

BEWARE OF RANSOMWARE VIA YOUR PRINTER

The criminals who are infesting our computers with ransomware are constantly looking for new avenues of entry. There is now evidence that they have discovered that printer port 9100 may be “open” on some of our systems, thus providing easy access for their malware.

Here’s how to find out whether or not port 9100 is open and vulnerable:

1. Open your favorite browser.
2. Search for grc.com/shieldsup, which will take you to the following page.

Welcome to ShieldsUP!

If you have not visited for some time, please note that:

- Our new **Perfect Passwords** facility is used by thousands of people every day to generate ultra-high-quality random passwords for securing WiFi and other services.
- Our weekly **Security Now!** audio podcast has covered **every security issue** you might have. These mp3 audio files are freely downloadable, and since we have transcripts of every podcast, you can use our sitewide search to find any podcast by keyword.

If you are new to this site and our services:

Please take just a moment to read and consider these three points:

Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probes must travel from **our** server to **your** computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.

NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.

If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: **4.79.142.192** -thru- **4.79.142.207**. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATTACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.

Proceed

3. Click on the **Proceed** box that appears on the webpage.
4. After a brief delay, the following section will appear.

5. In the blank box, type **9100**, then click **User Specified Custom Port Probe**.
6. When the next screen appears, scroll down to find a section that looks like this:

| Port | Status | Protocol and Application |
|------|---------|---|
| 9100 | Stealth | pdl-datastream Printer PDL Data Stream |

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

7. This demonstration shows that port 9100 is “closed” or stealthed. Thus, through the eyes of any hacker, this port does not exist on the Internet.

What should you do if port 9100 is open? Your printer driver is probably out-of-date. Go to your printer manufacturer’s website and download the most recent driver for the model of your printer.