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.

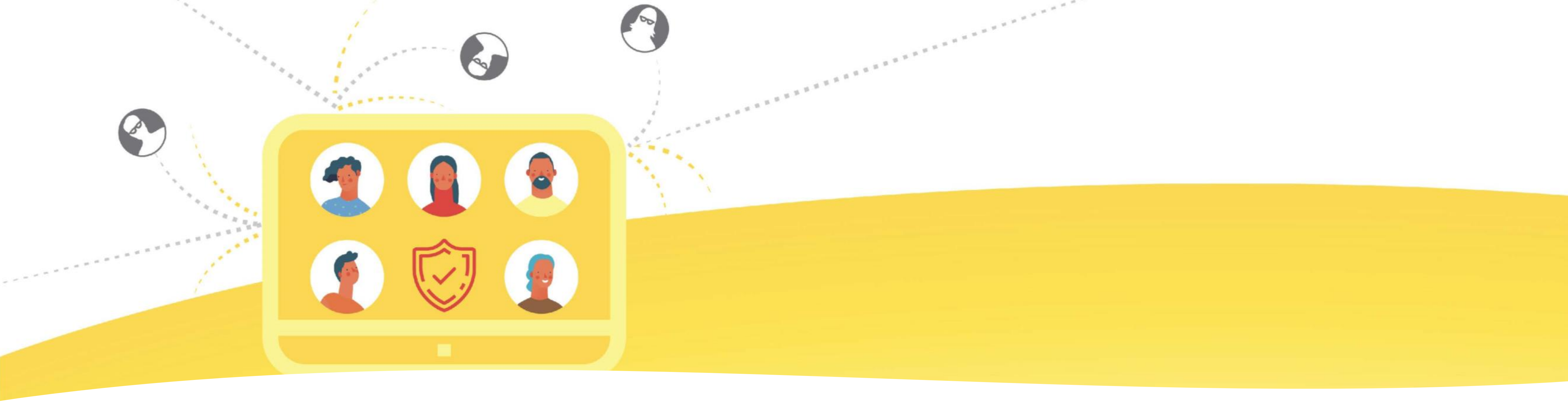
Stay cybersecure.

At home.

At UCalgary.

