MANAGING
your digital footprint

BY:CHLOE PAYNE AND MIKE WISEMAN
INFORMATION TECHNOLOGY SERVICES

Content Credit: This presentation has been adapted from the original "Managing Your Digital Footprint" presentation by Tamara Adizes Jacobs.

Where to start with risk ?

Educause security working groups say:

#1 Phishing & Social

#2 User Awareness

Managing Your Digital Footprint

=

Staying Safe

KNOWLEDGE IS POWER

SCARY STORY TIME...

"Stole my SIN, changed my name, charged my cards over $10,000..."

"Someone hacked into our baby cam and uttered profanities through the monitor while our baby was sleeping..."

"I was watched through my web cam...'

"Locked out of all University systems and demanded ransom to get the data back.."

IT'S EVERYWHERE

Your digital footprint is larger than you think.

It spans from your fitness bracelet, to your social media, to your audio streaming service, browsing and search habits to your hockey pool to your bank.
It's endless.

WHY DOES IT MATTER

"I have nothing to hide..."

It's true that you may not have anything to hide, but your digital footprint creates data about you that can be shared or leaked for commercial or malicious purposes.

AND...

HOW CAN YOU MANAGE IT ALL?

LET'S START WITH THE BASICS...

YOUR ONLINE PERSONAS

PERSONAL

The online version of you

PROFESSIONAL

Your online career profile

ALTER EGO

Aliases, avatars

01

PERSONAL

Your personal sphere includes everything from your banking, to your government dealings, to your shopping and photo sharing and online audio streaming and more.

02

PROFESSIONAL

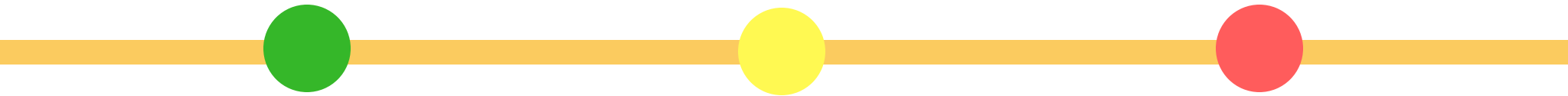
Your career snapshot. Most commonly it would include your website, university bio, your blog, your publications and/or online memberships to academic organizations.

03

ALTER EGO

The things you do online under a different name or an avatar...**But, how is this connected to your personal & professional spheres?**

WHAT'S YOUR COMFORT LEVEL?



Open Book

Somewhere in between

Super Secure

CONSIDER ADJUSTING YOUR SETTINGS

PRIVACY SETTINGS

The default privacy setting for most social media platforms is set to open. Before sharing, consider your comfort level and select your privacy settings accordingly.

PERMISSIONS

Before downloading any app take a moment to consider the permission settings. Do you want the app to have access to your camera, mic, or wifi connection info?

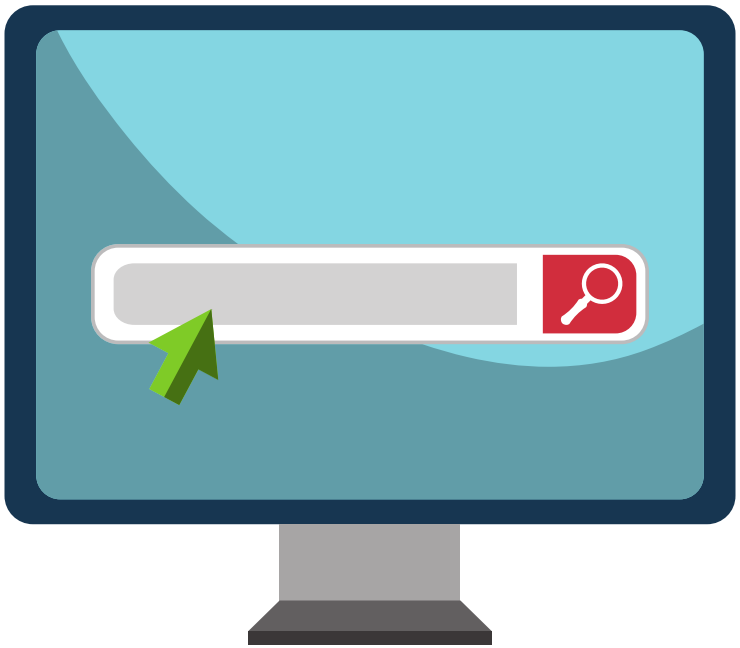
LOCATION

When using apps, consider whether they need access to your location. Often this is only a convenience and this info is often used for commercial offers.

SECURE YOUR BRAND

Maintaining your academic brand (your name) is important to you. Consider reserving your name space on common online services such as Twitter, Facebook, etc. If you don't intend to use it, just set the account to private and add it your list of accounts to maintain. Verify your accounts, if possible, to confirm your identify with each social media platform.

