We would like to acknowledge the traditional territories of the people of the Treaty 7 region in Southern Alberta, which includes the Blackfoot Confederacy (comprising the Siksika, Piikani, and Kainai First Nations), as well as the Tsuut'ina First Nation, and the Stoney Nakoda (including the Chiniki, Bearspaw, and Wesley First Nations). The City of Calgary is also home to Métis Nation of Alberta, Region 3.

Stay cybersecure.

At home.

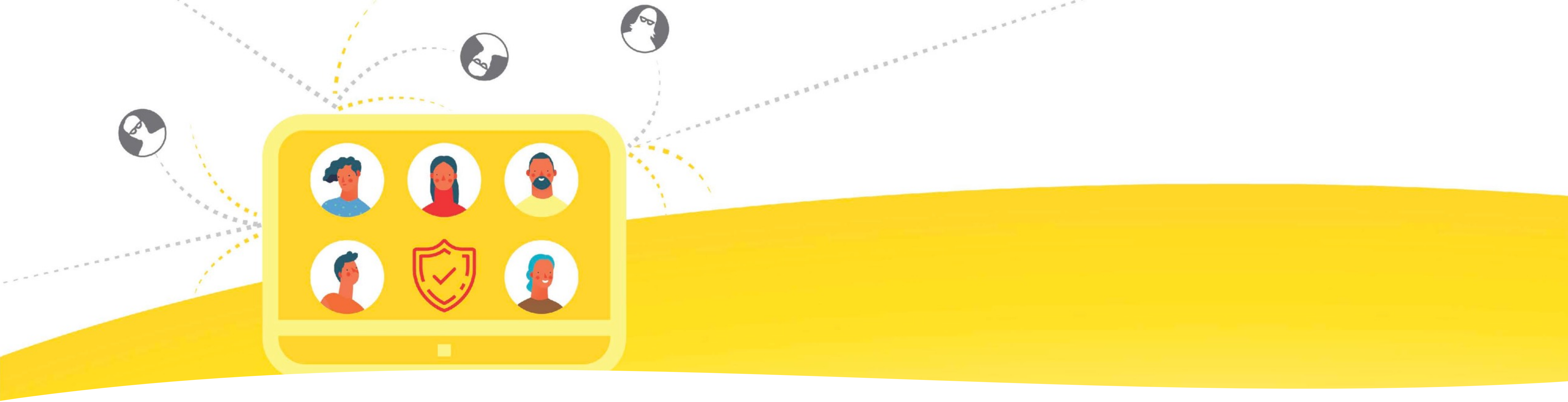
At UCalgary.

Follow us on Twitter @UCalgary_IT

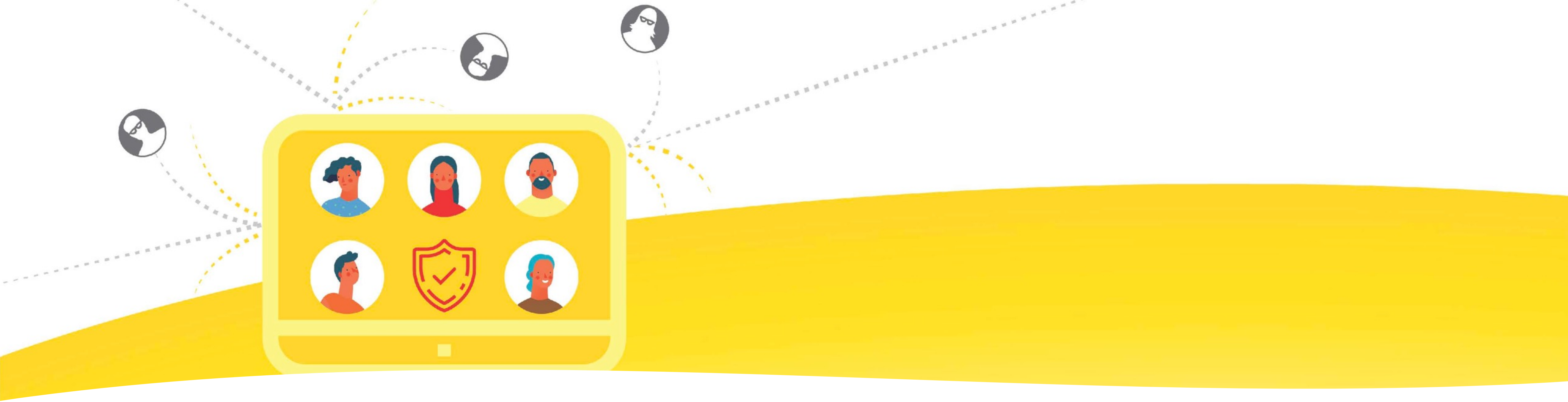
Visit us at - it.ucalgary.ca/it-security

