Everything You Need to Know About Printer Security in 2024

By Tyler Cross Senior Writer - December 18, 2024

Short on time? Here's how to secure your printer and wider network in 2024:

1. **Manage your access levels and security settings.** Use your printer's access management settings to control who can use your printer. If you leave it open, anyone could infect it with malware.
2. **Keep your devices and firmware updated.** Make sure your printer and every device connected to it is up-to-date. Software developers regularly release patches to fix exploits and vulnerabilities within your printer.
3. **Protect your printer from threats.** Use a firewall to protect your network, a VPN to encrypt your data, and an antivirus on the devices connected to your printer. Companies like Norton offer all these tools and more in a single package.

Like any device with an internet connection, printers are vulnerable to cyberattacks. Many printers don't have robust built-in security features, and even those that do need to be set up properly. This is a pretty big concern, because a skilled hacker can use a printer to infiltrate your entire network.

This article will go over everything you need to do to keep your printer safe. Bear in mind that every printer is different so there's no one-size-fits-all answer. Rather than provide dozens of specific step-by-step guides, I'll cover the general practices that everyone should follow.

Using an antivirus is an important part of securing your printer. There are a few great options, like Norton, that come with real-time protection to stop malware, firewalls to prevent network intrusions and safeguard your printer from unauthorized access, plus useful extras like VPNs to anonymize web traffic.

The 5 Pillars of Printer Security

It's essential to take a broad-based approach to printer security. You need to protect your printer from unauthorized access, shield your network from direct threats, keep your device firmware up-to-date, and more.

To make things easier to understand, I broke down everything you need to know into 5 pillars. If you want to avoid your printer being exploited by hackers, you'll need to follow the practices outlined in every single one.

1. Access Control

First off, you need to ensure that only authorized people can access your printer. Most printers enable you to set up some form of authentication, such as PIN codes, passwords, biometrics, and

card-based systems. Allowing anyone connected to the same Wi-Fi network to use your printer is simply dangerous.

If you don't currently need a password to access your printer, you can change the relevant setting. If your printer came with a default password like '12345', change it to something harder to crack (any good password manager will come with a password generator you can use to create and store strong passwords). Each printer has a slightly different way of doing this, but it should be easy to find in the printer's settings menu.

Tampering can also be a problem, so you'll need to physically secure the device as well. Whether you have a personal printer or use one at the office, make sure that only trusted people have access. If you don't, anyone could potentially change the settings to infiltrate your network.

Overall, maintaining access control is simple, but requires constant vigilance. Most printers will let you review a list of all the devices that have connected to them. I recommend checking this and changing your password regularly.

2. Wi-Fi Security

Having an unsecured wireless network is just inviting hackers to take control of your printer. Here's what you need to do to enhance your Wi-Fi network's security (the exact steps will vary depending on your printer, but these options should be available in your settings):

- **Protect your Wi-Fi with a strong password.** This will stop the least skilled hackers from using your printer to infiltrate your network.
- **Enable the best security protocols.** If possible, enable WPA3 (Wi-Fi Protected Access 3) encryption on your printer and router. Avoid using WEP or WPA2, as these protocols are outdated and vulnerable.
- **Disable WPS (Wi-Fi Protected Setup).** This will make it slightly less convenient to send jobs to your printer, but it will also make it a lot more secure. Feel free to use WPS while setting up your printer, but I recommend turning it off afterward.
- **Regularly review your Wi-Fi security.** It's possible for cybercriminals to change many of these settings without your knowledge, so make sure they're still enabled every month or so. You can do this manually.