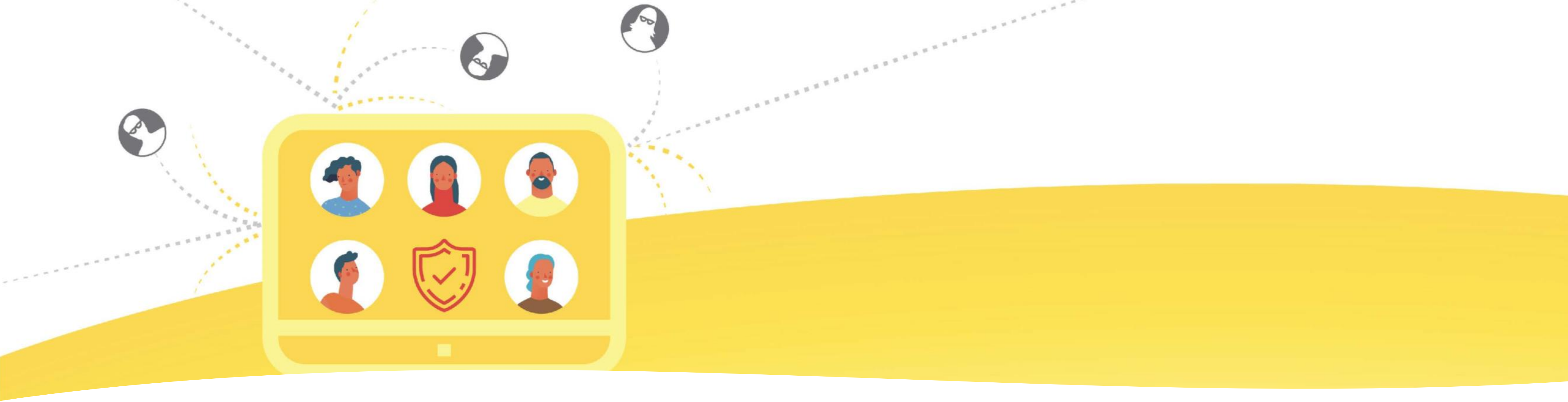
Follow us on Twitter @UCalgary_IT

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



Your UCalgary devices at home

- Connect to VPN at least every 30 days
- It should be your preferred device when working from home for UCalgary related business
- Turn on OneDrive backup under the backup tab in your OneDrive settings (Microsoft Windows only)
- Update/Patch your Mac
- Purchase a reputable firewall router and WiFi device
- Talk to your internet provider support for securing your router and WiFi
- Call UService if there are any concerns
- Visit our twitter @UCalgary_IT or IT webpage for updates and information



CIRA Canadian Shield – Your Internet Telephone Book

Protect your home network and devices

The Canadian Internet Registration Authority (**CIRA**) provides a free DNS Firewall Service called **CIRA Canadian Shield** which provides enhanced online privacy and security to individuals and families across Canada.

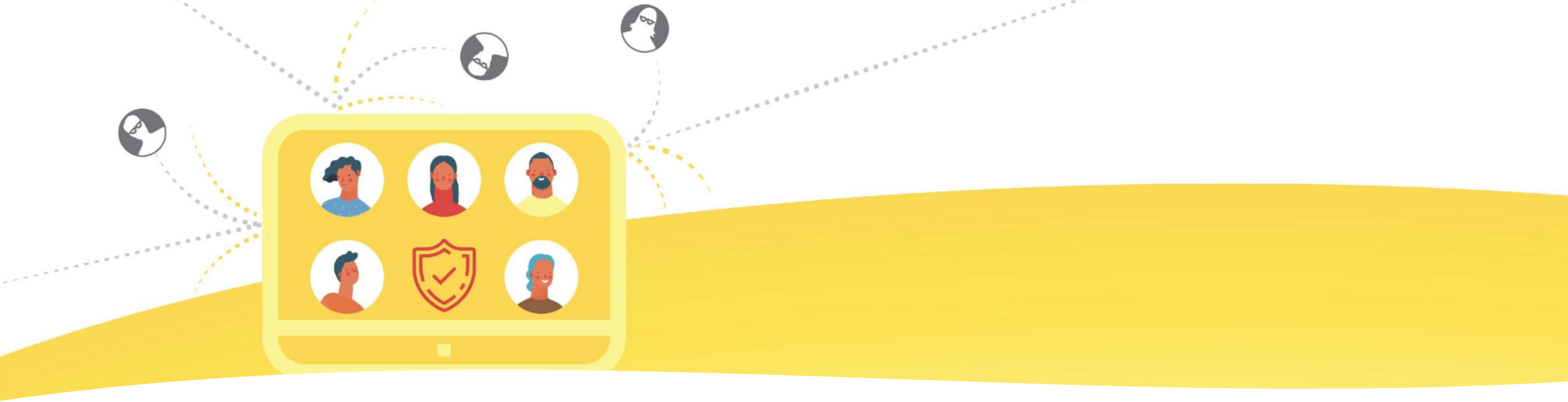
Three Levels of protection are available:

PRIVATE: prevents the commercialization of the user's DNS for better online privacy

PROTECTED: all features of Private plus added malware, botnet and phishing protection

