BACK TO CYBER BASICS

April 2024 – Cybersecurity Awareness

Presenters: Mark Sly (Director, IT Security and Architecture)
Luigi Riscaldino (Cybersecurity and Privacy Awareness Specialist)

UNIVERSITY OF CALGARY

The University of Calgary, located in the heart of Southern Alberta, both acknowledges and pays tribute to the traditional territories of the peoples of Treaty 7, which include the Blackfoot Confederacy (comprised of the Siksika, the Piikani, and the Kainai First Nations), the Tsuut'ina First Nation, and the Stoney Nakoda (including Chiniki, Bearspaw, and Goodstoney First Nations). The City of Calgary is also home to the Métis Nation of Alberta (Districts 5 and 6).

Welcome to our Webinar

BACK TO CYBER BASICS

Understanding cybersecurity helps protect both you and UCalgary, keeping both personal and sensitive information safe.

In this webinar we will guide you through key practices that will help you protect yourself from the most common cyber threats.

WHAT WE'LL COVER TODAY:

Top 10 Cybersecurity Tips Review

Artificial Intelligence and Social Engineering

Reporting Cybersecurity Incidents

TOP 10 TIPS REVIEW

1. TAKE CYBER AWARENESS TRAINING

Education and awareness are key to staying cybersafe

Required online training is coming this fall, including:

- ✓ Cybersecurity Awareness
- ✓ Privacy Awareness
- ✓ Research Security Awareness

All students have access to a Privacy and Cybersecurity Awareness course on D2L

2. BACKUP YOUR DATA REGULARLY AND ENCRYPT THE BACKUPS

Ensure you have at least two copies of your data (better yet three!) in separate locations in case of a disaster or ransomware incident.

Create a Data Management Plan for all your research data.

Always encrypt your backups.

TOP 10 TIPS REVIEW

3. PASSWORD BEST PRACTICES

Use (and don't reuse) strong passwords across devices, servers, software or applications.

Do not hardcode passwords while developing software, even if it's encrypted.

Configure your mobile devices with a secure PIN/password to gain access.
Do not email or share your passwords.

Use strong authentication, such as Multi-Factor Authentication, whenever possible.

Change factory or default passwords on all devices.

Where possible turn on the vendor device encryption for your computers, mobile devices and peripherals.

4. UPDATE YOUR DEVICES, APPLICATIONS AND OPERATING SYSTEMS

Stop threat actors from exploiting known vulnerabilities by always applying updates and patches from vendors for your devices, applications and operating systems (e.g., Microsoft, Apple, Linux).

Turn on automatic updates wherever possible.

Updates are not limited to operating systems, but also include updates for storage devices, external hard drives, TVs, etc.

TOP 10 TIPS REVIEW

5. BE AWARE OF WHO IS ACCESSING YOUR SYSTEMS

Regularly review what accounts are active on your operating systems, applications, and devices. If you don't recognize the account, or if they have not logged in for a long time, disable or remove them.

Use UCalgary approved remote access services (VPNs) to gain access to your servers or devices on or off campus.

6. THINK PRIVACY

Check out our webinar on Staying Safe on Social Media (https://it.ucalgary.ca/cyber-awareness-webinar)

Be informed about the UCalgary Information Security Data Classification Standard
If you are working with Level 3: Confidential or Level 4: Restricted data:

- ✓ Engage IT or Research Computing Services for support
- ✓ Contact FOIP/Privacy office for support
  - ✓ Check out **FOIP/Privacy's FAQ page** https://www.ucalgary.ca/legal-services/access-information-privacy/faqs

TOP 10 TIPS REVIEW

7. BE AWARE OF PHISHING EMAILS AND TEXT MESSAGES

Threat actors use email or texting to trick, convince, or command you to click a malicious link or download a malicious file.

Take our Cyber Security IT - Introduction to Phishing course on ELM and learn more about how to spot and report these malicious messages.

Use the “Report” function in Outlook to flag and report suspected phishing emails.

Email Encryption is available for emailing sensitive information to external addresses

If you are sending bulk emails to try to avoid including clickable links to external sources.

8. BE CYBERSAFE WHILE TRAVELLING

UCalgary has cybersecurity information and travel policies to help protect UCalgary researchers, faculty and staff while travelling for business. This information highlights potential risks and offers solutions for protecting your devices while abroad. This includes offering a loaner device program and cyber tips for staying safe while travelling.

