Information Security Office (/)

Network Printer Security Best Practices

Multifunction printers (MFPs) are experiencing an identity crisis: IT administrators don't always see them as the full-fledged networked computers they really are. But attackers do - and they are finding them increasingly very attractive!

These printers, shoved in the corner of the office and quietly going about their business of copying, printing, faxing and scanning, might not seem to pose any real security risk. But like any networked device, if not properly managed, they can expose sensitive campus data to unauthorized access and misuse.

To secure your printers from unauthorized access, print configuration alterations, eavesdropping, and device compromise follow these printer security best practices:

Manage Printer Access

Campus printers should not be exposed to the public Internet

Take the following appropriate measures to make sure that the printer is configured only to allow access from approved networks and devices:

- Campus departments should consider using RFC1918 private IP address space to restrict access to printers to campus hosts only, making printers unreachable from the Internet
  - **Note:** RFC1918 private IP address space is offered by IST Network Operations and Services (https://technology.berkeley.edu/services/network-voice-and-connectivity/data-networking-services) and can be ordered from the Berkeley Telecom Catalog (http://telcat.berkeley.edu/)
- Restrict access using a IST network firewall, available free to campus departments
  - **Note:** IST network firewall services are offered by IST Network Operations and Services (https://technology.berkeley.edu/services/network-voice-and-connectivity/data-networking-services) and can be ordered from the Berkeley Telecom Catalog (http://telcat.berkeley.edu/)
- Configure the printer's access control list (ACL) to restrict access by subnet or device
- Remove the default gateway in the IP configuration to disable Internet routing, making printing only available on your local network segment
- Use a low-cost hardware firewall to block public Internet access to the printer
- Configure another machine as a dedicated print server with appropriate access controls

Change the default password to the administration control panel webpage

Do it now! If your printer's administrative panel is not securely configured, attackers can potentially:

- Change the printer's network address and reroute print jobs
- Perform a Denial of Service (DOS) attack and render the device inoperable
- Use the printer as a platform to attack other systems on the network

An attacker with unauthorized access can also install malware on the printer allowing remote back-door access.

Use encrypted connections when accessing the printer administrative control panel

For example, when accessing the printer interface via a web browser, use an "https://" address (which uses SSL encryption) instead of a regular "http://" address. If you need command line access, use SSH instead of Telnet to prevent eavesdropping.

Don't Run Unnecessary Services

Many printers have insecure and unnecessary protocols enabled by default (e.g., Telnet, HTTP, FTP). Leaving these services enabled provides attackers with the ability to access the printer data directly. While a practical joker with limited knowledge of printer job language (PJL) might only Telnet to change the "Ready" message to something cute ("Insert Coin"), a more malicious attacker could potentially browse the printer's hard drive and view all the data stored there.

Disabling these services prohibits your printer from being used for unintended purposes, such as hosting pornography, or as an FTP server for copyright-protected music and movies.

Update and Patch

Just like computers, printers and multi-function devices need updates and patches. Check for firmware updates on all printer and network devices as part of your regular patch management schedule. Updates can add new or improved security features, patch known security holes, and fix other issues.

Make sure your multi-functional printer doesn't create a gaping security hole and expose sensitive campus data to unauthorized access and misuse.

Choose the Right Printer

Home and small office printers are usually not well-suited to be connected to UC Berkeley's high speed, open network. These low-cost printers often do not meet the campus basic Minimum Security Standards for Networked Devices (https://security.berkeley.edu/minimum-security-standards-networked-devices-mssnd) (MSSND). If the printer is used to handle sensitive information, a home or small office printer is even less likely to have the security functionality necessary to meet the more stringent MSSND requirements for sensitive data.

For shared departmental printing, make sure to select a business workgroup printer. These printers store print jobs, passwords and other information on their hard drives, and provide disk encryption to protect sensitive data stored on the device. They can also erase data after the print job has run.

Remember that everything printed, copied, faxed or scanned is stored on the printer hard drive - and make sure that when a printer is de-provisioned or sent offsite for servicing, it is wiped clean of any stored data.

The UCSF Print Management Program (http://campuslifeservices.ucsf.edu/documentsmedia/services/print_management) is available to UC Berkeley campus departments as a complete printer/copier management service.

Unwanted Printouts

If you notice unwanted printouts (spam, harassment, or offensive material) happening in your department, please contact IT Client Services (submit online ticket (https://berkeley.service-now.com/ess/) or email itcsshelp@berkeley.edu (mailto:itcsshelp@berkeley.edu)) as soon as possible to assist in securing your printers and report the security issue (https://security.berkeley.edu/i-want/report-security-incident) to the Information Security and Policy team.

Back to Top