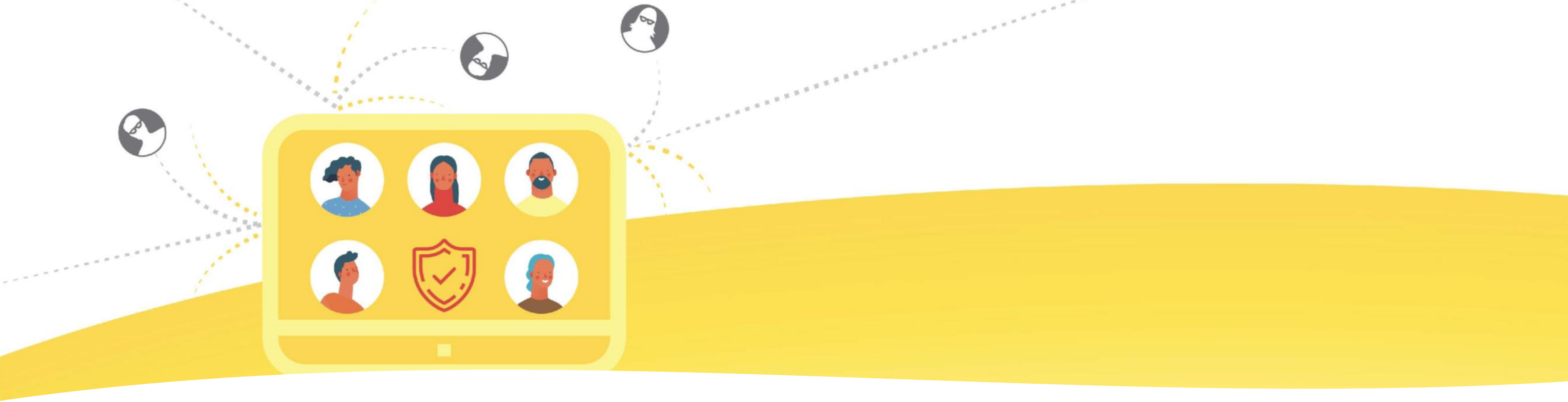
FAMILY: all features of Protected plus added adult content blocking

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



Coming back to work

- Connect to VPN before coming back
- If your computer has been on campus and powered off, come in and turn it on before you need to use it, this is so it gets caught up on updates, reboots, etc.
- Expectations are that people are to set up the equipment they took home by themselves, and they can put in a ticket if they have trouble.
- Call UService if there are any concerns
- Visit our twitter @UCalgary_IT or IT webpage for updates and information