✓ Find the International Travel Policy at: https://www.ucalgary.ca/legal-services/university-policies-procedures/international-travel-policy

✓ Find UCalgary Travel Requirements at: https://www.ucalgary.ca/risk/risk-management-insurance/travel

✓ Researchers should also reach out to the Research Security Division at researchsecurity@ucalgary.ca when travelling, and find more information at: https://research.ucalgary.ca/conduct-research/safeguarding-your-research

TOP 10 TIPS REVIEW

9. FOLLOW OTHER SECURITY BEST PRACTICES

Know when your devices, applications and operating systems reach the end of their support life.

Only turn on the services that you need. Threat actors will use default services to access your system if you don’t configure them properly. If you don’t use them, turn them off.

Only install trusted applications from a trusted source.

Use antivirus and anti-malware software to protect your operating systems.

Ensure your firewall is turned on.

10. BE MORE SECURE - USE UCALGARY IT SERVICES

- ✓ Using UCalgary IT services is your best protection against cyber threat actors. UCalgary IT offers a variety of services to support research and academic requirements.
- ✓ Learn more about Research Computing Services at the address below or email them at support@hpc.ucalgary.ca.
  - ✓ https://it.ucalgary.ca/research-computing-services
- ✓ Always report cyber incidents to UCalgary IT: If you have any cybersecurity concerns, contact IT through UService or with a ServiceNow ticket.
  - ✓ https://www.ucalgary.ca/uservice

UNIVERSITY OF CALGARY

SECURITY AT HOME

CIRA Canadian Shield

Free (tax-payer funded) DNS Firewall Service which provides enhanced online privacy and security to individuals and families across Canada.

A DNS Firewall is a network security solution that prevents network users and systems from connecting to known malicious Internet locations.

Three Levels of protection are available:

- ✓ PRIVATE: prevents the commercialization of the user’s DNS for better online privacy
- ✓ PROTECTED: includes all features of Private plus added malware, botnet and phishing protection
- ✓ FAMILY: includes all features of Protected plus added adult content blocking

CIRA Canadian Shield is also available as a mobile app to protect Canadians’ smartphones and tablets. It is a free download!

https://www.cira.ca/cybersecurity-services/canadian-shield

Use Antivirus and firewall Protection: You have it at work, you need it at home, too.

Be Cautious Online: Understand your privacy settings. You do have a choice. Enjoy your apps but understand what is happening, it’s your choice!

Use secure connections: When accessing sensitive information online, ensure the website is secure (look for "https" in the URL)

Educate yourself: Stay informed about the latest cybersecurity threats and best practices to protect yourself and your family online.

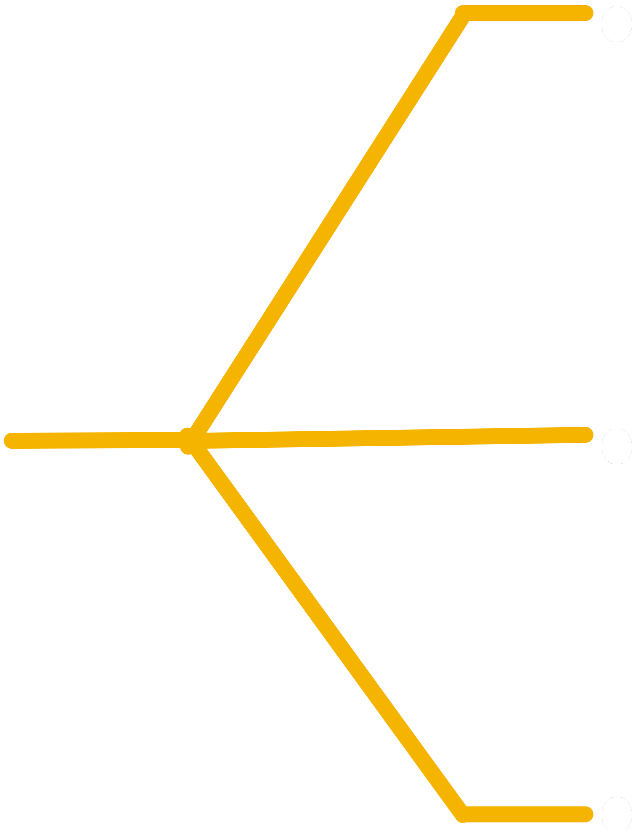
Get Cyber Safe: Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

https://www.getcybersafe.gc.ca/en

AI: IMPACTS ON CYBERSECURITY AND YOU

The threat landscape in Higher Education continues to evolve as new technologies emerge. Threat actors are developing more sophisticated tactics around phishing, malware, ransomware, data breaches, and other malicious activities targeting academic institutions.

