



Managing Risk and Staying Safe Online

Presented by Mike Wiseman and Chloe Payne,
Information Technology Services

INTRODUCTION

Carrie Schmidt, Senior Manager, Education and Awareness, Information Technology Services

Isaac Straley, Chief Information Security Officer, Information Technology Services

Mike Wiseman, Associate Director, Information Security and Enterprise Architecture, Information Technology Services

Chloe Payne, Program Coordinator, Education and Awareness, Information Technology Services

WHAT DOES **RISK** MEAN TO YOU?

Ask yourself and your colleagues questions:

“This data is valuable. I don’t want it in the wrong hands. What is the right way to store it? What is the right way to share it?”

“I want to communicate with my students online. Is it OK to use Twitter? Slack?”

“I’m travelling to the United States next week and China next month. Can I bring my laptop and my phone?”

“This email is from a friend so I should be able to open the attachment. But why did he send me an attachment?”



IN THE LAST YEAR ALONE:

- A **malicious email** was distributed to University of Toronto (U of T) employees that demanded a large sum of Bitcoin be delivered to the sender's account within 24 hours, or explicit footage of the victim would be sent to the victim's social media and contacts list.
- **Unauthorized journal access** was the target identified by the United States Department of Justice for nation-state phishing attacks at U of T.
- A number of U of T staff received a **phishing email** instructing readers to purchase \$500 worth of gift cards. The email appeared to be from a senior U of T official, and fostered a sense of urgency and secrecy that pressured recipients to respond to the request quickly.



Another
way to think
about risk is
**level of
comfort.**
Are you...



An open book



Super secure



Somewhere in between



ADJUST 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 setting 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 Wi-Fi 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.

KEEP YOUR ONLINE PERSONAS **SEPARATE**

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

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.



STAYING SAFE ON SOCIAL MEDIA

- Enable multifactor authentication on **Google**, **Facebook** and **Twitter**.
- Service to monitor social media attacks – **ZeroFox**.
- Review privacy and security guidelines for the social media provider:
 - <https://www.facebook.com/about/basics>
 - <https://help.twitter.com/en/safety-and-security/account-security-tips>
 - <https://help.instagram.com/369001149843369>



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, LinkedIn etc.
- If you don't intend to use these accounts, just set them to private and add them to your list of accounts to maintain.
- 'Verify' your accounts, if possible, to confirm your identity with each social media platform.



GOOGLE YOUR NAME

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.



WHAT IF I GET DOXXED OR HARASSED?

- Interact with social media provider using the links on the previous slide.
- Seek assistance at the University.
 - If you receive a threat to life or property, call 911.
 - Access mental health, personal safety and/or sexual harassment support at:
<http://safety.utoronto.ca/>

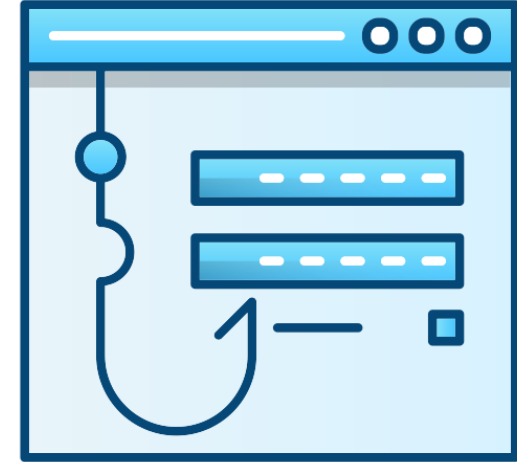




TECHNIQUES FOR MANAGING RISK ONLINE

PHISHING

- Malicious attempts to steal your personal information.
- Install malware (malicious software, e.g., ransomware).
- Prompts for passwords.
- Messages often appear to be from your contacts.
- Not only email: can also come through text or phone calls.
- Spear phishing – targeted at you.

