TOP STUDENT TIPS

TOP 10 CYBERSECURITY BEST PRACTICES

Queen's University
Information Technology Services

Welcome to Queen's! We know that adjusting to university can be a bit overwhelming at times. Here are the top 10 best practices to keep you cyber-secure and protect your digital identity.

1 Use a strong and unique password

Use a unique password for each account to prevent a single data breach from compromising all your accounts. Using a password manager can aid in securely storing and managing passwords across multiple accounts.

2 Use Multi-Factor Authentication (MFA)

MFA is an authentication method that provides an extra layer of security. Using MFA helps keep your digital assets, information, and user identities safe.

3 Keep your software up to date

Keeping software updated ensures it has the latest defense against malware. Install updates promptly for your device, browser, and other applications to stay protected.

4 Secure your device

Secure your device when not in use to prevent theft or unauthorized access. Always lock your device and avoid leaving mobile devices unattended.

5 Secure your network

Avoid unsafe or unknown networks to prevent internet traffic monitoring. Only use your device on trusted networks, requiring unique logins or managed by trusted individuals, to avoid risks in public places like coffee shops or hotels.

6 Be vigilant of phishing emails

Recognize phishing, where malicious actors trick individuals into sharing sensitive data or installing malware. Familiarize yourself with common signs and report suspicious emails promptly.

7 Avoid clicking on suspicious links

Stay cautious of suspicious URLs; avoid clicking untrusted links. Watch for numbers, misspellings, or odd endings. If doubtful, use a search engine or saved links to access the site.

8 Download from reputable sources

Explore the Queen's Software Center for numerous free resources and tools. Discover various applications and services available to students, including Microsoft and others.

9 Back up your data

Store and back-up files on OneDrive and Teams for free and safe storage, anywhere online access, and real-time collaboration. Routinely backing up your data to prevent loss of work through damage, lost, or theft of your device

10 Be mindful of what you share on social media

Be cautious when sharing and do not overshare personal information, such as your home address or phone number. This information can be used by malicious actors for identity theft, fraud, or other malicious purposes.