Beef Up Your Physical Security

CYBER SECURITY JUNE 2018

Employing good physical security practices does not have to include hiring a detachment of the queen's guard for your campus (though this might be a nice attraction for prospective students!). Instead, just getting the word out to your community about the importance of a few basic physical security tips can substantially improve your institution's security risk profile. Below are some tips to share with your community:

- Prevent tailgating
  In the physical security world, tailgating is when an unauthorized person follows someone into a restricted space. Be aware of anyone attempting to slip in behind you when entering an area with restricted access.

- Don't offer piggyback rides
  Like tailgating, piggybacking refers to an unauthorized person attempting to gain access to a restricted area by using social engineering techniques to convince the person with access to let them in. Confront unfamiliar faces! If you're uncomfortable confronting them, contact campus safety.

- Put that shredder to work
  Make sure to shred documents with any personal, medical, financial, or other sensitive data before throwing away. Organizing campus-wide or smaller-scale shred days can be a fun way to motivate your community to properly dispose of paper waste.

- Be smart about recycling or disposing of old computers and mobile devices
  Make sure to properly destroy your computer's hard drive. Use the factory reset option on your mobile devices and erase or remove SIM and SD cards.

- Lock your devices
  Protecting your mobile devices and computers with a strong password or PIN provides an additional layer of protection to your data in the event of theft. Set your devices to lock after a short period of inactivity; lock your computer whenever you walk away. If possible, take your mobile devices and/or laptop with you. Don't leave them unattended, even for a minute!

Beef Up Your Physical Security

CYBER SECURITY JUNE 2018

- Lock those doors and drawers
  Stepping out of the room? Make sure you lock any drawers containing sensitive information and/or devices and lock the door behind you.

- Encrypt sensitive information
  Add an additional layer of protection to your files by using the built-in encryption tools included on your computer's operating system (e.g., BitLocker or FileVault).

- Back up, back up, back up!
  Keeping only one copy of important files, especially on a location such as your computer's hard drive, is a disaster waiting to happen. Make sure your files will still be accessible in case they're stolen or lost by backing them up on a regular basis to multiple secure storage solutions.

- Don't leave sensitive data in plain sight
  Keeping sensitive documents or removable storage media on your desk, passwords taped to your monitor, or other sensitive information in visible locations puts the data at risk to be stolen by those who would do you or your institution harm. Keep it securely locked in your drawer when not in use.

- Put the laptop in your trunk
  Need to leave your laptop or other device in your car? Lock it in your trunk (before arriving at your destination). Don't invite criminals to break your car windows by leaving it on the seat.

- Install a remote location tracking app on your mobile device and laptop
  If your smartphone, tablet, or laptop is lost or stolen, applications such as Find My iPhone/iPad/Mac or Find My Device (Android) can help you to locate your devices or remotely lock and wipe them.