What is Privacy?

- An individual's ability to determine for themselves when, how, and for what purpose their personal information is being handled by others.



PRIVACY CHECK-UP



Risks of Social Media

- Hashtags and Geo-location
- Phishing attacks
- Data Mining
- Reputational Harm

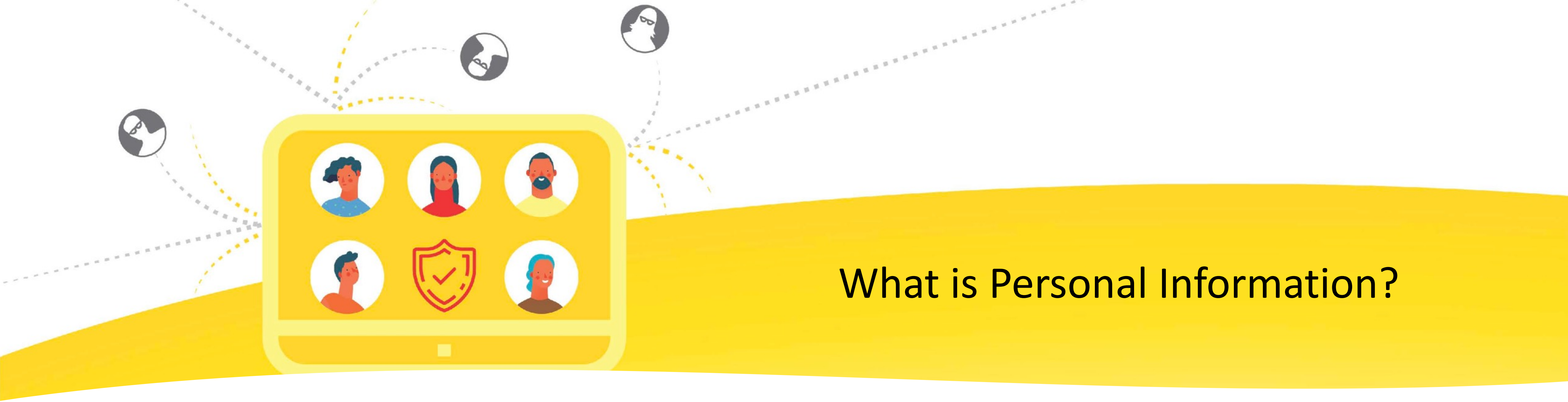
What can I do?

Secure your digital footprint

- Have you completed a privacy check?
- Look at the Privacy policy and Terms of Use
- What functions are enabled in the app?

FOIP 101

- **Freedom of Information & Protection of Privacy Act**
  - Provincial legislation that applies to all Post-Secondary Institutions since 1999
  - As employees, we must comply with FOIP’s requirements
  - Governs the processing of access to information requests
  - Governs the way we collect, use and disclose personal information



What is Personal Information?

- “Recorded information about an identifiable individual” including
  - Name; address; email; phone; race; religion; SIN; UCID; birthdate; fingerprints; health information; educational record; financial data; criminal history…
  - Someone else’s opinion of you
  - Although Personal information belongs to the individual the information is about, the record is in the custody of the university

What student information can be disclosed?