GOOGLE YOURSELF



When was the last time you searched your name?

It's good practice to search your name at least a few times a year and know what's out there with your name or picture on it.

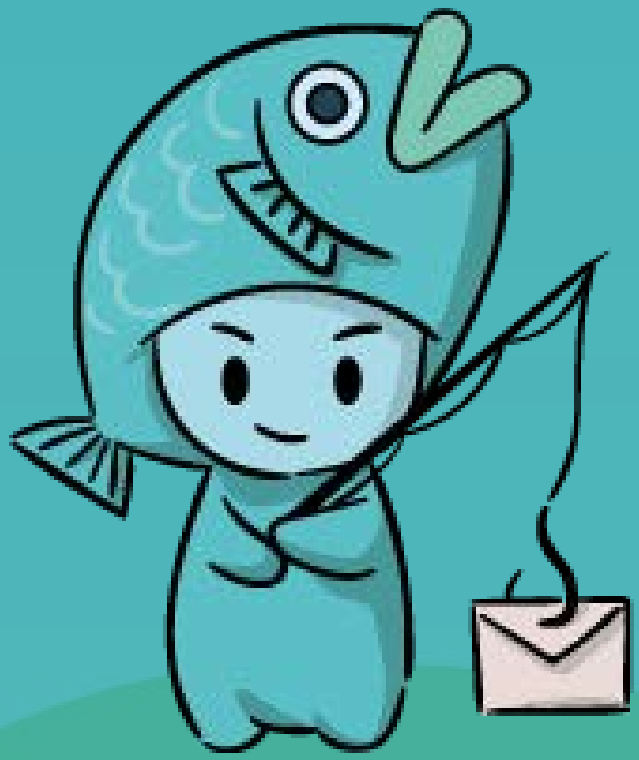
Subscribe to Google Alerts to automate this task.

KEEPING SAFE STATS

From a recent Microsoft RSAConference presentation:
90% of intrusions via phishing email

Verizon Breach Report:
Attacker sends 100 emails...
30 will open the email...
12 will open attachment or click on a link...
All within 3 min. 45 sec...

PHISHING



- install malware (malicious software, eg. ransomware)
- prompt for passwords
- messages that appear to be from your contacts
- text, phone calls
- spear phishing - targetted at you
- verify communications
- ask for assistance if you're unsure.

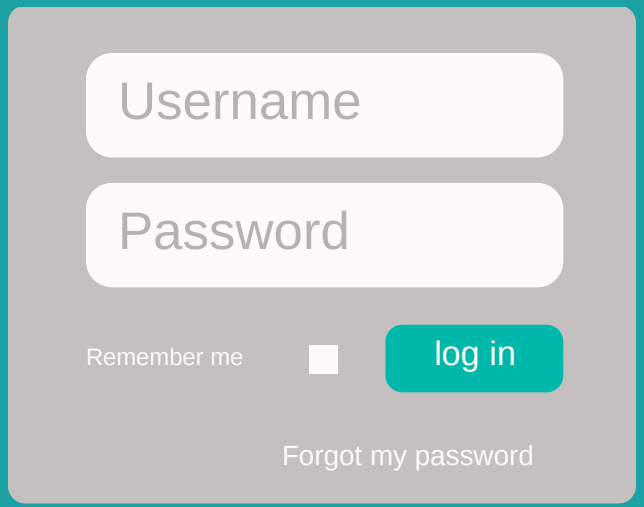
PASSWORDS

Strength:
8 char. for phone (with entry delay)

10-14 char. for desktop (use 3 of 4 char. sets)

15-24 char. for desktop (use passphrase)

Char. sets: upper, lower alpha, numeric, special



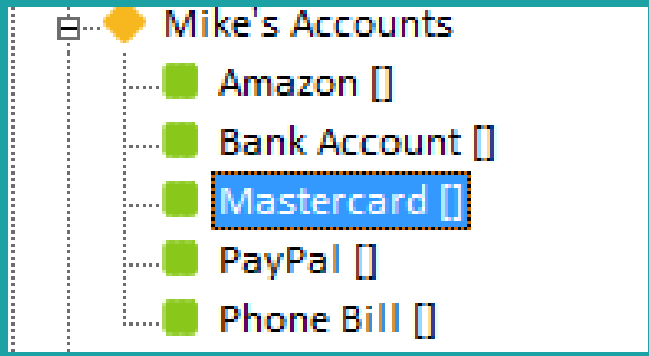
PASSWORD MANAGERS

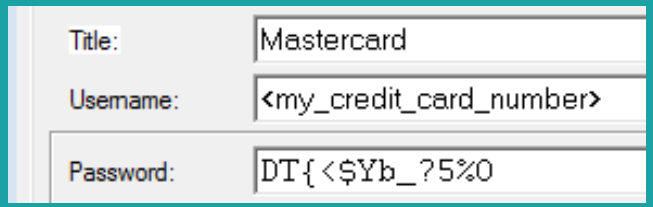
Store tens, hundreds of accounts.