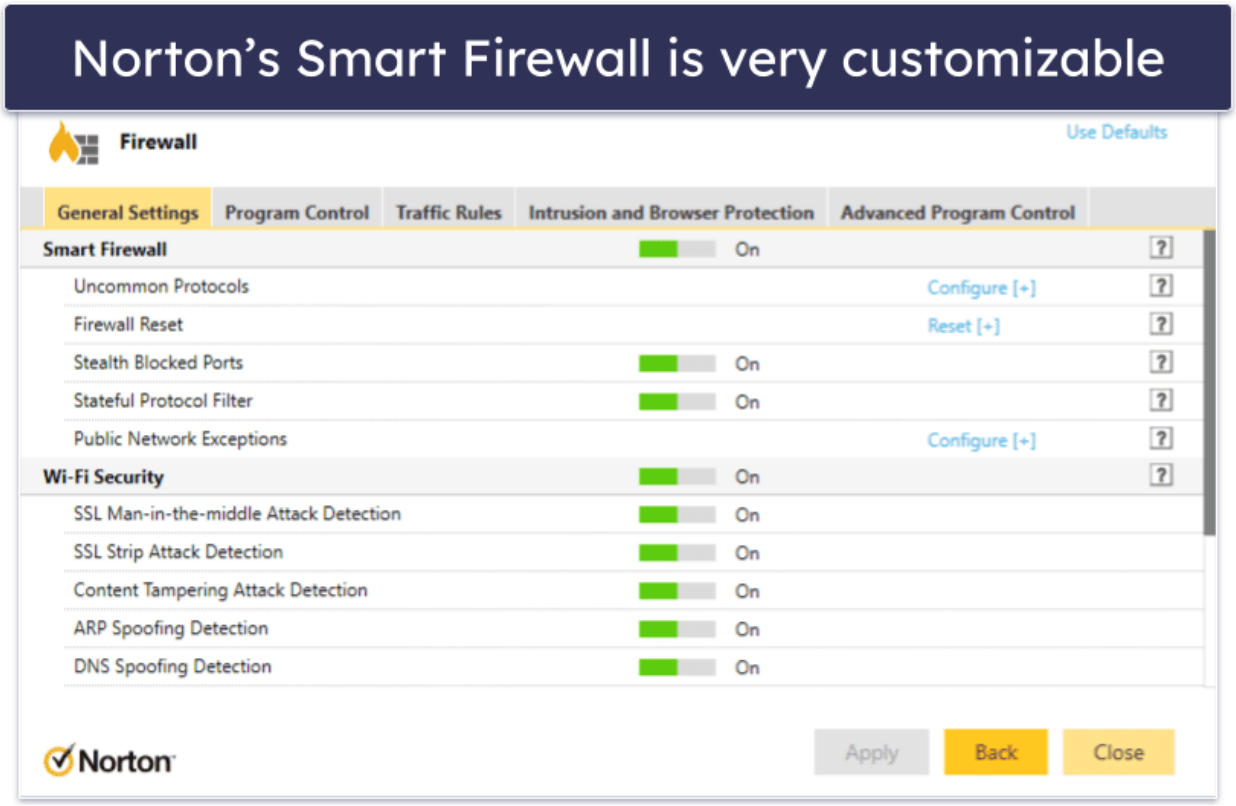
3. Network Security Management

Hackers can use an unsecured printer to launch attacks on your network. And if your network isn't secure, anyone can gain access to your printer. This interconnectedness means you need to make sure all of your devices are secure.

The first thing you should do is close unused ports and disable any unnecessary network protocols. Printers typically use communication protocols like FTP, Telnet, or SNMP. If these are left open when the printer is not in use, it's trivial for hackers to access your wider network. Only keep essential ports open, like IPP or HTTPS. If possible, I also recommend running your printer on a subnet or virtual LAN (VLAN) rather than your broader Wi-Fi network. This is a bit tricky to do, but you'll find plenty of guides online.

A good firewall is essential. In addition to blocking attempts to access your network, you can also use a firewall to monitor every device on your network for suspicious activity. Antivirus suites like Norton and Bitdefender include powerful firewalls. Firewalls are also helpful because they can be used to easily manage your ports, which as we just learned, helps protect your printer against external

threats. Many also allow you to set ports to stealth mode, which creates a big stumbling block for opportunistic hackers.



Finally, you have to continually monitor your network so you can spot any unusual behavior. Again, firewalls make this much easier, but you should be able to manually pull up a list of connected devices using your printer' settings menu or web interface. Businesses may also want to set up Intrusion Detection Systems (IDS) and other network monitoring tools.

4. Data Protection

Taking steps to protect your data will go a long way toward securing your printer, especially if you regularly use it to print out sensitive information. A printer hack could result in identity theft under the right circumstances.

- **Regularly clear your printer's data cache.** Printers store data, including any files that get printed and documents that are scanned. You may be able to make it so your printer automatically deletes its data (again, check the settings menu). If not, you'll need figure out how to manually erase data and do so regularly.
- **Encrypt your data.** Most modern printers have a setting to automatically encrypt incoming and outgoing data, but this only encrypts your data in storage. Make sure your data is encrypted during transmission and use secure protocols like SSL/TLS.
- **Consider using a VPN to encrypt all of your traffic.** While standalone options like ExpressVPN are excellent and come with the most security features, you can get a good reliable VPN with many antivirus suites. If you're able to install the VPN on your router, all of your devices will have their data automatically encrypted.

5. Device Protection

Last but not least, you also need to secure your printer and all the devices connected to it. Here's what it takes to secure your devices:

- **Keep your device firmware up to date.** Always opt to install updates when prompted to on all of your devices. Some printers won't do this automatically, so I recommend regularly checking the manufacturer's website for new updates. Each update includes security patches and fixes for newly discovered vulnerabilities.
- **Install a reliable antivirus.** Each device that connects to your printer should have reliable antivirus software installed. Norton is my top pick when it comes to printer security thanks to its advanced firewall, excellent malware protection, and bonus features. You won't be able to install the software on your printer, but Norton comes with apps for Windows, Mac, Android, and iOS devices.
- **Use a password manager.** To be upfront, this is only tangentially related to printer security, but it will help. Use a password manager to keep track of your unique passwords, PIN codes, and more. A product like 1Password lets you store an unlimited number of passwords, notes, documents, and more within its encrypted vaults.