- dates of registration at the University of Calgary;
- faculty/department or program of registration at the University of Calgary;
- degree(s)/diploma(s) awarded from UCalgary;
- convocation dates;
- attendance at or participation in a public event or activity related to the institution (e.g. graduation, sporting or cultural event); or
- personal information already in the public domain.

What employee information can be disclosed?

- employment status
- business contact information
- job title, job profile, rank, job family
- salary range, discretionary benefits
- relevant educational qualifications
- attendance at or participation in a public event or activity related to the institution (e.g. sporting or cultural event)
- personal information already in the public domain, or
- publications listed in an academic staff member’s annual report.

Protecting our records

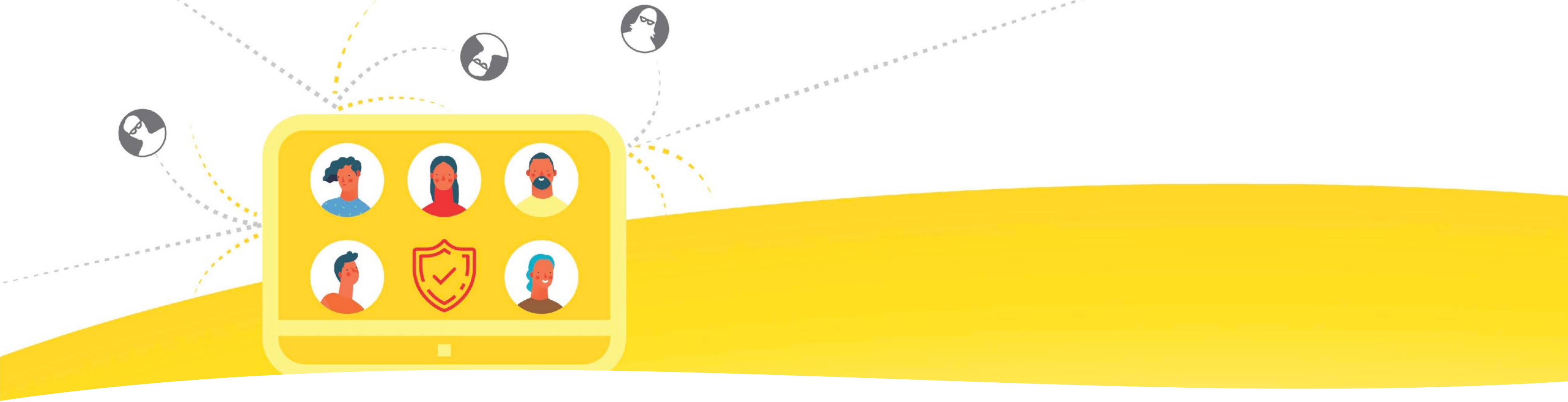
- Email should be reviewed regularly based on university retention rules

- Email is not appropriate for long term storage of information

Breaches

It happened – what now?

- Report the breach to the FOIP office/IT immediately.
- Maintain communication and follow directions for mitigation.
- Breaches of information collected under the authority of the Health Information Act (HIA) or Research Ethics Board (CHREB) should also be reported.



Top 10 Cybersecurity Tips

1. Take cyber awareness training

Education and awareness are key to staying Cybersafe
UCalgary offers the following cyber security courses:

- Privacy Training: **FOIP General Awareness**
- Cyber Awareness Training
  - **Cyber Security IT - Introduction to Phishing**
  - **Introduction to Research Security**
  - **Cyber Security for Researchers**
- Software development training: **OWASP top 10: LinkedIn Learning**
- Students:
  - Privacy and Cybersecurity Awareness course on D2L: How to register

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

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

Be nice to your digital identity
Contact IT — we’re here to support you.

3. Password Best Practices

- Use (and don’t reuse) strong passwords across devices, servers, software or applications
- Do not hardcode your passwords into software code, even if it's encrypted
- 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
- Use a password manager
- Configure your mobile devices with a secure PINs/password to gain access
- Canadian center for cyber security password guidance:
  - Use passphrases
  - A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces
  - Your passphrase should be at least 4 random words and 15 characters in length

4. Update/Patch your devices, applications and operating systems

Having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. To defend against known risks turn on automatic updates if that’s an available option.

