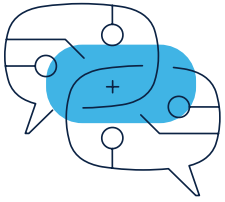


Working Remotely

Cybersecurity Tips



The recent increase of remote work arrangements for UBC faculty and staff has placed a greater risk to the security of UBC systems and information.

Follow these simple yet effective steps to increase security and privacy



- Ensure your primary work device has [full-disk encryption](#).
- Always [use myVPN](#) to remotely connect to the UBC network.
- Verify that you are properly enrolled with an [Enhanced CWL](#).
- Implement a [strong password policy](#) on all of your accounts and logins.
- Never leave your device unattended or on public display, and remember to log out when you're not using it.
- Beware of [phishing](#) and [spear-phishing emails](#) and text messages. Do not click on links or open attachments without verifying their source.
- Complete the [Privacy & Security Fundamentals Training](#) (disconnect from VPN before starting the training).
- Certify that all UBC files and data that you share with others is done so via a [secure file share method](#).