Cybersecurity Awareness for Executives

CyberAlberta
Cybersecurity Services Division
Technology & Innovation, Government of Alberta

CYBER ALBERTA

The News Is…

Cybercrime is omnipresent!

The Hill: A hacking group accessed the database of National Public Data, a background check company (Aug 12, 2024)

Reuters: RCMP Says They Were Targeted by Cyberattack (Feb 23, 2024)

FT: North Korean Hackers Use AI For More Sophisticated Scams (Feb 21, 2024)

CBC: AutoCanada investigating cybersecurity breach , as it announces loss from previous incident (Aug 13, 2024)

WP: 'World's Most Harmful' Cybercriminal Group Disrupted in 11-Nation Operation (Feb 19, 2024)

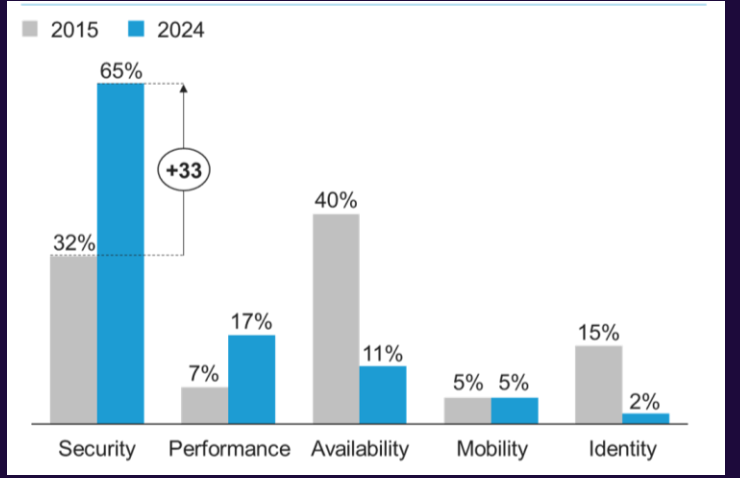
CBC: City of Hamilton says its phone and email systems have been hit by 'cybersecurity incident' (Feb 26, 2024)

Cybercrime is the world's 3rd largest economy!

		GDP $T
1.	United States	$21T
2.	China	$15T
3.	**Cybercriminals**	**$6T**
4.	Japan	$5T
5.	Germany	$3T
6.	United Kingdom	$3T

Source: Worldbank, Reposify

Percentage of respondents who would not deploy an app without…



CYBER ALBERTA

The Cyber Threat

In today's highly digital world

Reasons why attacks are increasing in number and in sophistication:

- Organizations are rapidly expanding attack surfaces with their commitment to digital services and mobile users.
- Weak authentication systems continue to be the main vector into our digital environments.
- Vulnerabilities in unsupported legacy products (Cobol, mainframe, etc.) and Supply Chain (Log4J, SolarWind, MOVEit).

The Insiders (unwitty or malicious)

Goal: Accidental or Profit.

Method: We gave them access to the assets they need!!!

Nation States / Terrorists / Hacktivists

Goal: Disrupt services or shame organization.

Method: Highly organized and sophisticated group hacks.

Cyber Criminals and Spies

Goal: Steal secrets and make a quick profit.

Method: Social engineering and systems vulnerabilities.

Natural Disasters

Goal: None (random).

Method: Disastrous events disrupting digital services.

How they get in

- **Social engineering** such as email phishing for credentials, website drive by to upload malware and keyloggers. Put you in a situation where you don't have time to think.
- **Legacy systems** vulnerabilities and third-party software vulnerabilities (e.g., Log4J, TEC Java 1.7 code, MOVEit). Taking advantage of poor computer hygiene.
- **Brute force attacks** of weak passwords or authentication (e.g., password crackers, digital trust established between environments). Creating false accounts and increasing privileges.
- **Application Program Interfaces (API)**. APIs facilitate communication between apps and apps components. Newer, but most effective! (e.g., hacking a car via OnStar).

CYBER ALBERTA

Executives are a Target

From an attacker's perspective an executive is a high-value target because they:

- Have access to confidential information and business practices.
- Have access privileges that may be higher than those of a non-executive employee.
- Often have access codes and passwords to the organization's financial information.
- Tend to be very busy and may click on links or provide information without noticing irregularities in targeted communications.

CYBER ALBERTA

Spear Phishing Executives

Generative AI complicates phishing detection. Spelling and grammar errors are no longer reliable indicators.

Key signs to watch for:

- Well-formatted messages that appear legitimate.
- AI-generated content may have contextual errors.
- Odd phrasing or repetitive sentences.
- Inconsistencies or irrelevant information.

Safety tips:

- Even if a message looks legitimate, never provide credentials or personal information.
- Verify the sender's email address carefully; cybercriminals often alter one letter or character.
- Check links for spelling errors and avoid clicking unusual ones.
- When in doubt, contact the sender using known, valid contact information.

CYBER ALBERTA

Doing Business Outside of the Office

Executives often travel for business, taking their devices and accessing sensitive information.

Protect company devices and information by following best practices for cyber-secure travel.

The following information will help you to limit risk while working away from the office.

