

Donovan Rhone is a Senior Account Manager for Knight Office Solutions and has been in the office equipment industry for over 25 years, specializing in working in the AEC Industry for the past 15 years. Along with Managed IT Services, Mr. Rhone also helps companies by providing printers, MFPs, plotters and document workflow solutions. He is passionate about customer service and bringing the latest technology to all of his customers.

Improving Your Printer Security

The recent flurry of high-profile cyberattacks has many business leaders rethinking their IT security strategies, but even as organizations ramp up their efforts, one vulnerability often goes unchecked. What are we talking about? Printers.

Think about all the data that passes through your organization's print environment: customer payment information, sensitive internal memos, employee records. Now consider the fact that the vast majority of network-connected printers can be accessed remotely.

"Okay, but what can a hacker really do from my printer dashboard?"

More than you might think. Most MFPs allow you to change scan-to-email addresses remotely, allowing hackers to intercept any document scanned from that device. Some printers even allow you to access documents that have been previously printed on that machine.

Combined with the fact that these devices are often protected by weak security, it's not hard to see why hackers are setting their sights on printers & copiers. This email will walk you through five steps you can take to secure your print environment:

1. Make sure you've locked down your network.

If your users connect to printers over the network, ensure that your environment is protected by a firewall, encrypted, and secured by a strong password. You may also want to consider routing your data through an encrypted server for an added layer of protection. This will prevent cyber attackers from intercepting your data in transit. Want to go a step further? There are a variety of security scanning tools on the market that can help you identify vulnerabilities in your print network.

2. Regularly change your printer passwords.

Just as you change your PC passwords on a regular basis, so too is it important to change the passwords that secure your printing devices. Update your passwords at least every three months, and make sure that your passwords include upper and lower case letters, numbers, and symbols. This will ensure that hackers can't guess your password, and will limit employee access to those who regularly need admin privileges.

3. Keep your firmware updated.

"Printers and copiers are basically set-it and forget-it, right?"

You might think so, but the truth is that your printing devices receive updates and security patches just like your PC. Keep your devices up to date with the latest firmware to ensure that hackers are unable to exploit vulnerabilities within your equipment. Also, be sure to keep an eye on your aging equipment. If your printer is more than eight years old, there's a chance that the manufacturer has discontinued releasing updates for your device. This can leave you unprotected from new attacks, and hackers actively seek ways to exploit the vulnerabilities present in unsupported devices.

4. Implement a document hold solution.

Have you ever printed a document that contained information that shouldn't be shared throughout the organization? If you're like most people, the answer is yes. Consider implementing a document hold solution on machines in common areas to ensure that your sensitive documents are viewed only by those who printed them.

5. Don't forget about your onboard hard drives.

If your printers include onboard storage for spooling, make sure that hard drive encryption is enabled. This will prevent prying eyes from gaining access to data stored in your print history. For the same reason, be sure to wipe the hard drives of any old machines that are being retired or relocated.

Printers and copiers are an easy target for individuals looking to gain access to your sensitive business data. These tips will help you secure your print environment to ensure that your protected data stays that way.