Information Security Tips and Best Practices

Security Tips & Best Practices

Keeping your system and data secure by following good security practices can help others in the University community benefit from decreased risk. The following security best practices have been sorted based on your needs:

Secure Your Office

- When leaving, lock the door and keep unauthorized users away from systems.
- Keep all media containing confidential information in a secure place.
- Keep any paper records of passwords in a secure place.
- Avoid applications that use excessive bandwidth.
- Turn computers off when leaving for the day, or during extended periods of inactivity, unless a special need requires that they stay on.

Secure Your Computer

- Password-protect your screen saver in high traffic or insecure areas and on mobile devices. When changing your password, make sure you change it everywhere you may have your credentials stored.
- Close applications and log out when you're away from your computer for any length of time.
- Install and maintain anti-virus and anti-malware software and update the definitions regularly. Scan all removable media for viruses before using them. Free anti-virus software is available for Fredonia students, faculty and staff.
- Mac and Windows computers come with built-in firewalls
- Keep systems updated with all of the current security patches. Where possible, turn on automatic updates to apply operating system security updates. When using images to support multiple systems, be sure the image is updated regularly with all applicable patches and virus definitions. Check regularly for updates to third party applications such as Adobe, Flash, Java, etc., or consider using an automated patching solution. Automatic updates offered by Windows and Macs do not always patch these applications. Fredonia ITS centrally manages automatic updates for all university owned computers.

Secure Your Data

- Backup systems thoroughly and often, and store your backups in a separate secure location.
- Do not save sensitive information to portable drives. Be sure to encrypt sensitive data wherever it is stored.

Secure Your Email

- Verify the contents of any email attachment before opening and never open attachments from unknown persons.
- Do not respond to any email requesting confidential information (username, password, social security number, etc.). Legitimate businesses will never ask for this information via email.
- Delete messages that you no longer need - some common practices include emptying your trash and outgoing mail folders.
- Report spam, or suspect messages to isecurity@fredonia.edu.
- Change your password at least once a month using the Fredonia strong password guidelines.

Tips for Faculty & Staff

- Limit the use of administrator privileges. Restricting access rights in this way will help prevent the potential installation of malware and other unwanted software by unsuspecting users.
- Keep systems updated with all of the current security patches. Where possible, turn on automatic updates to apply operating system security updates. When using images to support multiple systems, be sure the image is updated regularly with all applicable patches and virus definitions.
- Delete all data from computers before they are sent to Property Control.
- Ensure your computer firewalls are always enabled on your personal devices. University owned computers have their firewalls disabled by default to allow for automatic updates and remote assistance.
- Ensure that all users complete Security Awareness Training when available.
- Enforce policies to prevent the installation of unlicensed/unapproved software.

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Fredonia Mail Data Loss Prevention Policy for Credit Card Numbers (CCN) and Social Security Numbers (SSN)
- Can I use the Duo Security internationally?
- Do I need a smartphone to use Duo?
- If I choose to use my personal smartphone using the Duo Mobile app, what kind of information does Duo have access to?
- Using Hardware Tokens with Duo