Taking Your Devices With You

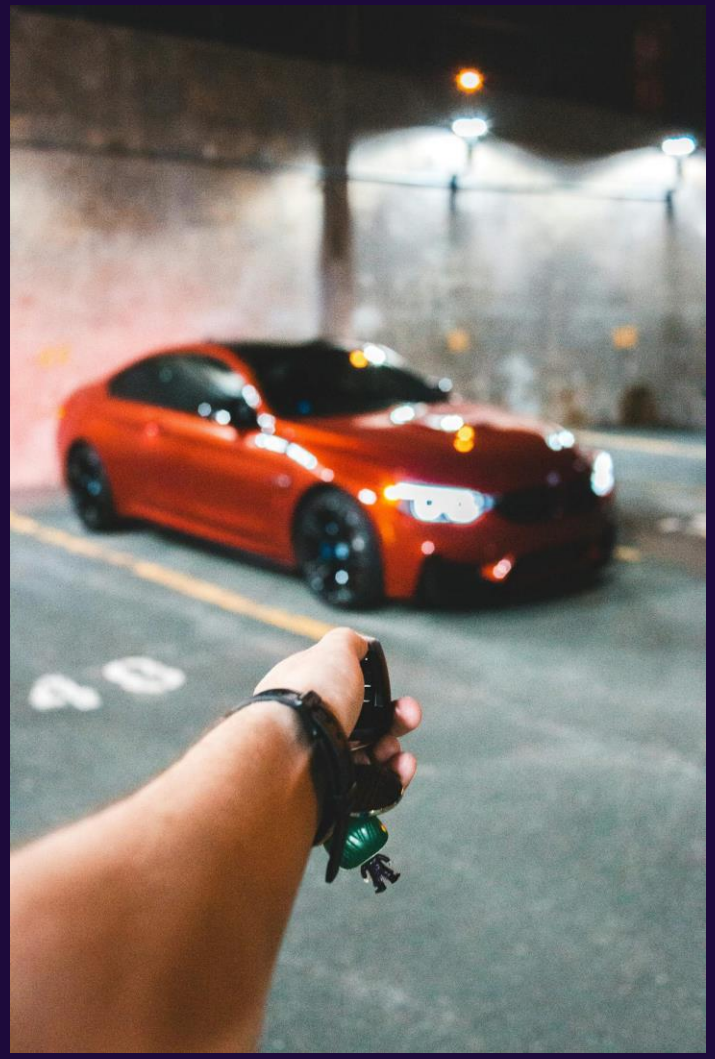
- Ensure all devices have strong, unique passwords and enable two-factor authentication (2FA) where possible.
- Regularly update operating systems, applications, and antivirus software to protect against vulnerabilities.
- Avoid using public Wi-Fi networks for sensitive activities. If necessary, use a VPN to encrypt your connection.
- Turn off automatic connections to Wi-Fi and Bluetooth to prevent unauthorized access.
- Always lock devices when not in use.

- Only take essential devices and data on the road. Use cloud services for access instead of storing sensitive files on your device.
- Ensure devices can be remotely wiped in case of loss or theft.
- Watch for "shoulder surfers" who may try to see sensitive information on your screen.
- Establish a protocol for reporting lost or stolen devices, including who to contact and what steps to take.

CYBER ALBERTA

Safe Practices for Using Rental Cars

- Never leave devices in plain sight. Store them in the trunk or a less visible area.
- Avoid using rental car Wi-Fi, as it may not be secure. Use your own mobile hotspot or a VPN if you must connect.
- When using a GPS or infotainment system, be cautious about connecting your device. Disable any features that may share personal data.
- Remove any personal data from the car's system before returning the vehicle.
- Keep your devices with you whenever possible to minimize risk.



Protecting Your Devices from Surveillance

Screen Protectors: Use privacy screen protectors for laptops and smartphones to prevent shoulder surfing and unauthorized viewing of your screen.

Faraday Pouches: Store smartphones in Faraday pouches to block signals and prevent tracking or remote access.

Additional Tips:

Cover Cameras: Use webcam covers or tape to block laptop and smartphone cameras when not in use.

Disable Microphones: Turn off or mute microphones on devices when not needed to prevent eavesdropping.

Strengthen your Organization's Security

To counter threats, organizations should adopt comprehensive security measures including:

- **Robust Authentication and Access Control**: Implement multi-factor authentication and strict access controls to prevent unauthorized access.
- **Advanced Threat Detection**: Use AI-driven threat detection systems to identify and respond to unusual activities and potential intrusions.
- **Regular Security Audits and Penetration Testing**: Continuously assess and test the security of systems to identify and mitigate vulnerabilities.
- **Employee Training and Awareness**: Train personnel to recognize phishing attempts and social engineering tactics to reduce the risk of human error.
- **Network Segmentation**: Isolate critical networks from regular IT networks to limit the spread of malware and other threats.
- **Incident Response Planning**: Develop and regularly update incident response plans to ensure quick and effective action in the event of a security breach.

CYBER ALBERTA

CyberAlberta hopes you found this information useful.

CYBER ALBERTA