APPLIED COMPUTING 1P01
Fluency with Technology
Security

APCO/IASC 1P01

Brock University
Protecting Yourself Online

Because our banking, personal information, and (for many of us) entire lives are integrated with the web, it makes sense that we should protect our online information about as carefully as we protect our homes and possessions.

We want to ensure that others can’t:

- Access confidential information
- Impersonate us
- Make orders, or starts services in our names
- Alter what we see
- Deny us service

Here’s a thought: suppose someone had stolen your Netflix login, but also had taken ownership of your email account. How hard would it be to cancel the service? How hard would it be to reclaim the service?
Sharing Passwords

Suppose your friend is helping to fix your computer, so she asks for your password.

- Do you tell it to her?
- Why or why not?
- Is there another way to handle it?

Who *can* you safely tell your passwords to?

- The *vast* majority of “hacked” accounts were either directly or indirectly connected to someone sharing their password!
Phishing

Congratulations! You’ve just won the Italian lottery! To collect, just tell me all of your banking information! Yes, I really do think you’re stupid enough to fall for this!!1!

- Scams are generally easy to spot, but some types of spam can be a bit sneakier.
- Obviously, if you get an email asking for your login/password, delete it
  - But what if they’re telling you to log into the legitimate website?
  - Is it the legitimate website?
  - Ensure that links are definitely valid
    - When in doubt: don’t use the link; go to the site yourself and log in manually

e.g. https://rbcroyalbank.com.g.ru/login.php?sessionid=38442184893&loginrequired=yes&refid=3xc7839486
Ads can be annoying, but are typically otherwise harmless. However, malicious software may be disguised as ads.

Similarly, you may see things like, *Downloader Required*, or *Codec pack*, etc.

Generally speaking, if you didn’t arrive at a page with the expectation of installing specific software... don’t.
Cookies and Sessions

We remember cookies, but do you know what a session is?

- Sessions are effectively just periods of time in which you can be considered authenticated, and continue to communicate.
- When you log in to a website, the server creates a new session, with a new session id. So long as that cookie is still on your computer, and the session hasn’t timed out, anyone using that computer is still “you”.

Oftentimes, websites won’t require a session timeout at all. If you still have the cookie tied to the last authentication, then you’re assumed to still be you.

- What websites do you stay permanently logged into?
- How much information could someone collect about you if they had access to your online profiles?
Using Public Computers

Have you ever used a public computer?
  - Think carefully... have you completed any of the labs for this course?
  - Although, do those really count?

When using a public computer, there are three major concerns:

1. Could anyone nearby see what you’re typing, or see any sensitive information on your screen?
2. Did you remember to click 'log out' when done? (Remember the last slide!)
3. Do you know what a keylogger is?
Password Selection

Each website has their own set of rules for what qualifies as a valid password.

- e.g. 3 of UPPERCASE, lowercase, numbers, and punctuation

As a general rule of thumb, pick something:

- Unique
- Hard to guess for anyone who knows you
- Easy for you to remember
- Reasonably long

Additionally:

- Never write your passwords down!
- Avoid the temptation to just add a '1' to your last password
- Don’t use really unusual characters (e.g. accents, esoteric Unicode characters, etc.)

http://xkcd.com/936/
Reusing Passwords
(again)

Ideally: Don’t do it.
Also: Don’t do it.

Not planning on following that advice? In that case...

- Keep your email password unique
- Keep your banking passwords unique
- Keep anything that stores credit card/banking information unique

http://xkcd.com/792/
Storing Passwords

Outside of your brain, where do you keep your passwords?

- **Written down?**
  - As mentioned, don’t do this!

- **In the browser**
  - Are passwords filled-in whenever the page comes up?
  - Is that really any safer than simply staying logged-in?
  - Is it *worse*?
    - Most browsers let you manage your saved passwords, and can even *display* them to you!

- **On a keyring (keepass, etc.)?**
  - *Usually*, these are fine, so long as they’re protected by your *securestest. password. ever.*
  - These programs can often generate new cryptographically strong passwords for you

- **On an external device?**
  - ... what happens if I find that device?
How Much of your Information is in Your Devices?

I hinted at this earlier... what would a person find if they were to find/steal your laptop, tablet, or cell phone?

(Worse yet, what if they got all three?)

How protected are these devices?
Open WiFi
(again)

Is anyone here still using BrockNet?

- Eavesdropping (packet sniffing) is remarkably easy
- It’s trivial to follow entire conversations, harvest personal information, and save files being transferred
- What might be the most important is knowing this:
  - Packet-sniffing and data harvesting are not limited to only a few nefarious nerds. It is unbelievably easy to do, and made easier by prepackaged (free) software that removes the requirement for expertise or domain knowledge.
  - Any idiot can do it.
Remember that HTTPS is simply the result of putting a security layer (SSL/TLS) between the TCP and HTTP protocols.