- Set your mobile phones to update automatically
- Set your MAC, Chrome book or Windows PC’s to update automatically
- Updates from vendors are not limited to operating systems, but also include updates for storage devices, external hard drives, TVs, etc.

5. Be aware of who is accessing your systems

- Regularly review what accounts are active on your operating systems and devices. If you don't recognize the account, or if they have not logged in for a long period of time, disable or remove them.
- Use UCalgary approved remote access services (VPNs) to gain access to your services or devices on campus.

6. Think Privacy

- 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 Privacy/FOIP office for support
  - Check out FOIP's Privacy FAQ page
- BREACH: It happened – what now?
  - Report the breach to the FOIP office/IT immediately.
  - Maintain communication and follow directions for mitigation.
  - Breaches of information collected under the authority of the Health Information Act (HIA) or Research Ethics Board (CHREB) should also be reported.

7. Be aware of Phishing emails and text messages

Attacks via texts, social media, or emails try to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.

Watch out for:

- Unsolicited emails (do you recognize the sender?)
- Attachments
- Hidden links & Spoofed websites – check the URL
- Spoofed Senders (familiar_name@gmail.com)
- Login pages
- Urgent requests
- Sending sensitive information over email or texts

Report the phish to UService and reportphishing@ucalgary.ca

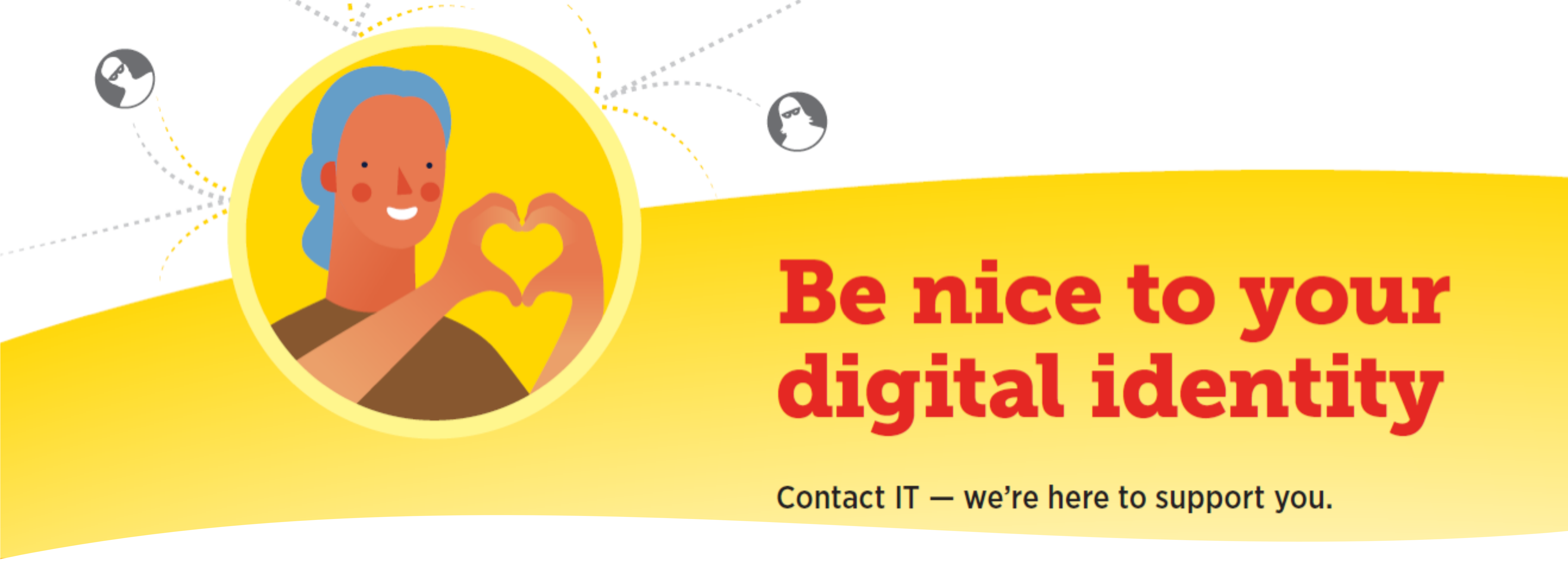
Note: If you are sending bulk emails, try to avoid including clickable links and do not direct to webpages that ask the user for their use name and password.

