Article: 7 Ways to Protect Your Printers
Date: 30/12/2011
Posted by: HeelpBook Staff
Source: Link
Permalink: Link

Can a hacker burn down your business by remotely setting one of your printers on fire?

However, even if your printers can't be used as remote firestarters, there are many risks involved in networking a printer.

Businesses often overlook keeping the printing environment secure.

Data security gets a lot of attention, and file servers provide encrypted, access controlled storage. Workstations are encrypted as well, with password and even biometric access required. Databases and even files often require a password just so you can see what's inside. Then you print that sensitive data, sending it off to a printer that may not be nearly as secure as the rest of your system.

You can avoid most networked printer problems by following the first three basic steps listed below. If you deal with highly sensitive data, then you need to go beyond those by protecting your printout at every step along its journey.

HP has detailed information on how to use its products to protect your data, and other printer providers offer similar solutions as well. Regardless of the vendors you use, consider all seven of these steps to keep your businesses data secure through the printing process.

1. Unplug

If you want to avoid network printer problems, don't network your printer. Connecting directly from a PC via USB keeps your printer and your print jobs private.

2. Password

Most networked printers can be accessed remotely with a password. **Change the default password!** This is perhaps the most important step of all for a networked printer.

3. Firmware

When security issues are discovered, printer makers release updates to its firmware. Keep your printer firmware updated. By keeping your printer secure with a strong password, and closing any known security holes with up-to-date firmware, you'll avoid most basic network printer issues.

4. Secure Your Infrastructure

Whether you have two printers or 200, they need to be managed. Keeping passwords updated, installing the latest firmware, and securing access are just a few of the steps you can handle through remote-management software.

HP's **Web JetAdmin** is one example, allowing you to keep tabs on all your HP printers from one workstation. You should also use firewalls to protect against outside attacks and probing, and be sure that *Wi-Fi networks are secured*.

5. Secure Your Data

When you send a print job, be sure that it's on a secured network. Use encryption so a print job can't be intercepted along its path. Print jobs can even be sent to an encrypted print server, and then securely "*pulled*" from the server when ready.

6. Secure Your Printers

Beyond changing the default password, implementing access control can protect the printer from being accessed remotely or on-site. Printers with hard drives for spooling should be encrypted. Once a job is printed, traces of it should be erased from the hard drive and from memory.

7. Secure Your Printouts

If you generate secure documents with special paper, secure trays are available to protect the media. Avoid leaving documents sitting in a printer tray. Use private printing to send your jobs to the printer, or at least send them as "*manual feed*".

This will assure that a user must be at the printer to release the job, reducing the chance of a printout being forgotten and falling into the wrong hands.