Proper Disposal of Electronic Devices | CISA

Why is it important to dispose of electronic devices safely?

In addition to effectively securing sensitive information on electronic devices, it is important to follow best practices for electronic device disposal. Computers, smartphones, and cameras allow you to keep a great deal of information at your fingertips, but when you dispose of, donate, or recycle a device you may inadvertently disclose sensitive information, which could be exploited by cyber criminals.

Types of electronic devices include:

- **Computers, smartphones, and tablets** — electronic devices that can automatically store and process data; most contain a central processing unit and memory, and use an operating system that runs programs and applications;
- **Digital media** — these electronic devices create, store, and play digital content. Digital media devices include items like digital cameras and media players;
- **External hardware and peripheral devices** — hardware devices that provide input and output for computers, such as printers, monitors, and external hard drives; these devices contain permanently stored digital characters; and
- **Gaming consoles** — electronic, digital, or computer devices that output a video signal or visual image to display a video game.

What are some effective methods for removing data from your device?

There are a variety of methods for permanently erasing data from your devices (also called sanitizing). Because methods of sanitization vary according to device, it is important to use the method that applies to that particular device.

Before sanitizing a device, consider backing up your data. Saving your data to another device or a second location (e.g., an external hard drive or the cloud) can help you recover your data if you accidently erase information you had not intended to or if your device is stolen (this can also help you identify exactly what information a thief may have been able to access). Options for digital storage include cloud data services, CDs, DVDs, and removable flash drives or removable hard drives (see Using Caution with USB Drives for more information).

Methods for sanitization include:

- **Deleting data.** Removing data from your device can be one method of sanitization. When you delete files from a device—although the files may appear to have been removed—data remains on the media even after a delete or format command is executed. Do not rely solely on the deletion method you routinely use, such as moving a file to the trash or recycle bin or selecting "delete" from the menu. Even if you empty the trash, the deleted files are still on device and can be retrieved. Permanent data deletion requires several steps.
    - **Computers.** Use a disk cleaning software designed to permanently remove the data

stored on a computer hard drive to prevent the possibility of recovery.
    - *Secure erase.* This is a set of commands in the firmware of most computer hard drives. If you select a program that runs the secure erase command set, it will erase the data by overwriting all areas of the hard drive.
    - *Disk wiping.* This is a utility that erases sensitive information on hard drives and securely wipes flash drives and secure digital cards.
  - **Smartphones and tablets.** Ensure that all data is removed from your device by performing a "hard reset." This will return the device to its original factory settings. Each device has a different hard reset procedure, but most smartphones and tablets can be reset through their settings. In addition, physically remove the memory card and the subscriber identity module card, if your device has one.
  - **Digital cameras, media players, and gaming consoles.** Perform a standard factory reset (i.e., a hard reset) and physically remove the hard drive or memory card.
  - **Office equipment (e.g., copiers, printers, fax machines, multifunction devices).** Remove any memory cards from the equipment. Perform a full manufacture reset to restore the equipment to its factory default.
- **Overwriting.** Another method of sanitization is to delete sensitive information and write new binary data over it. Using random data instead of easily identifiable patterns makes it harder for attackers to discover the original information underneath. Since data stored on a computer is written in binary code—strings of 0s and 1s—one method of overwriting is to zero-fill a hard disk and select programs that use all zeros in the last layer. Users should overwrite the entire hard disk and add multiple layers of new data (three to seven passes of new binary data) to prevent attackers from obtaining the original data.
  - *Cipher.exe* is a built-in command-line tool in Microsoft Windows operating systems that can be used to encrypt or decrypt data on New Technology File System drives. This tool also securely deletes data by overwriting it.
  - *Clearing* is a level of media sanitation that does not allow information to be retrieved by data, disk, or file recovery utilities. The National Institute of Standards and Technology (NIST) notes that devices must be resistant to keystroke recovery attempts from standard input devices (e.g., a keyboard or mouse) and from data scavenging tools.
- **Destroying.** Physical destruction of a device is the ultimate way to prevent others from retrieving your information. Specialized services are available that will disintegrate, burn, melt, or pulverize your computer drive and other devices. These sanitization methods are designed to completely destroy the media and are typically carried out at an outsourced metal destruction or licensed incineration facility. If you choose not to use a service, you can destroy your hard drive by driving nails or drilling holes into the device yourself. The remaining physical pieces of the drive must be small enough (at least 1/125 inches) that your information cannot be reconstructed from them. There are also hardware devices available that erase CDs and DVDs by destroying their surface.
  - *Magnetic media degaussers.* Degaussers expose devices to strong magnetic fields that remove the data that is magnetically stored on traditional magnetic media.
  - *Solid-state destruction.* The destruction of all data storage chip memory by crushing, shredding, or disintegration is called solid-state destruction. Solid-State Drives should be destroyed with devices that are specifically engineered for this purpose.
  - *CD and DVD destruction.* Many office and home paper shredders can shred CDs and DVDs (be sure to check that the shredder you are using can shred CDs and DVDs before attempting this method).

For more information, see the NIST Special Publication 800-88 Guidelines for Media Sanitization.

How can you safely dispose of out-of-date electronic

devices?

Electronic waste (sometimes called e-waste) is a term used to describe electronics that are nearing the end of their useful life and are discarded, donated, or recycled. Although donating and recycling electronic devices conserves natural resources, you may still choose to dispose of e-waste by contacting your local landfill and requesting a designated e-waste drop off location. Be aware that although there are many options for disposal, it is your responsibility to ensure that the location chosen is reputable and certified. Visit the Environmental Protection Agency's (EPA) Electronics Donation and Recycling webpage for additional information on donating and recycling electronics. For information on recycling regulations and facilities in your state, visit the EPA Regulations, Initiatives, and Research on Electronics Stewardship webpage.