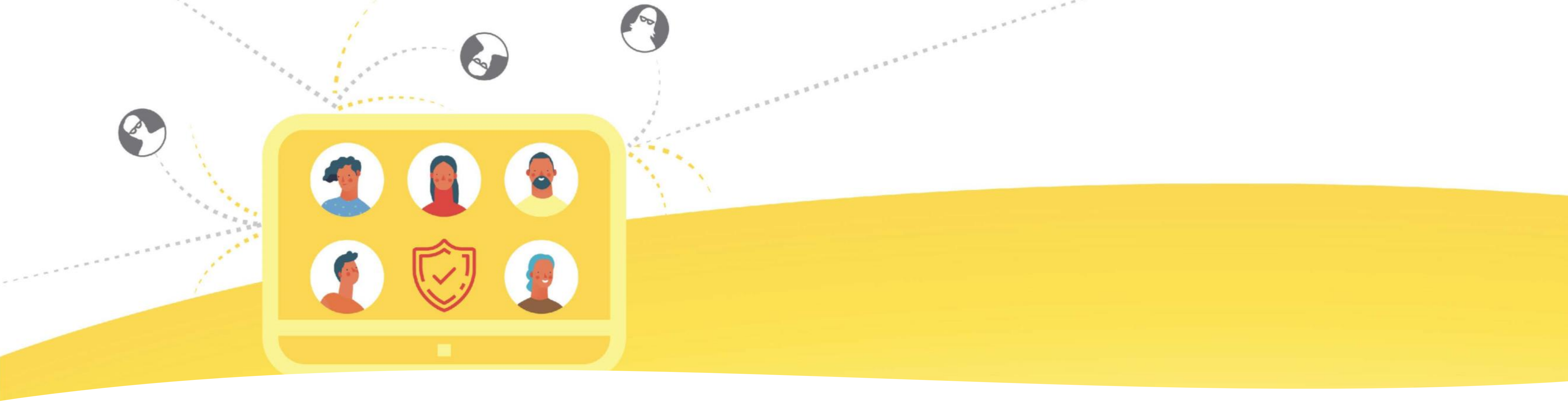


Top 10 Cybersecurity Tips

1. Take cyber awareness training

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

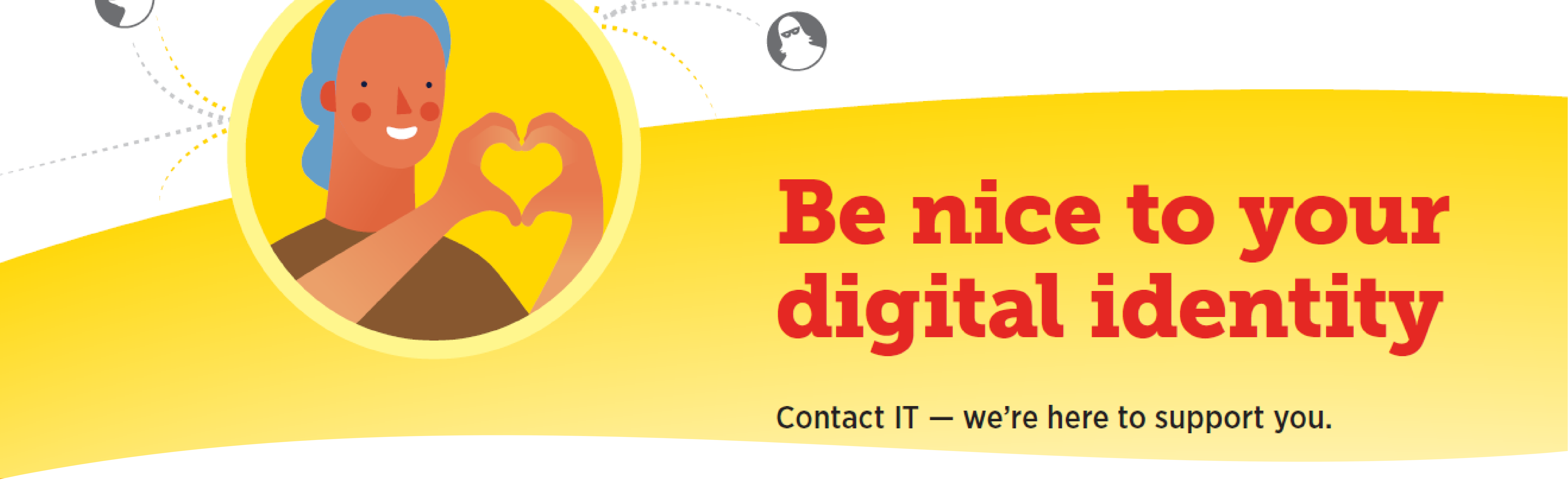
- Privacy Training: **FOIP General Awareness**
- Cyber Awareness Training
  - **Cyber Security IT - Introduction to Phishing**
  - **Introduction to Research Security**
  - **Cyber Security for Researchers**
- Software development training: **OWASP top 10: LinkedIn Learning**