Editors' Note: ExpressVPN and this site are in the same ownership group.

What Are the Dangers of an Unsecure Printer?

Printers aren't as simple and safe as they seem. They are almost always networked, and they store the data of every document they process (which could include personal information). Despite the risks, most printers don't have the same level of security that computers have. Here are some of the ways hackers can exploit printers to cause real harm.

- **Data theft.** Hackers who have infiltrated your printer will be able to steal your data. If you store and print sensitive documents, like contracts, financial paperwork, or identity-related paperwork, this should be very concerning. Luckily, many antiviruses (including Norton) come with dark web monitoring tools that will alert you if your data is leaked online and provide assistance in the event of identity theft.

- **Network breaches.** Hackers often exploit vulnerabilities in unprotected printers to gain entry into your broader network. Once inside, they can access other devices, exfiltrate data, or install ransomware.
- **Malware infections.** A compromised printer can act as a host for malware, spreading malicious code to other devices connected to the same network. Needless to say, a good antivirus is essential.
- **Unauthorized print jobs.** Attackers might use your printer to send out massive print jobs, including spam, pornography, and illegal content. Hackers have also been known to send printouts containing malicious QR codes and URLs for dangerous websites.
- **Non-compliance fines.** If your organization's printer is tied to a data breach, you could face steep fines for non-compliance with government regulations, like the GDPR. If extremely sensitive data gets compromised, these fines can end up costing you millions.

How to Tell if Your Printer Was Hacked or Has a Virus

It's not always obvious when a printer has been compromised, but there are some warning signs. Here's how you can tell if your printer was hacked or is infected by malware:

- **Strange or unexpected print jobs.** If your printer suddenly starts making strange prints, like random symbols or characters, memes, or explicit material, there's a good chance that it's been hacked. Sometimes this is a simple prank, but it could also be a distraction from a more serious attack going on under the hood.
- **Slow or erratic performance.** A hacked or infected printer may become noticeably slower, freeze during print jobs, or behave unpredictably. Malware and unauthorized access can overload its processing power, causing these performance issues. One or two glitches here and there are normal, but if it frequently acts up or behaves in ways that make no sense, there's a strong chance it's been compromised and it's time to act.
- **Unexpected changes.** If you notice settings like passwords, network configurations, or remote access permissions have been altered without your knowledge, this could be a sign of a breach. Attackers often modify these settings to maintain long-term control over your printer and launch further attacks on your network.
- **Suspicious network activity.** Printers that communicate with unknown or unauthorized IP addresses, send unusual amounts of data, or remain active when idle could be infected. Norton's firewall includes tools to monitor your network while features like stealth mode add extra security.
- **Frequent error messages or restarts.** Malware can interfere with a printer's firmware, causing constant crashes, unexpected restarts, or error messages. It's normal for any device to crash or restart here and there, but it's always a bad sign if this happens frequently and for seemingly no reason.
- **Security alerts.** If your antivirus software or firewall flags your printer for unusual behavior, this is a strong indication of a problem that requires immediate attention. It's not unusual for your antivirus to flag your printer the first time you connect to it, but it's a crimson red flag if you get an alert every time you connect to it.

What to Do if Your Printer Has a Virus

If you think your printer has become infected, don't panic. There are a few easy steps you can take to fix the problem. For some of these steps, you'll need to have a good antivirus and a VPN.

1. **Disconnect the printer from your network.** Immediately disconnect your printer from the internet or your local network to prevent the virus from spreading to other devices. The longer something stays connected, the greater the chance it will also become infected.
2. **Check for firmware updates.** Visit the manufacturer's website and download any available firmware updates or security patches. With any luck, the latest patches will have already fixed the vulnerabilities that led to the infection.
3. **Factory reset your printer.** If updating the firmware doesn't resolve the issue, perform a factory reset on the printer. This step wipes stored data and settings, removing any malware. Be warned that this also erases any data or settings that you have saved to your printer and that you'll have to re-configure any settings you changed.
4. **Scan and secure your network.** Use your antivirus to scan any computers or phones that are connected to your printer and make sure they're virus-free. Afterward, set up a firewall with intrusion prevention and then encrypt your network using a VPN.
5. **Manage your printer security settings.** Every printer is different when it comes to specific security features, but they all have some. Enable encryption, set strong administrative passwords, and disable unused features such as remote access, Wi-Fi Direct, or USB ports. Revisit your settings periodically or if your network condition changes to make sure they're still configured properly.