Cyber Attack

Cyber incidents can disrupt university operations, compromise sensitive information, and impact the safety and security of the campus community. Cyber attacks may include phishing attempts, ransomware, malware infections, unauthorized access to accounts, data breaches, denial-of-service attacks, or other malicious activities targeting university systems and individuals.

The Master's University Information Technology Department, in coordination with Emergency Management, Campus Safety, and external partners, continuously works to prevent, detect, and respond to cyber threats. Every member of the university community plays an important role in protecting institutional systems and information.

Recognize Potential Cyber Threats

Common indicators of a cyber attack include:

- Suspicious emails, text messages, or phone calls requesting personal information
- Unexpected password reset notifications
- Pop-up messages demanding payment or ransom
- Unusual computer behavior or slow system performance
- Unauthorized account activity
- Missing, altered, or encrypted files
- Unexpected software installations
- Alerts from antivirus or security software

If You Suspect a Cyber Attack

STOP: If you believe your computer, account, or device has been compromised:

- Stop using the affected device immediately.
- Do not click additional links or open attachments.
- Do not attempt to investigate the attack yourself.

- Disconnect the device from the internet if instructed by Information Technology personnel.

REPORT: Immediately report suspected cyber incidents

- Contact the TMU Information Technology Department.
- Contact TMU Campus Safety at (661) 713-7561 if the incident involves threats, extortion, harassment, or criminal activity.
- Report:
    - The type of suspicious activity
    - When the activity occurred
    - Any messages, links, or attachments involved
    - Whether sensitive information may have been compromised

PRESERVE EVIDENCE

- Do not delete suspicious emails or files.
- Take screenshots if possible.
- Record any error messages or unusual activity.
- Leave the affected device powered on unless instructed otherwise.

Phishing and Social Engineering

Cyber criminals often attempt to deceive users into providing passwords, financial information, or access to university systems.

Protect Yourself:

- Verify unexpected requests for information.
- Never share passwords or multi-factor authentication codes.
- Be cautious of urgent or threatening messages.
- Check sender email addresses carefully.
- Hover over links before clicking.
- When in doubt, contact the sender through a known and trusted method.

Ransomware Attacks

Ransomware is malicious software that encrypts files and demands payment for their release.

If you encounter a ransomware message:

- Disconnect from the network if possible.
- Do not pay the ransom.
- Do not attempt to bypass security controls.
- Immediately contact Information Technology personnel.
- Preserve all messages and evidence.

Account Security

Help protect university systems by:

- Using strong, unique passwords.
- Enabling multi-factor authentication whenever available.
- Keeping devices and software updated.
- Locking computers when unattended.
- Avoiding the use of unauthorized software.
- Reporting suspicious activity immediately.

During a Major Cyber Incident

A significant cyber attack may impact university operations and communications.

If university systems become unavailable:

- Follow instructions from university leadership and Information Technology personnel.
- Utilize alternate communication methods if necessary.
- Continue to monitor official university communications.
- Be prepared for temporary disruptions to technology services.

After the Incident

- Change passwords if instructed.

- Monitor accounts for unauthorized activity.
- Complete any required security training or reporting.
- Cooperate with university officials during recovery efforts.
- Continue to exercise caution regarding follow-up scams or phishing attempts.

Remember: If something seems suspicious, trust your instincts and report it. Prompt reporting is one of the most effective ways to protect yourself and the university community from cyber threats.