2. Backup your data regularly and encrypt the backups

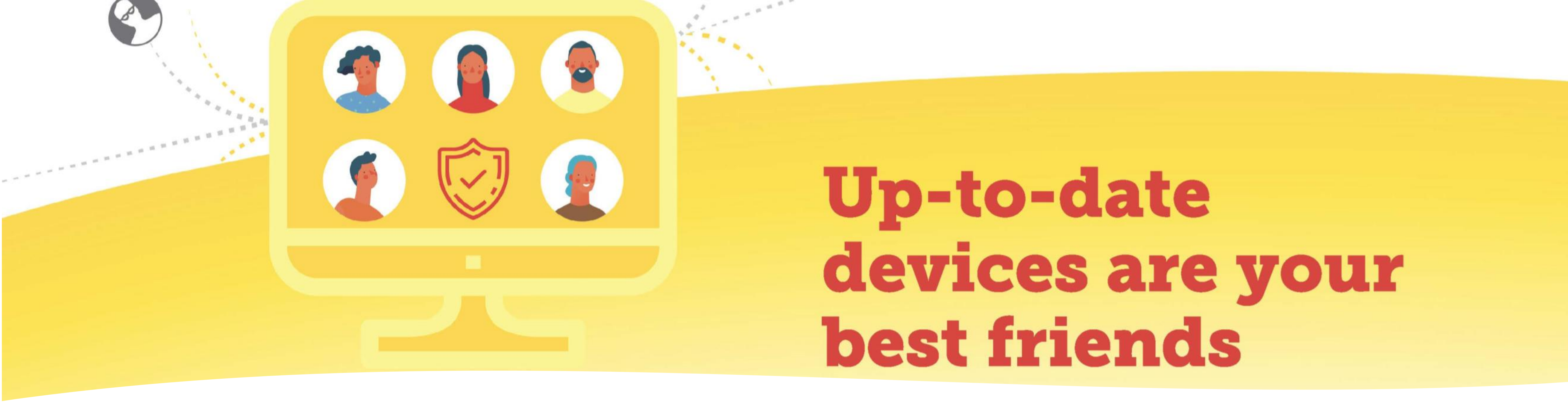
- Ensure you have at least two copies of your data (better yet three!) in separate locations in case of a disaster or ransomware incident
- Create a Data Management Plan for all your research data
- Always encrypt your backups

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

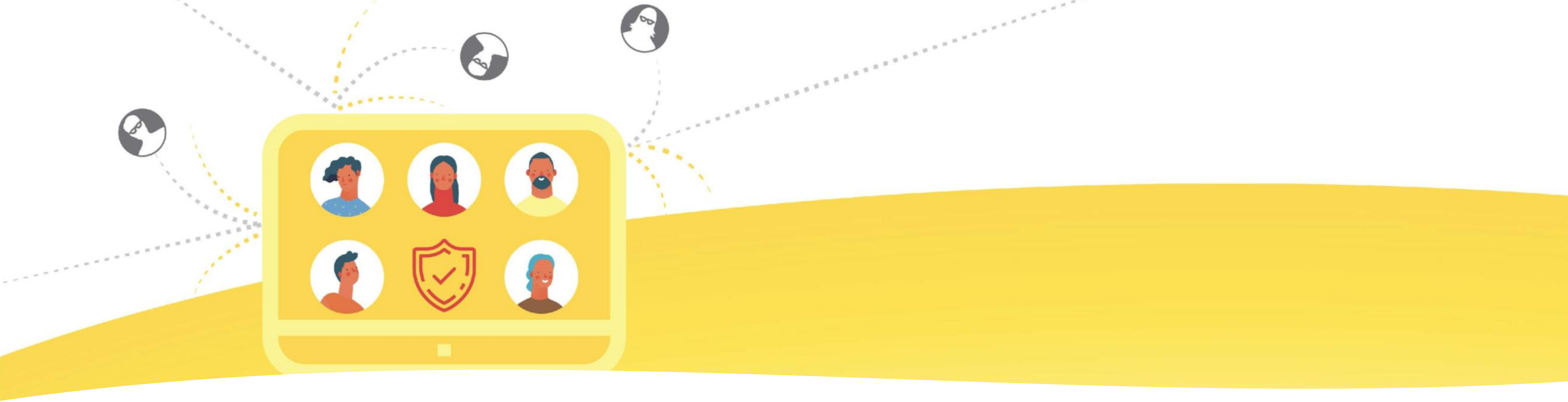
- Use (and don't reuse) strong passwords across devices, servers, software or applications
- Do not hardcode your passwords into software code, even if it's encrypted
- Do not email or share your passwords.
- Use Strong Authentication, such as Multi-Factor Authentication, whenever possible
- Change factory 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.