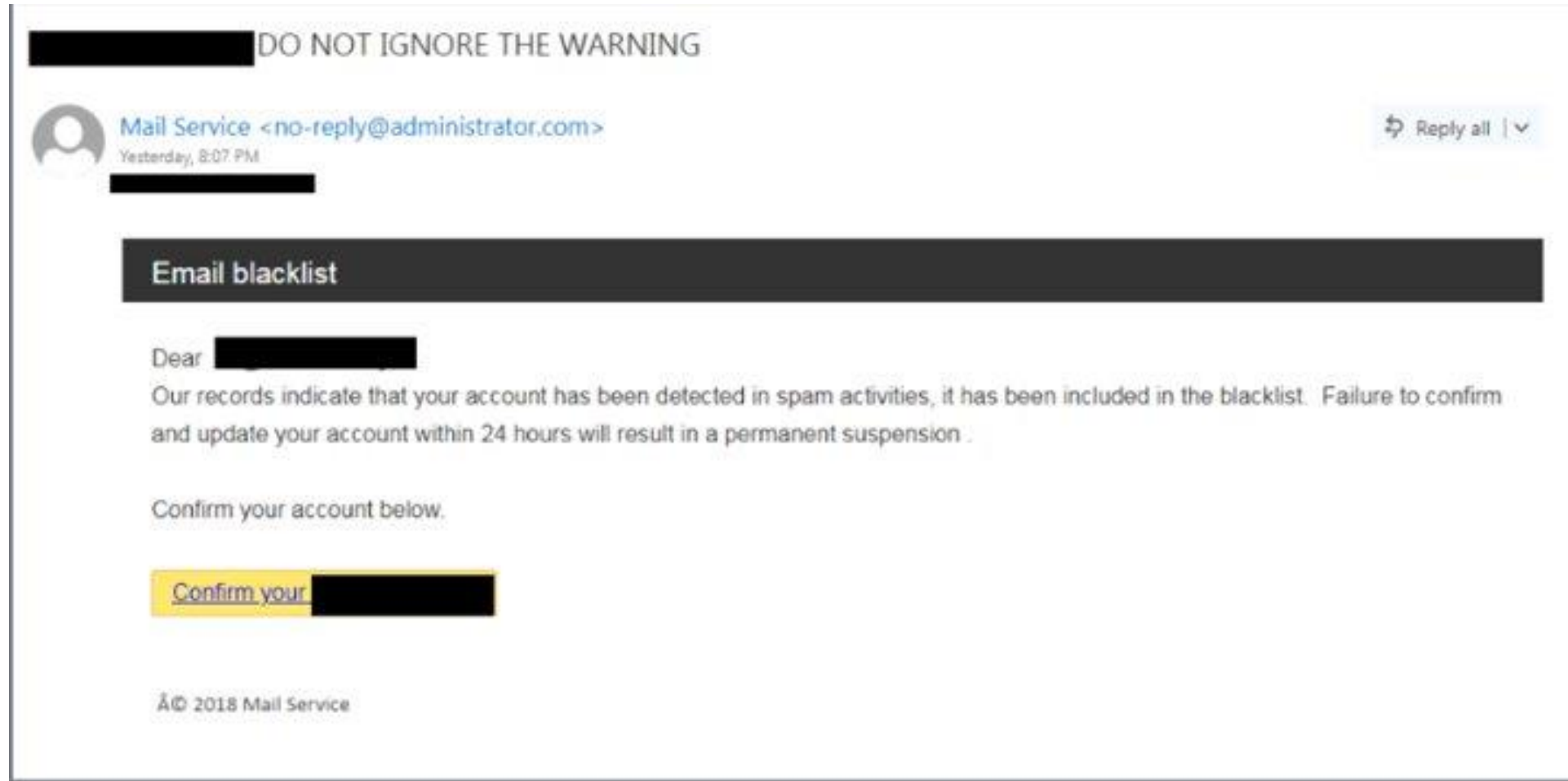


Signs that you're being phished could include: messages that seem odd or have a sense of urgency, bad grammar/spelling, phony links and a reply field that doesn't match the sender.

If an email seems suspicious, always trust your instincts. Verify communications and ask your IT office or email help.desk@utoronto.ca for assistance if you're unsure.

Report suspected phishes to report.phishing@utoronto.ca.

PHISHING AT U OF T



Report suspected phishes to report.phishing@utoronto.ca.

EDUCATION AND AWARENESS

- The 2018 Verizon Data Breach Investigations Report (DBIR) found that **93 percent** of data breaches in 2017 involved **phishing** and pretexting.
- The best way to combat these 'social attacks' is through **educating** organizational members and making them **aware** of the signs.
- U of T is taking on this security risk through running strategically planned **anti-phishing campaigns**. These campaigns simulate real phishing emails and educate individuals who become susceptible.
- Information Technology Services is currently running campaigns for 12 different faculties. We distribute three scenarios for each faculty over the course of nine months.

PASSWORDS AND PASSWORD MANAGERS

- **Keep passwords strong:** Use long, complex passwords or passphrases or shorter, highly complex passwords.
- **Use more than one:** Use a different password for each account.
- **Never share your password:** Do not share your password, even if someone claiming to be the bank, the university or another institution asks.
- **Password Managers** are an easy way to practice good password hygiene:
 - Store tens, hundreds of account passwords.
 - Convenience of a list of bookmarks.
 - Auto fill-in username and password.
 - Examples: **Password Safe**, **KeePass**.
 - Instructions for KeePass: <https://isea.utoronto.ca/infotip-using-a-password-manager/>



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.
- <https://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.
- Instructions to encrypt thumb drives:
<https://isea.utoronto.ca/infotip-index/>



TEACHING

Avoid using Facebook to facilitate your course.

- No control over 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.
- Only use [Quercus](#) for course facilitation.



Do not use personal social media or email accounts to facilitate your course.

- Only use your .utoronto.ca email address.
- Keeping personal and professional information separate makes all of your data more secure.



