responsible for what is done on your account.

Be Careful Around Messages

The other thing you'll find in school is that your inbox will be constantly full of new messages. Whether you are dealing with texts, email, or messenger apps, make sure to ask yourself a few questions:

- **Does this involve money?** Whenever money is involved, you want to be extra careful around online messaging. There are a lot of scams out there that offer great deals or threaten you with costs. Verify who you are communicating with, and don't give any of your financial information online.
- **Do I know this person offline?** It is pretty easy for someone to create an account pretending to be a family friend or someone you met. People use these accounts to take advantage of your trust. Double check outside of social media that this is who you think they are.
- **Is this attachment safe?** Classes, friends, and organisations will have tons of stuff to offer you through digital attachments. Make sure to check if this is something you expect, and even if you do expect it, make sure to scan any files for viruses or malware.
- **Where will this link take me?** Links can be embedded in almost any kind of message these days, and that makes it really easy for someone to sneak in a malicious address. Hover over the link before clicking on anything and make sure that it is taking you where you'd expect.

Watch What you Share

Today’s online world thrives on shared information, but watch what you share. It might seem fun to share every detail of your life online, but you don’t always know who is watching.

- **Online photos and information can be used to impersonate you or as blackmail.** Keep privacy in mind when you share photos and information, and remember that social media is never truly private or secure, even when using private messaging.
- **Don’t share someone else’s information.** Even if something seems harmless, ask yourself if you’d want your own photos or information to be spread around the internet. Social media makes it really easy for things to multiply out of control, so it is important to take care of each other.
- **Read the ‘Terms Of Use’.** Many companies will sell your information and content to advertisers or worse. Make sure you know where your information could end up.

Keep your Devices Secure and Up To Date

Make sure that all your devices are password protected and up-to-date with the latest updates. So much is connected through your phones, tablets, and laptops, so make sure that they can’t be accessed by just anyone.

- **Wireless Devices.** Keep a password on any device that can connect wirelessly: (media systems, consoles, “smart” home devices, etc…). You never know who is on the network trying to get access.
- **Regular Updates.** Schedule regular updates on your phones, tablets, and computers. Keep the OS updated, as well as the software on those devices.
- **Entertainment Systems.** Look into the security settings of game consoles and entertainment systems. Many have integrated cameras and microphones and need to secured.
- **Anti-Malware Scans.** Run regular anti-malware scans on your devices to check for infection.

Further Reading

Center for Internet Security - Back to School
https://www.cisecurity.org/newsletter/back-to-school/
The College Student’s Complete Guide to Cybersecurity
https://www.pandasecurity.com/mediacenter/tips/college-students-cybersecurity/
University of Victoria – Information Security
https://www.uvic.ca/systems/services/informationsecurity/index.php
BC Government – Information Security Awareness
https://www.gov.bc.ca/informationsecurityawareness