

Printer Security Checklist





Are your all-in-one printers secure?

We can help! \$800.875.5042

info@milner.com

Use a firewall for your devices The firewall blocks suspicious activity and protects the network from unauthorized access via the device. This firewall should be in addition to general network firewalls.
Restrict access to printers, faxes, scanners and copiers Devices should only be physically accessible to authorized staff in secure areas. Device or network settings should restrict access to specific users to prevent unauthorized access.
Ensure only authorized users can access the devices Printers, faxes, copiers and scanners or all-in-one devices can be accessed and used by anyone unless settings are modified to ensure only specified users access the device.
Disable USB ports USB keys can contain undetectable malware and corrupt the device. Users can also use USB ports to obtain data without authorization.
Erase device hard drives periodically
Printers, copiers, faxes, scanners and multifunction devices can maintain copies of documents on their hard drives. Erase periodically to mitigate potential data loss.
Implement SSL encryption for information transmission Data needs to be secure in transmission and at rest on the device's hard drive. SSL provides the best form of encryption to protect information throughout its use.
Monitor copiers, printers, scanners and faxes Maintain audit trails that specify who used the device, what information was accessed, when it was accessed and the date and time accessed.

Prohibit printing from non-company assets

and other network components.

Employees or guests should not be able to print using cellphones or personal computer devices. These devices can easily contain malware that can infect printers