Protecting information while using remote technologies: Tips for academic institutions

March 2024

ITSAP.00.140

The implementation of remote access technologies has become essential for academic institutions. Remote technologies allow faculty, staff, researchers, and students to work and learn from anywhere. Remote technologies include virtual private networks (VPN), learning management systems (LMS), and collaborative tools and platforms.

However, when studying or working remotely, you may lose some of the on-premises cyber security safeguards set up by your institution. These safeguards should be replicated in your remote location and on your remote devices to mitigate risks from common cyber threats.

Risks of using remote technologies

To protect your institution's sensitive information, you should understand the risks to remote technologies so you can enforce the appropriate mitigation measures. You should consider the following risks when implementing remote technologies into your organization.

- Misconfigured implementation can leave systems vulnerable for threat actors to damage and steal sensitive information, such as intellectual property and personal information.
- Data being accessed, processed, or stored outside of Canada could be further shared or even subject to surveillance.
- Unsecured endpoint devices and networks (such as public Wi-Fi) can provide an opportunity for threat actors to gain access to your organization's network.

Your organization must implement remote technologies appropriately and must be aware of the level of sensitivity of any information being shared. If these risks are not handled appropriately your organization could experience serious repercussions such as:

- Reputational damage
- financial loss
- potential lawsuits

Common threats

Common threats to academic institutions include the following examples.

Insider threats: Anyone who has access to institutional networks, systems, and information can cause harm. This can happen intentionally (for example, stealing data for personal gain) or unintentionally (for example, unknowingly handling information inappropriately).

Phishing: This is when a threat actor calls, texts, emails, or uses social media to trick users into clicking a malicious link, downloading malware, or sharing sensitive information.

Malware: Malicious software can infect networks, systems, and devices, allowing threat actors to gain access to sensitive information.

Ransomware: This is a type of malware that will make your data inaccessible (for example, by locking systems and encrypting files) until a ransom is paid.

If a threat actor is successful in using these attacks, they can take over accounts, make unauthorized transactions, and steal sensitive information.

Replace end-of-life devices

Devices that have reached end-of-life (EOL) pose a security risk to your organization. EOL means that the vendor stops marketing, selling, and providing support and updates to the device. When you use devices that are not updated to the latest firmware, you can open yourself up to cyber attacks. Firmware is the software that is installed and updated by the manufacturer and contains important security measures. You can check whether your router is EOL by looking at the vendor's end-of-life product list or accessing the router's records in its system logs.

AWARENESS SERIES

Cat. No. D97-1/00-140-2024E-PDF
ISBN 978-0-660-69932-5

Security measures

The following steps can help protect networks, systems and sensitive information from common cyber threats when using remote technologies.

For institutions

You institution should ensure that you implement safeguards that they can monitor and enforce while still offering collaboration.

- Use an LMS for faculty and students to distribute and submit materials
- Use a VPN, firewalls, and anti-virus software to defend your networks from common threats
- Apply the principle of least privilege to protect information from unauthorized access

For a higher level of sensitivity, your institution should consider the following measures:

- Use a virtual desktop infrastructure to access institutional networks from personal devices
- Use a managed service provider to support and handle your institution's specific security measures
- Use an approved cloud service provider (CSP) and cloud access security broker (CASB) to enforce security policies
- Select service providers that are based in Canada to ensure your sensitive information is protected under Canadian privacy laws
- Establish a strong identification and authentication process, including the use of multi-factor authentication (MFA)
- Ensure administrators and users with privileged rights use dedicated administrative workstations to perform their tasks

For faculty and students

- Use institutionally supported security tools, platforms, and applications when handling work remotely
- Secure your home Wi-Fi by enabling security features and changing the default password
- Use secure Wi-Fi networks when working in public locations and avoid using public Wi-Fi when accessing sensitive information
- Use unique passphrases and MFA for all accounts
- Avoid sharing sensitive information through video teleconferencing (VTC) applications
- Lock VTC meetings with a password that is shared only with authorized individuals
- Keep your operating systems and devices up to date

If faculty and students are handling highly sensitive data, consider the following measures:

- Use secure or encrypted messaging applications supported by your institution if data needs to be shared
- Use alternate forms of communication to verify the identity of the individual you are sharing data with
- Understand local risks and implement the appropriate measures to secure the data from local monitoring

CANARIE network

CANARIE provides support and development tools, including cloud resources for Canadian research hospitals, universities and colleges, science facilities. CANARIE also provides identity management services and international connectivity for Canada's National Research and Education Network. CANARIE and the Canadian Shared Security Operations Centre have partnered to offer enhanced cybersecurity capabilities. Canadian Shared Security Operations Centre Cybersecurity Program

Learn more

Read our supporting publications for more details on cyber security best practices:

- How to protect your organization from Insider threats (ITSAP.10.003)
- Protect your organization from malware (ITSAP.00.057)
- Ransomware: How to prevent and recover (ITSAP.00.099)
- Virtual private networks (ITSAP.80.101)
- Using virtual desktop at-home and in-office (ITSAP.70.111)
- Cloud network security zones (ITSP.80.023)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Video-teleconferencing (ITSAP.10.216)
- Protecting your organization while using Wi-Fi (ITSAP.80.009)
- Identity, credential and access management (ICAM) (ITSAP.30.018)