Convenience of a list of bookmarks.

Auto fill-in username and password.

Examples:
Password Safe
Keepass





STAYING SAFE ON SOCIAL MEDIA

- multifactor authentication in Google, Facebook and Twitter.
- Service to monitor (and fix?) social media attacks - ZeroFox
- review privacy and security guidelines for the provider (see next slide).

STAYING SAFE ON SOCIAL MEDIA

https://www.facebook.com/about/basics

https://help.twitter.com/en/safety-and-security/account-security-tips

https://help.instagram.com/369001149843369

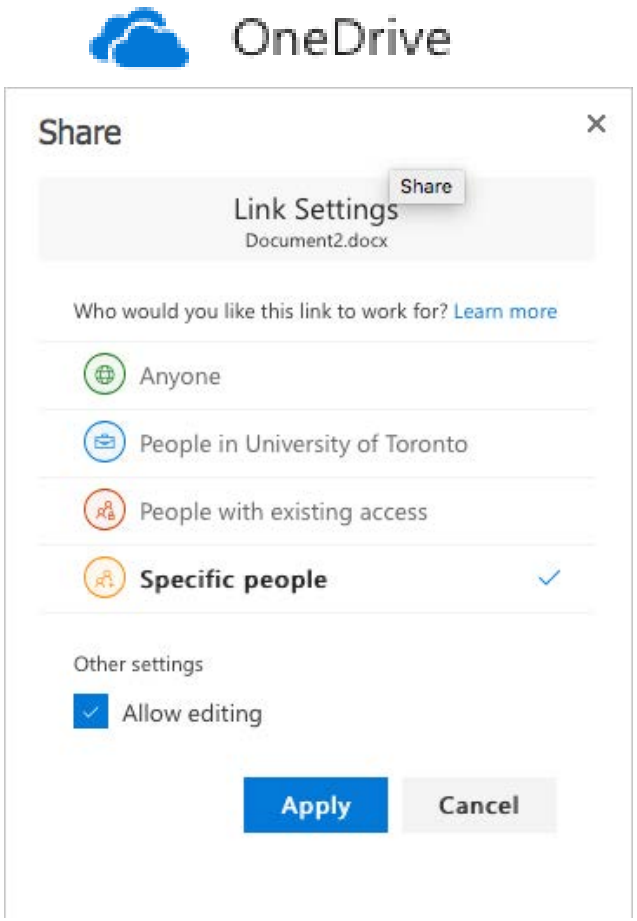
WHAT IF I GET HACKED?

- Before you get hacked:
- have backups if you need them or plan to rebuild the device.
- plan for who to call: helpdesk at school or someone at home
- If you get hacked:
- Don't be embarrassed - ask for help!
- Ransom request? Think about what has been lost and how it can be recovered - backups will help here.

WHAT IF I GET DOXXED/HARASSED?

- interact with Social Media provider using previous links
- seek assistance at the University

COLLABORATING ON RESEARCH



- Where is your data?
- O365 email: one copy of attachment for internal and external sharing.
- O365 OneDrive: share data but maintain control and visibility.
- http://office365.utoronto.ca/office-365-tip-14-sharing-files-with-onedrive/
- avoid using thumb drives, or any portable media unless encrypted.
- send to the wrong person? fix it using OneDrive.

RESEARCH AND TRAVEL

- Access your files via Office 365's web interface
- Use the U of T VPN
- Bring "empty" travel devices
- Bring a "burner phone"

TEACHING

Avoid Using Facebook to Facilitate Your Course

- No control how Facebook will use your students' data
- IP inadvertently shared
- No control over cheating and/or defamation on Facebook
- Our policies do not apply to Facebook

Please Use Quercus or Blackboard.

STAYING SAFE AT HOME

- Use separate devices for work and play.
- Use separate browsers for work and play.
- Use separate accounts on the same device.
- Multiple passwords and password manager.
- Non-privileged accounts are best in Microsoft Windows.
- Backups are important - Acronis is a good product.

STAYING SAFE AT U OF T

- UTORid password should be reserved for single purpose.
- Enroll in self-service password reset service!

- www.utorid.utoronto.ca/cgi-bin/utorid/acctrecovery.pl

- Talk to your helpdesk staff - they have advice on services and best practices.

RESOURCES

- Information Security Awareness & Education Site: http://securitymatters.utoronto.ca
- Google Alerts: Subscribe yourself and get alerts when something new is posted about you! https://www.google.ca/alerts
- Have I Been Pwned? Verify if any information about you has been leaked via security breaches: https://haveibeenpwned.com/
- Facebook/CA check https://www.facebook.com/help/1873665312923476?helpref=search&sr=1&query=cambridge

THANK YOU

for your time!

SECURITYMATTERS.UTORONTO.CA