Settings. The proper setting of machine options can optimize security. The vendor can assist or merely review the menu on the equipment to choose the security options.

A security audit of copiers, fax machines, printers, and multifunctional devices connected to the Internet or network can assure that all firewalls are in place, up to date, and effective. When this equipment is discarded, all IP and email addresses must be deleted. This can be done through the menu on the machine and the vendor can explain this process as well.

Hard Drive Destruction is the most effective means of assuring data security. Destruction of the hard drive, replacement with a new one and reinstallation of the operating system eliminates all data. Physically shredding the hard drive will guarantee confidentiality. This service is available through both vendors and manufacturers.

Maintaining and securing confidential information is the user's responsibility, but the office technology industry understands the problems and knows the solutions. Whether the goal is to protect a business, or to comply with HIPAA, Sarbanes-Oxley, or Gramm-Leach, the tools are available. Ask the right questions and contact your office technology vendor for help. Begin the process when evaluating the equipment and make security part of the equipment solution.

For additional information:

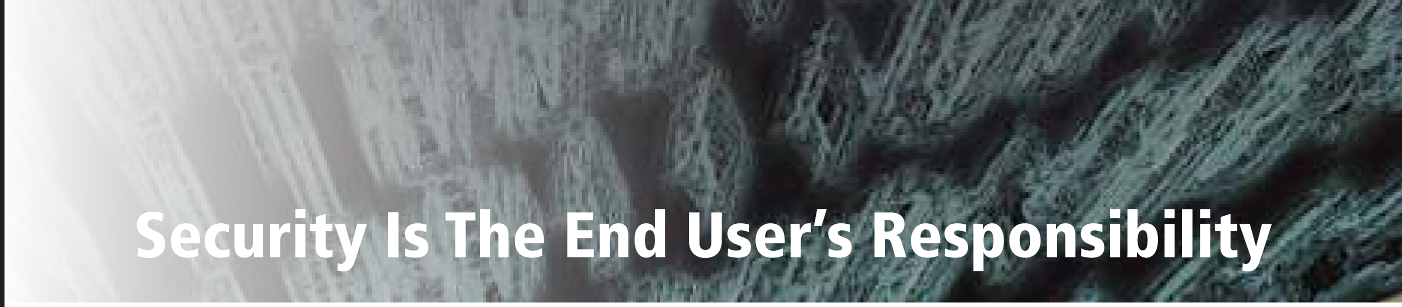
Business Technology Association
12411 Wornall Road
Kansas City, Missouri 64145
816/941-3100
www.bta.org

DATA SECURITY for Copiers, Faxes, Printers & Scanners

Business Technology Association

Unquestionably the age of technology has vastly changed the way businesses operate with increased speed of communication, document production and replication. Similarly, security issues have grown well beyond the need to throw away a carbon copy. In fact, successful offices today are alert and attuned to security issues throughout their businesses and have detailed security protocols in place. Documents are shredded to prevent Dumpster Diving. Firewalls are installed to prohibit hackers. Employees are trained to refrain from opening unsolicited emails, responding to phishing emails, or transmitting sensitive information without encryption. Passwords are unique and changed regularly and even physical security has been increased with limited access to buildings, file cabinets, and networks. With all of these measures in place, one would expect security to be almost unbreachable, but one important area often remains unprotected: copying and printing devices. State-of–the-art copiers, printers, fax machines, and multifunctional devices are all potential security hazards.

When these machines improved from analog to digital operations, they became much more efficient, but caused new confidentiality problems. In recent years these devices contain a hard drive that renders them a computer in disguise. Failure to recognize this fact meant no measures were taken to deal with erasing a hard drive and, therefore, information was subject to theft.



Security Is The End User's Responsibility

When copying or printing confidential information, it is up to the end user to ensure the data will be protected. Whether at the office, copy shop, library, or grocery store the copy or print one takes away may leave a trail of data for others to access. Most likely the personal or home use devices are not equipped with a hard drive and use volatile memory that is erased once the image is processed. As the functionality of the device increases, so do the security risks. Is it possible to take advantage of this new, improved equipment and still protect the integrity of the information? **It is if:**

The End User Asks the Right Questions of the Right People

1. Check with your vendor or manufacturer's website to determine if the device has a hard drive or other method of data storage. Also find out if the hard drive is actually used in the copy-making process. Once it is clear that the machine does present a problem, remedies are available.

2. Determine from the vendor what standard features and settings are built into the device and how additional options can be activated to provide greater security.

3. Some devices have options that can be installed to address this issue such as:

Image overwrite systems provide for instant, scheduled, or on-demand overwrite. Effective overwriting will electronically shred data. Overwriting may affect the speed of the machine's operation if done immediately, however a few seconds for security is well worth the time. In contrast, simply deleting the file will only mask the location but keep the data intact.

Encryption packages render images indecipherable. Many of these packages meet Department of Defense and Advanced Encryption Standards and are offered by all manufacturers and implemented through your vendor.