- In non-nerd-lingo, it means it’s just a normal webpage, but a bit of magic is squeezed in to provide:
  - Authentication
  - Confidentiality

So long as you aren’t receiving a warning (no scary red pages, no little ’X’ on the lock, etc), everything you’re sending should be safe from prying eyes. Also, you should really be communicating with the people indicated by the URL.

- It is for both of these reasons that you should *only* send credit card/banking information over HTTPS connections.
WEP
Wired Equivalent Privacy

WEP is the old standard of wireless encryption. Though still fairly common, it’s almost nonexistent in new wireless setups.

- The problem with WEP is that there’s a defect in the header of each packet, wherein a small hint is given that could (when collected with several other packets) be used to determine the wireless key (and gain entry to the network)
- Once they have access, they can both use your connection and eavesdrop on your communications (as if it had been completely open/unencrypted)
- So, how long do you have to use your wireless before someone else can break in?
  - About a minute
  - Though, even if you aren’t using it that long, there are other tricks to make it even easier
WPA
WiFi Protected Access

WPA/WPA2 are the newer standard that replaced WEP. Generally speaking, though it can be broken, there isn’t normally any reason to be too concerned.

- Think of wireless encryption as being like protecting a home:
  - House A is always unlocked
  - House B has a simple lock in the doorknob
  - House C has a quality deadbolt

- All three can be broken into. All three will probably be just fine. C is safer, though.
Why Should You Care?

Suppose you don’t care about anyone leeching off of your WiFi, and aren’t concerned about eavesdropping...

- Is there *anything* another person could possibly download on your internet connection that might get, say, the RCMP’s attention?
- Do you think, “that totally wasn’t me!” is the best defense possible?
- Do you want to find out?
Auditing Leases

Though few people bother to do this, one way to keep yourself safe is to actually take the time, every now and then, to verify that you really are keeping other people out.

- One simple thing to do is to look at the DHCP leases on your router, to see who connected recently.
A man-in-the-middle attack is one wherein:

- Abby *thinks* she’s talking to Bob
- Abby is *actually* talking to Trudy, who is talking to Bob
- When Bob talks to Trudy, Trudy relays that information back to Abby

So, what’s the problem?

- Trudy can read the conversation as it’s going along
- Trudy can *change* the conversation as it’s going along
Wait, so why are we talking about this?

- Suppose you’re using someone else’s access point
- Suppose that access point has a compromised DNS
- Suppose you go to https://www.facebook.com
  - Not to worry! If the certificate comes up, you know that Trudy is not listening in or changing anything!
  - Similarly, if it actually directs you to a different server, it can’t use the Facebook certificate!
  - But... would you really notice if you were redirected to a different domain?
    - Let’s look at a really simple example...
Additional Precautions

Feel free to look through the documentation of your modem and router, to see if there are special ways to guard yourself. However, there’s at least one thing that people tend to forget...

- What’s the login/password to your router?
  - Is it admin/admin?
  - Is it admin/password?
  - Is it admin/password1?
  - Is it admin/? (i.e. no password)

- Those are the most common combinations, because they tend to be the default login

- When you set up a new device, change the bloody password!

If someone does gain access to your network, you wouldn’t want them to install new firmware, or start directing all of your traffic to another computer, right?
Protecting Files

Encryption

There are lots of valid reasons to protect your files from prying eyes.

Do we really need to enumerate the reasons why “privacy is good”? 
Password-Protected Logins

Suppose you need a password to log into your computer...

- How safe do you think that makes your data?
TrueCrypt is a neat program for two reasons:

- It provides an easy way to encrypting files; you get to choose just how secure you need to make it
- It provides a handy-dandy way to storing stuff into single files of predetermined size
  - This makes it very easy to backup to some forms of removeable media
Mobile Encryption

Though most cell phones let you set up a password/unlock, and removing the media from a phone is typically much harder (outside of SD cards), that still doesn’t mean your data is safe.

Some programs simply *hide* the files (i.e. actually mark them as ‘hidden’, so a polite program will choose to ignore it), while others will actually move the file to another folder and encrypt it.

- e.g. Vaulty
Disposing of Personal Documents

Suppose you don’t want a file anymore. You drag it to the recycle bin.

- Is it really gone?

Suppose you ‘empty’ the recycle bin.

- Is it gone now?
Deleting a file simply tells the file system to forget where to find it; that data’s still there.

Shredding software actively writes random patterns of ones and zeroes over the relevant portions of the disk, so that they can’t be recovered.

- They can be used for individual files, or entire disks.

It’s generally a good idea to use such software before giving a computer to someone else.
Additional Concerns
i.e. Why to wipe

- Are you sure you got rid of everything?
- Lots of programs use non-standard folders
- Even when using encryption... Operating Systems tend to store temporary files elsewhere
- What about thumbnails?