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

Risk Management and Insurance: https://www.ucalgary.ca/risk/risk-management-insurance/travel


Be nice to your digital identity
Contact IT — we're here to support you.

9. Other good cyber hygiene 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
- https://haveibeenpwned.com/ (check if your account has been compromised on other sites)

10. Use IT Services

- **Using IT services is your best protection against cyber threat actors.**
- UCalgary IT offers a variety of services to support research and academic requirements.
- UCalgary IT and the FOIP office offer technology threat risk assessments and privacy impact assessments
- Always report cyber incidents to IT: If you have any cybersecurity concerns, contact IT through UService or with a ServiceNow ticket.
- **Research Computing services**: https://it.ucalgary.ca/research-computing-services or email them at support@hpc.ucalgary.ca
- **UCalgary IT:** https://ucalgary.ca/it

Multifactor Authentication (MFA) Attacks

Like all social-engineering attacks, MFA prompt bombing exploits human behaviour to circumvent technical controls preying on human mental fatigue.

- Sending a bunch of MFA requests and hoping the target finally accepts one to make the noise stop.
- Sending one or two prompts per day. This method often attracts less attention, but “there is still a good chance the target will accept the MFA request.”
- Calling the target, pretending to be part of the company, and telling the target they need to send an MFA request as part of a company process.
- If you get an unexpected MFA prompt on your mobile app there is a good chance a threat actor has your password already

Students are a Target

Attacks we have seen on students:

- Credential stuffing: is when hackers use previously stolen login credentials from one website and then "stuff" these credentials into other websites until they find matches
- Phishing or Smishing:
  - Emails from already compromised student accounts
  - Offers of employment
  - Offers for remote international employment
  - Information about VISA's or immigration
  - Gift cards
- Ransomware: is a form of malware that infects your computer or device. When ransomware takes control of your computer or device, it locks you out of that computer or device entirely or certain files.
- Strangers in person requesting to use your login or computer to submit an assignment
- Spyware: is a form of malware that hides on your device, monitors your activity, and steals sensitive information like bank details, camera access and/or passwords

Useful Links

Cybersecurity Training:

There is a new Privacy and Cybersecurity Awareness Course on D2L that anyone can enroll in. Login and Registration required. Learn more here.

- **UCalgary IT Security:** https://it.ucalgary.ca/it-security
- **UCalgary Research Computing Services:** https://it.ucalgary.ca/research-computing-services
- **UCalgary IT:** https://ucalgary.ca/it
- **UCalgary Safe Travel:** https://www.ucalgary.ca/risk/risk-management-insurance/travel
- **UCalgary Adding web links in email guidance:** https://ucalgary.service-now.com/kb_view.do?sysparm_article=KB0033851
- **UCalgary How to connect to VPN**: https://ucalgary.service-now.com/it?id=search&t=kb&q=vpn

- **Get CyberSafe Canada:** https://www.getcybersafe.gc.ca/
- **RCMP Site:** https://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- **National Cybersecurity Site:** https://www.canada.ca/en/services/defence/cybersecurity.html
- **How to back up to OneDrive:** Back up your Documents, Pictures, and Desktop folders with OneDrive (microsoft.com)
- **Check if your account email has been compromised on other sites:** https://haveibeenpwned.com/
- **Canada Antifraud Centre:** https://www.antifraudcentre-centreantifraude.ca/