DEVICE MANAGEMENT

TOP 8 TIPS FOR PROTECTING YOUR DEVICES

Queen's University
Information Technology Services

Your devices contain lots of sensitive information and personal data. It's important to take proper precautions in order to protect that information and keep it safe. Below is a list of **Do's** and **Don'ts** to ensure the security of your devices.

1 DO remember to lock your devices

Virtually locking your devices prevents unauthorized access by malicious actors.

2 DO keep your devices with you

Even if you are only stepping away for a moment, bring your devices along. Keep your eyes on your devices. Physically keeping your devices on you is your best prevention against theft and unauthorized access.

3 DON'T leave your devices in the car

Leaving your devices in a locked car doesn't always keep them safe. Better to keep them with you.

4 DON'T plug your device into free charging stations

Malicious actors can insert malware onto your devices through charging ports.

5 DO use only trusted Wi-Fi sources

Connecting to unknown networks can result in your internet traffic being monitored. Avoid connecting to public networks (ex. coffee shop) unless it is a trusted network - requires a unique login or is managed by someone you trust.

6 DO keep your Applications and Operating System (OS) updated

Keeping your apps and software up to date ensures that they have the most updated security features.

7 DON'T download unsafe applications.

Downloading suspicious content can infect your device and lead to data compromisation. Malicious apps and files can compromise your data and devices. Avoid pop-ups and ads and be cautious of shortened URLs.

8 DO dispose of your devices properly

Staff and Faculty can use the Queen's Secure Electronic Destruction and Disposal (E-waste) for unwanted electronic items. Students should make sure to follow best practices when disposing of devices. Don't just throw it away.

Note about Queen's Endpoint Protection

Staff and Faculty can enroll their devices in Endpoint Protection and let your IT personnel take care of many of these things for you. Enrolling reduces the risk of cybersecurity incidents and increases the ability for Queen's to respond to endpoint threats. It will also ensure devices meet our standards, ensuring users can have more confidence in their device security.