PROTECTING INFORMATION WHILE USING REMOTE TECHNOLOGIES: TIPS FOR ACADEMIC INSTITUTIONS

MARCH 2021 ITSAP.00.140

The implementation of remote access technologies has become essential for academic institutions in the wake of the pandemic. Remote technologies enable faculty, staff, researchers, and students to work and learn from anywhere. There are many cyber security risks to remote technologies that academic institutions should be aware of and work to mitigate.

RISKS

To protect your institution's sensitive information, the risks to remote technologies should be understood to enforce the appropriate mitigation measures. Some risks to consider when implementing remote technologies into your organization include:

- Misconfigured implementation can leave systems vulnerable for threat actors to damage and steal sensitive information (e.g. intellectual property, financial information, personal information).
- Data being accessed, processed, or stored outside of Canada can be at risk of data sharing and local surveillance (e.g. privacy laws).
- Unsecured endpoint devices (e.g. personal devices) and networks (e.g. public Wi-Fi) can open opportunity for threat actors to gain access to your organization's network.

It is important that your organization implements remote technologies appropriately and takes caution with the sensitivity level in any information being shared. Your organization could experience serious repercussions (e.g. damage to reputation, financial loss, potential lawsuits) if these risks are not handled appropriately.

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, intentionally (e.g. steal data for personal gain) or unintentionally (e.g. unknowingly handle information inappropriately).

Phishing: 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: Malware (malicious software) can infect networks, systems, and devices allowing threat actors to gain access to sensitive information.

Ransomware: Ransomware is a type of malware that will make your data inaccessible (e.g. locking systems and encrypting files) until a ransom is paid.

If a threat actor's attack is successful in using these common attacks, they can take over accounts, make unauthorized transactions and changes, and steal sensitive or personal information.

AWARENESS SERIES

SECURITY CONSIDERATIONS

Although there are risks associated with using remote technologies, there are some steps that your academic institution, faculty, and students should consider to protect networks, systems, and sensitive information from common cyber threats.

FOR INSTITUTIONS

- Use a learning management system (LMS) for faculty and students to distribute and submit materials.
- Use virtual private networks, 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, institutions should take the following measures into consideration:

- 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.
- Select service providers that are based in Canada to ensure your sensitive information is protected under Canadian privacy laws.

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 multi-factor authentication (MFA) for all accounts.
- Avoid sharing sensitive information through video-teleconferencing applications.
- Lock video-teleconferencing meetings with a password that is shared only with authorized individuals.

If faculty and students are handling highly sensitive data, the following measures should be considered:

- Use secure (i.e. 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 (e.g. identity management).
- Understand local risks and implement the appropriate measures to secure the data from local monitoring.

LEARN MORE

Refer to some of our other publications for more details on cyber security best practices:

- *ITSAP.10.003 How to Protect Your Organization from Insider Threats*
- *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*
- *ITSAP.00.057 Protect Your Organization from Malware*
- *ITSAP.00.099 Ransomware: How to Prevent and Recover*
- *ITSAP.80.101 Virtual Private Networks*
- *ITSAP.70.111 Using Virtual Desktop At-Home and In-Office*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.10.216 Video-Teleconferencing*
- *ITSAP.00.266 Instant Messaging*
- *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*
- *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**