RECOMMENDED END-USER SECURITY PRACTICES FOR TECHNOLOGY USE

Definitions

Usernames are names identifying specific users of technology services.

Passwords are unique combinations of letters, numbers and symbols that function similar to a key.

Division Resources include access to information or applications, including but not limited to:

- Internet/Network access
- Email
- Student/Employee Personal Information
- School/Division Operational Information

Security Impact Assessments are formal reviews of a specific service, consisting of a detailed explanation of the potential benefits of the software and a formal risk assessment by a team that would need to include at least one member of Technology Services.

Mobile Devices include any technological devices with network capability which operate on battery power and are easily portable. This includes but is not limited to tablets, laptops, Chromebooks and cellular phones.

Managed Devices are devices which are subject to technical controls managed by the Technology Services department. This can include laptop and desktop computers, Chromebooks, Division issued cell phones and other devices.

Recommendations

Passwords

1. Users should avoid reusing passwords for both Division and external uses.

2. Users should change passwords on a regular basis, even if not forced to do so by a technical requirement.

3. Users should change passwords if they ever suspect that their password may have been compromised (e.g. they found a virus on their home computer which they use to access their email). This is in addition to notifying Technology Services of the potential breach.

Internet Security

1. Users should familiarize themselves with and utilize safe internet practices such as:

- Not clicking on links embedded within unsolicited emails, or emails uncharacteristic of the person who sent them. Among other potentially negative results, this is a common vector for the spread of Viruses or Trojans;
- Never providing any username or password to websites as a result of an unsolicited email or popup (this is a practice known as Phishing);
- Watching the URL (web address) of the site being visited. A site might "claim" it is the Bank of Montreal, but the actual web address is http://bankofmontral.com (this is an example of a practice known as Spoofing);
- Avoid providing your work email address to unnecessary services or posting it online. Both practices reveal that your email address is legitimate and may lead to an increase in Spam or Phishing attempts.

2. Users are responsible for familiarizing themselves with the basics of "Digital Citizenship". Resources to assist with this are located on the EICS website.

Maintaining a Clean Device

Users should monitor their devices closely for situations where unwanted software may be attempting to install itself and for noticing and acting upon warning indicators such as:

- Receiving warnings from known legitimate security software (i.e. the antivirus or other security software that is installed and monitoring the Device as per the requirements above);
- Receiving prompts to install "updates" unexpectedly while browsing the internet;
- Receiving prompts to purchase software to "clean discovered viruses" or "fix discovered problems";
- Experiencing unexpected behavior (e.g. excessive popups, unexpected toolbars or icons, errors, etc.) during or after a software installation;
- Requests for unusual permissions (e.g. an email app would appropriately require access to your contact list. A version of Solitaire would not).

Users are responsible for reporting potential issues to Technology Services (if a Division-owned laptop or desktop) or for ensuring that the device is inspected and, if necessary, cleaned by a professional (for other devices used to access Division information or Division resources).

Revised April, 2015