Patron Training (Tech Talk): Stay Safe & Secure

Lecture Outline

**Learning Objectives**

At the end of this program learners will be able to:

* Understand why passwords are important
* Understand what makes a strong password
* Know how to store their passwords
* Recognize when a website is secure
* Understand and recognize basic scams
* Un

**Time**: 1.5 Hours

**Materials**:

* 1 staff
* Handout: <http://wvml.ca/onlinesafety>
* PowerPoint

**Location**: Welsh Hall West

**Outline**

|  |  |  |
| --- | --- | --- |
| **Time** | **Content** | **Materials** |
| 7 – 7:05 | **Introductions & Outline** * Who I am:
	+ Digital Access Librarian
* What the seminar is for:
	+ Get the basics about passwords, computer and online security, keeping devices safe, and sharing personal information online
	+ Lots to cover – and this is the basics I have resources for more in-depth learning
	+ Time for questions and discussion at end
 | Slide 1: titleSlide 2: outline |
| 7:05 – 7:07 | **Passwords** (20)* They are everywhere! We have logins for everything.
* There are so many sites that we use and it is really hard to manage them
* It is important to create good passwords, and change them regularly
 | Slide 3: passwordsSlide 4: but |
| 7:07-7:13 | **Creating and Changing Passwords**1. Use more than 8 characters
2. Use different passwords for different services, use unique passwords for accounts with sensitive information, like your work email, your banking site, or any site with payment information.
3. Use longer passwords, as they are stronger than just using lots of character substitutions
4. Use the 1st, 2nd, or last letters from a sentence that you can remember.
	1. IE: What does the fox say?
	2. wdtfxsy?
	3. Add complexity: W#tfX5y?
5. Use a 'passphrase' two or more words put together that are unique and not easily guessed. They then can be combined with other words for different services
	1. IE: sundaylibrarian / greenlabradoodles / decemberflightbees
	2. Then substitute characters
		1. S/ndayL1brarian
	3. Can be used like:
		1. S/ndayL1brarianWork
		2. S/ndayL1brarianFacebook
		3. S/ndayL1brarianRavelry
6. Use several (4 or more) long words that are unrelated with spaces between them.
	1. IE: otter willow helicopter dancer
	2. Illustrated example <http://xkcd.com/936/>

**Do Not*** Use easy to discover words as your password, like the name of a spouse or child, your pet, or your name/surname.
* Use only 1-2 words from a dictionary without changes
* Use the same password for banking information/work email as you use for less secure sites (adobe, gaming sites).
 | Slide 6: Creating Good passwordsSlide 7: tipsDemo: techniques |
| 7:13-7:17 | **Other Password Tips*** Change your passwords - Try for annually – especially for banking and email
* Tiers –
	+ Unique ones for sensitive content (banking, email, government, etc)
	+ Lesser sets for social media (passphrase)
	+ “easy” ones for game sites, library ebooks, others that don’t have personal info.
* 2-Step auth
	+ Use when possible, this sends a text to your phone when you use a new device to access your account an “is this really you” check.
 | Slide 8: password tips |
| 7:17 – 7:25 | **Storing Passwords*** Apps/sites
	+ Lots out there – 1safe, lastpass, dashlane
* Physically
	+ Use an address book with hints
	+ Keep safe
* Most hacks don’t occur at your computer/person (although some do)
 | Slide 9: managing your passwordsDemo: LastPass |
| 7:25 – 7:40 | **Everyday Security** (30)**Computers*** Download and install system updates (all devices)
* Computers, have a firewall and anti-virus system
* **Viruses**
* **Malware:** software designed to damage or disable a computer
* **Spyware:** software that after installation
 | Slide 12: computers |
| 7:40-7:45 | **Wireless & Secure Sites*** If you are going to enter in personal information online always check for https: shttp
* Try not to share banking information over public wifi
* Make sure file-sharing is turned off
* Protect your own wi-fi! Use a password
 | Slide 13: wi-fi |
| 7:45-7:50 | **Apps*** Check to see if developed by a real company
* Look at reviews before you download
* Don’t download apps out of the respective official store
 | Slide 14: apps |
| 7:50-8:00 | **Email*** Pretty vulnerable
* Scams & Phishing: don’t reply to obvious bad emails
	+ Banks will never include a link to enter your password
	+ No one ever is going to randomly email you about receiving a great amount of money, if only you send them money first
	+ Hacked accounts of friends might sent out suspicious emails about needing money sent – try and contact them through a different method (call/text)
* Viruses: don’t open attachments that end in .exe, or aren’t expected.
 | Slide 15: email |
| 8:00-8:05 | **Physical Security** (5)* Remember passwords
* Device locks (software) – lock your computer when you step away
* Device locks (hardware) – laptop locks
* IEMI / Serial # - if phone/tablet is lost, helps police connect you with your phone, also knowing case colour, possible background image…
* Backing up data – not only for protection from physical accidents, but also loss, and a scam I’ll mention in a few moment
 | Slide 16: physical security |
| 8:05 – 8:10 | **Personal Information** (5)* Is it Safe to share?
	+ Mostly! So much goes on online, and most people never have an issue, but following the tips above will keep you safe
* Never: publically share credit card info, SIN, home address.
* Only trusted sites: phone number (usually only through person to person messaging like in facebook, craigslist)
* Pseudonyms: so some sites this might be best, like message boards, other places where you might be talking to strangers- dating sites, etc.
 | Slide 18: is it safe to share?Slide 19: Tips |
| 8:10-8:15 | **Scams & Fraud*** Ransomware: this is a scam that usually occurs on systems where
	+ Huge growth here
	+ Back up data you care about, keep backup

disconnected most of the time* + Keep computer up-to-date (many systems were XP)
* Text Message scams: growing issue. Don’t reply to unknown messages (report to your phone provider)
* Microsoft phone call: Microsoft will never call you. Do not engage with someone claiming to be from Microsoft.
* Craigslist/AirBnB – beware of sending money sight-unseen. Don’t accept a cheque for more than you asked for (it’ll bounce)
* Tickets: ask to see official receipts, or meet at ticketmaster to verify tickets
* Shopping online is fun, but always pay via Ebay, amazon, paypal – to protect yourself
* Many scams these days are dating related; protect yourself, avoid sending money.

Signs:* Spelling errors
* Appeals to emotion (oh, I can’t show you the apt, because….)
* But scammers are improving all the time (itunes, test)
 | Slide 20: Scams and Fraud |
| 8:15-8:20 | **3 things to do this weekend** (5)1. Change your passwords
2. Write down phone serial number
3. Run updates on all computers and devices
 | Slide 21: 3 things to do this weekend |
| 8:20-8:30… | **Discussion**1. What is your biggest concern?
2. What will you do to improve your personal security?
 | Slide 22: more information  |