Your mobile. Be safe.

Protect yourself from thieves. Use strong passwords and encrypt your mobile device.

Almost all of us use mobile devices (smartphones, tablet computers, laptops and USB drives). Many of these devices are used to store personal information, which we have a duty to protect. Do you know how to keep the information on your mobile device safe if it is lost, stolen or hacked?

Personal information is recorded information about an identifiable individual which might include social insurance number (SIN), UBC student number and bank account information.

Personal information can be put at risk when it is shared or stored on unsecure devices making it vulnerable to loss or theft by hackers, which could result in identity theft or significant harm to yourself, others and/or the University.

Instead of downloading personal information onto mobile devices it is preferable to use your device to access the information remotely at the campus datacentre.

It's your mobile. Be safe:

- Keep software current and apply vendor provided updates and patches
- Protect your device with a password
- Use anti-virus, if available for your device
- Don't leave it unattended, even for a minute
- Use a Virtual Desktop Interface VDI to access personal information without storing it on the device

If it is necessary to access/store personal information on your mobile device:

- Encrypt the device and set it to automatically wipe after 10 bad passwords
- Keep the minimum data required
- Use secured network storage to share personal information

Avoid wireless hotspots with non-secure connections:

- Use **UBC Secure** where possible
- Use **MyVPN** to connect before transmitting
- Securely remove all personal information from your device when no longer required

Learn more: **it.ubc.ca/mobilesecurity**