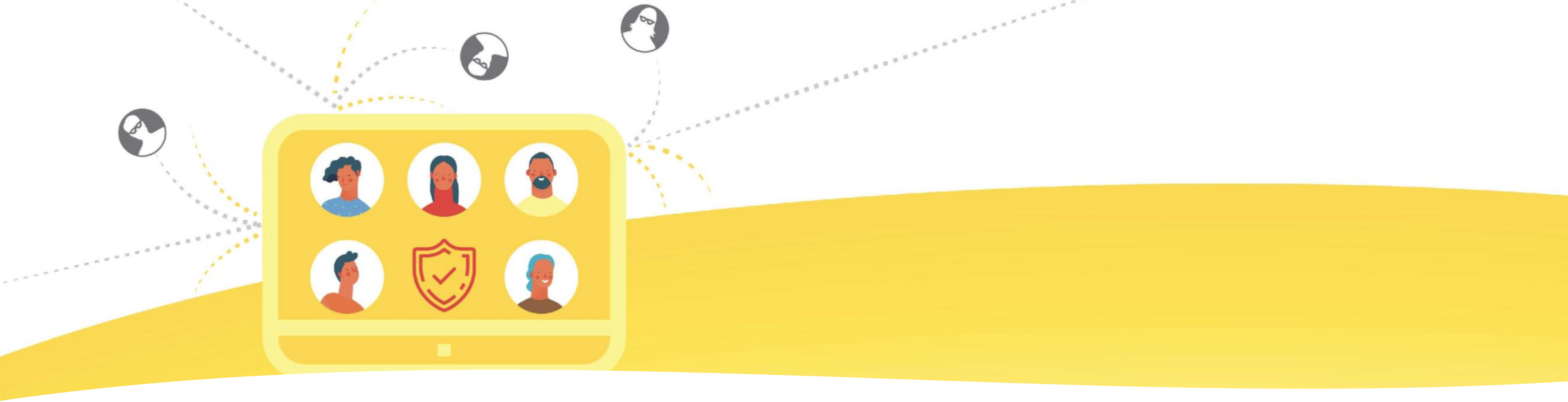
- Set your mobile phones to update automatically
- Set your MAC or Windows PC’s to update automatically
- Updates from vendors are not limited to operating systems, but also include updates for storage devices, external hard drives, TVs, etc.



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 servers 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
- 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

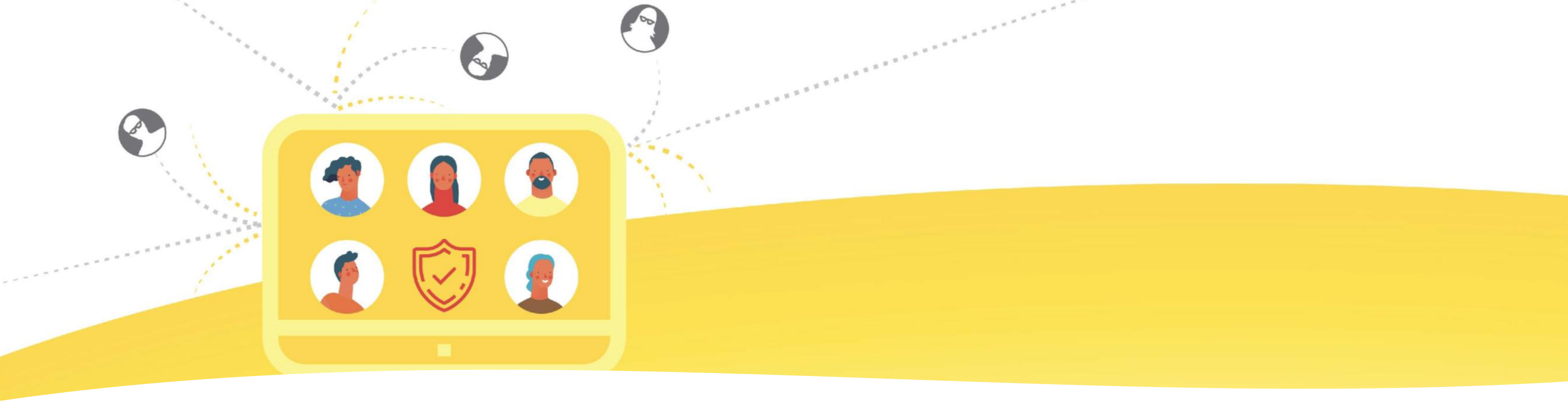
Attacks via texts or emails try to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.

