

# Cool Careers in Cyber Security

## Finding Devices

**Delivery:** Can be used as a table demo (hands-on) activity or during a presentation session.

**Session Overview:**  
Digital Forensics I

**Objectives:**

- Understand the importance of physical security.
- Understand how USB thumb drives can lead to security risks.
- Understand that technology threats come in different shapes and forms.

**Materials/Supplies:**

- Various USB drives
- Pocket books, briefcases, or other props filled with miscellaneous personal items and several USB drives

**Introduction:**

Not all data breaches are the result of a malicious attacker breaking into the network. Ex-employees can download sensitive documents to a personal USB drive and take it to their new employer or current employees can take information and try to sell to the highest bidder. Backup drives containing sensitive data can get lost or stolen. Employees trying to be productive by taking work home can misplace their flash drives. All these potential scenarios expose the organization to data loss and regulatory fines.

Companies in particular are at risk when sensitive data are stored on unsecured USB flash drives by employees who use the devices to transport data outside the office. The consequences of losing drives loaded with such information can be significant, and include the loss of customer data, financial information, business plans and other confidential information, with the associated risk of reputation damage.

**Scenario:**







What are potential ways for thieves to steal or copy important information? Today many companies do not allow electronic or storage devices to be taken into work. Several organizations/companies actually inspect coats, bags, and briefcases to make sure the policy is followed. Hidden USB drives can be planted in women's jewelry bag and/or brief cases. Can you find all the hidden storage devices?

A USB flash drive is a data storage device that includes flash memory with an integrated Universal Serial Bus (USB) interface

**NOTE: Make sure ALL flash drives are accounted for after each presentation. Between sessions or inspections you will need to restock the bags/briefcases.**

**Lesson:**

1. Several handbags and briefcases are filled with a variety of personal items along with several USB drives.
2. The following USB drives are examples. Ask that they show the flash drive if they reveal an item as containing a USB drive. In general, each bag should contain 3- 4 devices each.

Necklace flower pennant		Hollow nickel spy coin	
Executive pen-laser pointer, pen and USB drive		Panda	
Bracelet		Key	
Flash drive These may vary—but are to represent a flash drive most are used to seeing			

**Resources:**

- How to restrict USB drive access: <http://searchenterprisedesktop.techtarget.com/tip/Restrict-USB-drive-access-on-Windows-XP-redo>
- News Article, SC Magazine: <http://www.scmagazine.com/militarys-ban-of-usb-thumb-drives-highlights-security-risks/article/121326/>
- Best practice tips: <http://www.infosecisland.com/blogview/20554-Twelve-Security-Best-Practices-for-USB-Drives.html>
- Dangers of unsecured USB sticks: <http://www.cioinsight.com/security/the-dangers-of-unsecured-usb-drives>

**Final Thoughts:**

Points you might want to make:

- There is usually more than one way to “steal information, and in many cases it involves low tech or no technology. There is usually an inexpensive method (under \$10-\$20) to break even the most elaborate security systems. In this case, as simple as plugging a USB drive into the computer
- Make the bridge from hidden USB drives to the need for defense in depth – prohibit flash drives, look for flash drives, and have technology protection (turn off USB ports).
- Flash drives have the potential to capture a large amount of information quickly, or carry complicated threat software onto an otherwise secure network.

**Recommendations:**

How could you protect against this type of threat?

Answers will vary.

- Fortunately, there are some easy steps that can ensure the safety of all portable devices. A security policy being adopted by an organization means that all its staff members are obligated to follow the basic steps required to ensure safety of their laptops and USB Flash Drives. Some of the best practices for formulating a USB Flash Drive Security Policy include:
  - Ensure that your USB flash drive encrypts the data as soon as it is stored in the device with the full disk encryption feature. This will not only restrict the use of the drive to computers that have compatible encryption software but also help avoid unauthorized access to data.
  - The data stored on a USB flash drive should be put through regular audit trial.
  - Organizations should circulate notices to all the mobile device users to restrict the use of USB flash drives at particular places.
  - Every organization should have a security policy regarding personal storage devices, including USB flash drives, which should be a part of the disaster management policy.
  - There should be a centrally managed database for all portable storage devices issued by the company to keep a track of the use of these devices inside and outside network accessibility.
  - Make sure all USB flash drives are password protected in order to thwart unauthorized access of the confidential data.
  - Restrict USB drive (and USB port) access.
  - Some USB flash drives also come with biometric finger print identification software that helps recognize the legitimate user. The software scans finger prints, authenticates the user and only then allows him/her to access the data.
  - Another simple measure that users of portable storage devices can implement is to chain the device so that it does not get lost during outdoor use.
  - Some security professionals suggest a radical approach to locking down USB flash drives. Evidence Solutions, advises clients to use a clear silicone caulk and fill every USB port on every PC to prevent USB attachments. That way the only way employees can transmit sensitive business documents is by email, a method that can be easily monitored.
  - ActivIdentity, adds that many military organizations don't allow the drives at all, and they have resorted to gluing USB ports closed to prevent breaches.