ASSISTANTS AND STUDENTS

- Do not share your computer login info or UTORid login info with assistants and/or students. Your UTORid is a gateway to accessing your private personal and professional data.
- Only share confidential information (such as student grades or accommodations) over **O365** and **Quercus**.

GOOD PRACTICES

- Keep a clean desk.
 - Put away confidential files in a locked cabinet.
 - Your desk should be clear of any documents, USBs or external drives. They should all be locked away in a secure space.
- Keep a separate user profile for assistants and students on your computer.
- Enable lock screen passwords.
- Ensure your office hardware and software are up to date.
 - Updates will fix known security gaps.
 - If you have a managed desktop, U of T will upgrade your hardware and software for you.
- Sign up for self-serve password reset:
<https://www.utorid.utoronto.ca/cgi-bin/utorid/acctrecovery.pl>



TRAVEL: GOOD PRACTICES

BEFORE YOU TRAVEL

- Update all device software.
- Back up your information if you bring your personal device.
- Bring empty travel devices and a "burner" phone - an inexpensive device that can be discarded or used solely for travel.
- If you bring a portable hard drive or USB stick with you ensure they are encrypted.
- Turn off "remember me" and wipe stored passwords from travel devices.
- Make sure you have the authorization to take data off-site. Follow these security requirements: <https://securitymatters.utoronto.ca/resources/workingoffsite/>

TRAVEL: GOOD PRACTICES

AS YOU TRAVEL

- Make sure all devices are password protected and never left unattended (especially at security checkpoints).
- Turn off auto-connect for Bluetooth and Wi-Fi.
- Access your files via Office 365's web interface.
- Use the U of T VPN.
- Do not use public Wi-Fi connections to conduct work-related business.
- Beware of publicly accessible computers.
- Make sure you know how to remotely wipe your personal device in case you lose it, and the provider's phone number to suspend or block service.
- Do not plug in unknown or untrusted devices.
- Use multi-factor authentication where possible.
- When you return, use a trusted device to change all passwords used while travelling.

WHAT IF I GET HACKED?

Before you get hacked:

- Have backups if you need them or plans to rebuild the devices.
- Plan for who to call: Help Desk at school or someone at home.
- If you run a lab, create a plan for the lab staff.

If you get hacked:

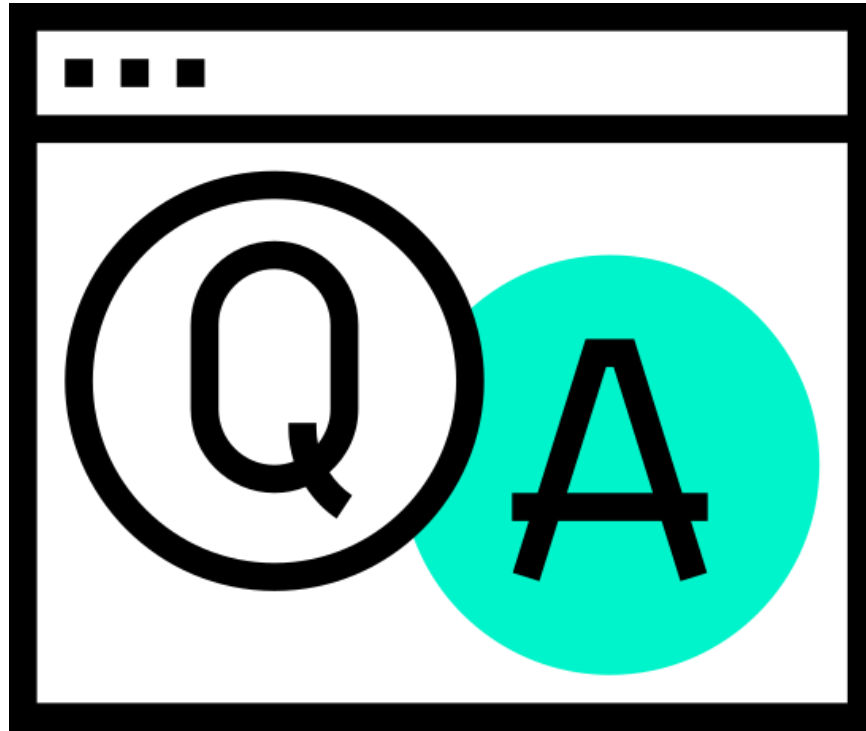
- Don't be embarrassed – ask for help!
- Ransom request? Think about what has been lost and how it can be recovered – backups will help here. It's never recommended to pay.



RESOURCES

- Security Matters resources for faculty: <https://securitymatters.utoronto.ca/resources/faculty-tas/>
- Security Planner by the Citizen Lab: <https://securityplanner.org/#/>
- Report an incident: <https://securitymatters.utoronto.ca/report/>
- Spotting phishing emails: <https://securitymatters.utoronto.ca/wp-content/uploads/Tip-Sheets-draft06-gray.pdf>
- Safety & Support: <https://safety.utoronto.ca/>

QUESTIONS & DISCUSSION



THANK YOU FOR YOUR TIME!

securitymatters.utoronto.ca