Watch out for:

- Unsolicited emails (do you recognize the sender?)
- Attachments
- Hidden links & Spoofed websites – check the URL
- Spoofed Senders (familiar_name@gmail.com)
- Log-in 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.

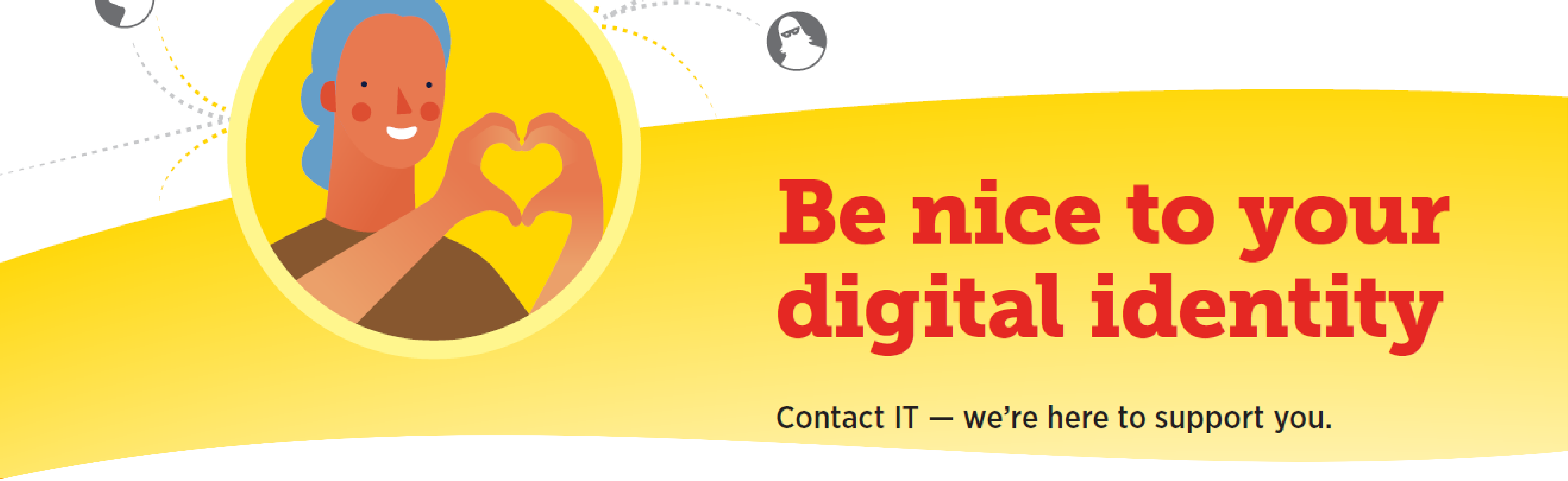


8. Be cybersafe while traveling

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.