Artificial Intelligence tools, such as ChatGPT, have improved threat actors attack techniques and present new privacy concerns.



Policy work around AI is ongoing at most government levels but there is still uncertainty which can increase the risk of misuse.

If you share information with an AI system, there is an increased risk that your sensitive information is being collected, exposed or misused.

Insufficient training data, incorrect assumptions made by the model, or biases in the data used may result in misleading or inaccurate results.

UNIVERSITY OF CALGARY

SOCIAL ENGINEERING AND AI

WHAT ARE AI DEEPFAKES?

AI-generated voices and videos that can easily mimic people you know, like family, friends, senior leaders at work, celebrities and politicians.

These may be used to trick you into giving up your credentials, sending money or authorizing financial transfers.

A REAL CONCERN:

- ✓ It is very easy to clone someone's voice from a three-second clip, which in many cases can easily be found online on social media.
- ✓ Incidents of deepfake phishing and fraud when up 3,000% in 2023 https://www.forbes.com/sites/forbestechcouncil/2024/01/23/deepfake-phishing-the-dangerous-new-face-of-cybercrime/?sh=322ab0604aed

REPORTING CYBERSECURITY INCIDENTS

PHISHING EMAILS

- ✓ Report the suspected email using the "Report" or "Report Message" button and then selecting "Phishing" in Microsoft Outlook
- ✓ For more information see the "How to report phishing emails" article on ServiceNow at ucalgary.ca/it

FOR ALL OTHER CYBERSECURITY INCIDENTS, CONTACT ONE OF THE FOLLOWING:

- ✓ Submit a ticket directly to the cybersecurity operation team through the ServiceNow portal at ucalgary.ca/it
  (search for "How to identify and report a Cybersecurity / Information Security Incident" or "KB0033937")
- ✓ Contact UService at 403.210.9300 and provide all the details.
- ✓ Contact your local IT Zone support manager

***At any point UService or the zone team can escalate your issue to the Cybersecurity Operations Team. It will be assessed and if necessary, the team will execute the Cybersecurity Incident Response Process.

USEFUL LINKS

- ✓ **UCalgary IT Security:** it.ucalgary.ca/it-security
- ✓ Top 10 Cybersecurity Tips: it.ucalgary.ca/it-security/top-10-cybersecurity-tips
- ✓ Staying Cybersafe: it.ucalgary.ca/it-security/staying-cybersafe
- ✓ Cybersecurity Tips for Travel: www.ucalgary.ca/risk/cybersecurity-travel
- ✓ International Travel Loaner Device Program: www.ucalgary.ca/risk/risk-management-insurance/travel/international-travel-loaner-device-program
- ✓ **UCalgary Research Computing Services:** it.ucalgary.ca/research-computing-services
- ✓ **UCalgary guidance on adding weblinks in emails:** ucalgary.service-now.com/kb_view.do?sysparm_article=KB0033851

- ✓ **How to back up to OneDrive:** ucalgary.service-now.com/kb_view.do?sysparm_article=KB0032351
- ✓ **UCalgary How to connect to VPN**: ucalgary.service-now.com/it?id=search&t=kb&q=vpn
- ✓ **Get CyberSafe Canada:** www.getcybersafe.gc.ca
- ✓ **RCMP Internet Safety Site:** www.rcmp-grc.gc.ca/is-si/index-eng.htm
- ✓ **National Cybersecurity Site:** www.canada.ca/en/services/defence/cybersecurity.html
- ✓ **Check if your email has been compromised:** https://haveibeenpwned.com/
- ✓ **Canada Antifraud Centre:** www.antifraudcentre-centreantifraude.ca/

UNIVERSITY OF CALGARY