

How to Update Printer Firmware Now to Stop Hackers

With hackers exploiting security vulnerabilities, now is the time to update printer firmware to keep your network and devices safe.

You keep your computers, phones, and tablets updated with the latest security patches to keep hackers at bay, but what about your printers? With hackers exploiting security vulnerabilities, now is the time to update your printer firmware to keep your network and devices safe.

Check if the printer is affected

For the current threat, Brother printers are the primary target, but they are not the only brand. Please check the regularly updated list to see if your printer model is affected. This does not mean that hackers have compromised your machine. It just means that the vulnerability is still there and you need to update your printer firmware now.



The screenshot shows the CVE Details website interface. At the top, there is a search bar with the placeholder text "Enter keywords (e.g.: CVE ID, sql injection, etc.)" and a "Search" button. Below the search bar, there are links for "Search tips" and "Provide feedback". A notice banner states: "Notice: Expanded keyword searching of CVE Records (with limitations) is now available in the search box above. Learn more here." The main content area displays the CVE ID "CVE-2024-51977" with a "PUBLISHED" status tag. To the right of the ID are links for "View JSON" and "User Guide". A "Collapse all" button is located below the CVE ID. The section "Required CVE Record Information" is expanded, showing a dark blue header for "CNA: Rapid7, Inc." and the following details: "Published: 2025-06-25 Updated: 2025-07-25" and "Title: Unauthenticated Leak Of Sensitive Information Affecting Multiple Models From Brother Industries, Ltd., FUJIFILM Business Innovation, Ricoh, Toshiba Tec, And Konica Minolta, Inc."

Easy printer firmware updates

Even if your printer isn't on the list, you should still update the firmware. Depending on your printer's manufacturer and settings, the firmware may update automatically, but you'll usually have to confirm the process manually.

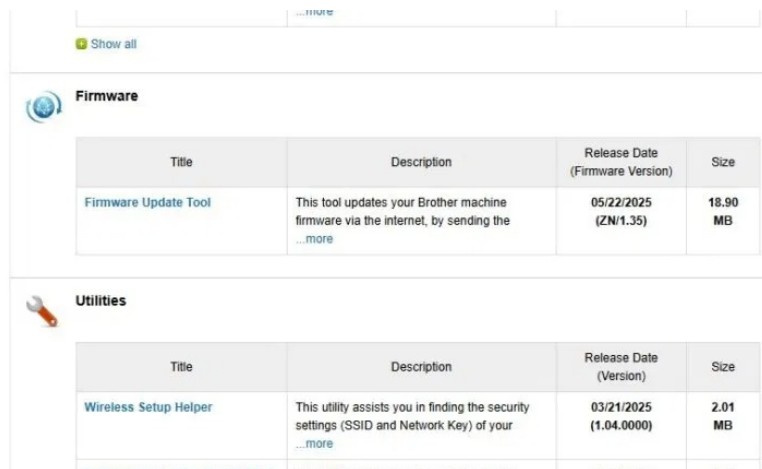
The exact process will vary depending on your printer manufacturer. Typically, there are a few common options:

1. Use printer update software, which may be included with the printer software.
2. Use the online portal using the printer's IP address (If you're having trouble connecting your printer over Wi-Fi, try these fixes)
3. Download to USB drive and plug directly into printer.
4. Download and run the firmware update while the printer is on and connected.
5. Update with printer screen.

Since Brother printers are primarily affected, we'll use Brother as an example. Start by visiting the printer manufacturer's website. Go to the **Support** section. This may also be a **Help**, **Downloads**, or **Resources** page, depending on the printer brand.

Enter your printer model to search for downloads and resources. Locate your printer model on the printer itself, in the printer settings on your computer, or in the printer's user manual.

Find available downloads. Select your operating system, if necessary, then navigate to any firmware downloads.