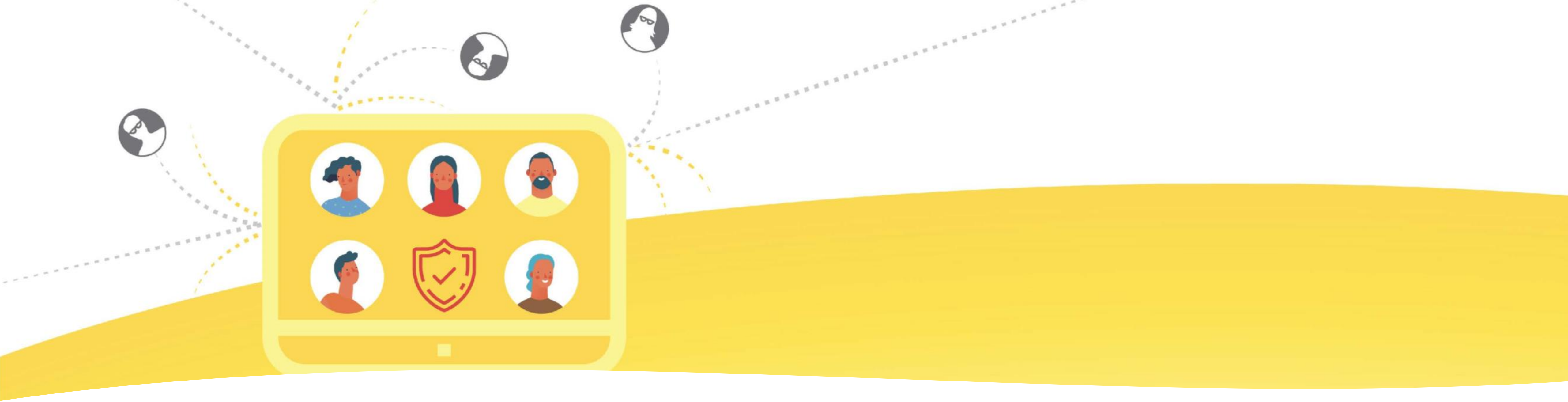
This includes offering a loaner device program

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.

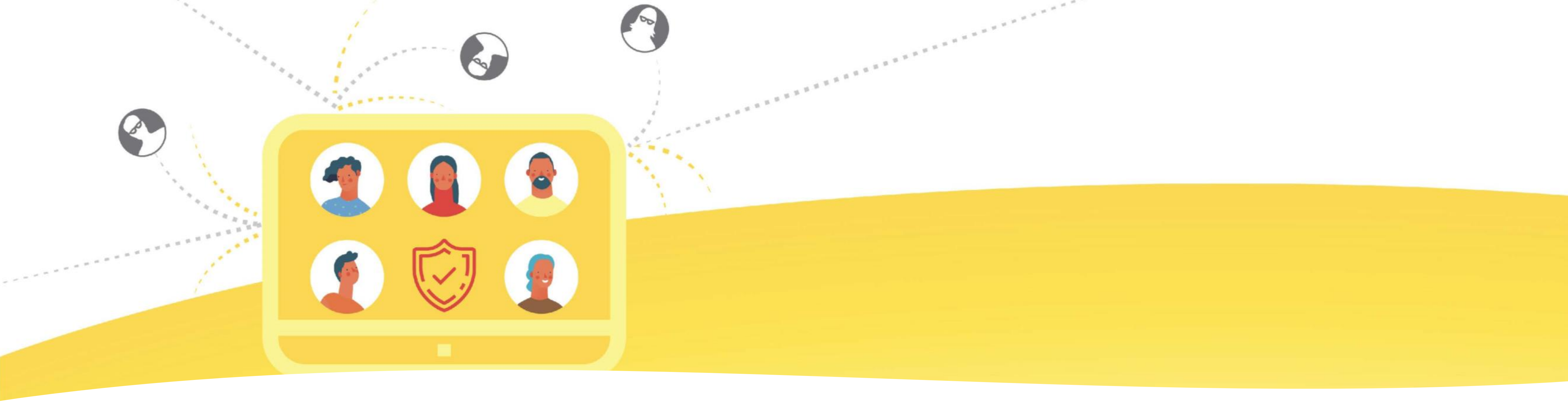
UCalgary IT offers a variety of services to support research and academic requirements.

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



Useful Links

Cybersecurity Training: There are a new learning resources available to all faculty and staff on our **Enterprise Learning platform,** which will educate learners about cyber awareness for phishing and research. You can enrol yourself and your staff by navigating to the My UCalgary portal in your preferred web browser and select the menu “My Work” at the top and click “PS Enterprise Learning” under the “Direct Access” menu

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/