Prevent Laptop Theft: Best Practices

Small electronic devices remain the prime targets on our campus, with Apple products being the most desired items by thieves. It only takes seconds for an experienced thief to nonchalantly grab a device.

Risk/Inconvenience of Theft:

Please take a moment to consider the risk and loss associated with the theft of your electronic device by asking yourself the following questions:

1- What would happen if your portable device was lost or stolen?

2- What data do you have on your device, such as research papers or homework assignments that cannot be easily retrieved or replicated. Is there confidential patient, customer or employee data that could put you or others at risk?

3- Are important files backed-up, password encrypted and archived off-site?

4- Can you financially afford to replace the device if lost or stolen?

5- Is there insurance coverage to cover the loss? How long might it take to settle a claim? How much time would be required filing and obtaining a copy of a police report?

6- How long can you be without the device?

Prevention:

While we're fortunate that campus crime remains relatively low, there are things you can do to reduce opportunities for the potential theft of your electronic equipment; in most instances, your careful action can prevent thefts. Following are some helpful tips to keep in mind and best practices to adopt:

1- **Don't leave devices unattended**. This is a common problem in our study centers and food courts. Ask a trusted colleague to keep a watchful eye should you need to step away for a moment.

2- Keep offices locked and use secured cabinets and drawers whenever possible.

3- Consider using a security chain while in study centers (contact Security for further information if you would like to use this method but don't have a chain).

4- If in your apartment, ensure that doors are locked, especially upon leaving.

5- Be aware of the opportunity for theft while on public transportation, and take steps to be sure you do not make yourself a target if using devices while traveling.

6- Record the make, model and serial number of your devices. This information should be accessible and stored in a secure place, other than or in addition to your devices.

7- Consider investing in electronic tracking, locking and wiping software if these are not already part of your device's operating system.

Campus Security Emergencies Ext. 4111 Non-Emergencies X2019

EINSTEIN
Albert Einstein College of Medicine
OF YESHIVA UNIVERSITY