The screenshot shows a web interface with a search bar at the top. Below it, there are two sections: 'Firmware' and 'Utilities'. Each section contains a table with columns for Title, Description, Release Date (Version), and Size.

Title	Description	Release Date (Firmware Version)	Size
Firmware Update Tool	This tool updates your Brother machine firmware via the internet, by sending the ...more	05/22/2025 (ZN/1.35)	18.90 MB

Title	Description	Release Date (Version)	Size
Wireless Setup Helper	This utility assists you in finding the security settings (SSID and Network Key) of your ...more	03/21/2025 (1.04.0000)	2.01 MB
Network Configuration Basic Tool	This utility assists you in restoring settings	11/05/2024	4.57 MB

In this example, you'll download the Firmware Update Tool to update the firmware online, sending the update directly to your Brother printer.

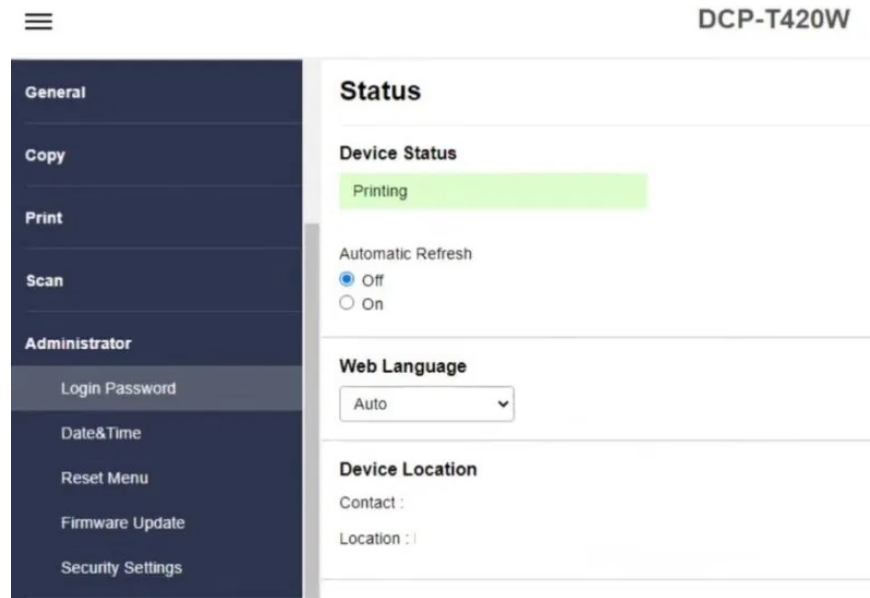
Regardless of your printer manufacturer or model, you should find update files and instructions on the manufacturer's website.

The update process usually only takes a few minutes. You may need to restart your printer after it's complete. In some cases, you'll also need to reconnect your printer to your device and/or network.

Change printer password

Most of the printer manufacturers affected by this vulnerability are releasing firmware updates to fix the issue. However, if the update is not available or fails to install for whatever reason, another way to protect yourself is to change your printer password.

Using the default admin password makes it easy for hackers to take control of your printer just by reading the model and serial number. If the password were different, it would be an obstacle that hackers might not bother with, especially if they are just trying to create a botnet instead of accessing your entire network.



Again, this process will vary depending on your printer manufacturer. There are a few common methods:

1. **Open the printer software/app** . Check the Settings section to see if there are any security or privacy options. This may allow you to change your password.
2. **Connect to the printer via a web browser** . Enter the printer's IP address and log in with the default admin password (found in the user manual and sometimes on the printer itself). Change the password and save the settings.
3. **Use the printer control panel** . Access settings, privacy, or security options from the printer menu and change the password from there.

Obviously, hackers aren't just targeting printers. But consider this incident a reminder of why you should always keep your printer firmware up to date. Also, make sure you're using antivirus and/or antimalware software to protect your other devices.

You finished reading the article "**How to Update Printer Firmware Now to Stop Hackers**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.