Can hackers really access a printer and order it to overheat until it catches fire? Or, even, worse, use it as a copy machine for identity theft? Sounds far fetched, but not according to researchers at Columbia University.

The researchers claim to discover a security exploit in internet-connected HP Laserjet printers using little more than an infected firmware update. Hackers could send a file containing the hack directly to a device, since most printers look for firmware updates every time a job is received--but rarely check the validity of incoming files.

In a demonstration, the researchers hijack a printer and make it overheat the fuser unit (the heated rollers bonding toner particles to paper), nearly burning the paper inside until the thermal switch inside the printer shut the system down.

The researchers say this way cheaper printers lacking a thermal switch can turn into a potential fire hazards.

HP of course challenges such claims-- saying the "potential security vulnerability" has been identified and fixed already. The company is also working on a firmware upgrade to "mitigate the issue," and suggests users should secure their networks by placing printers behind a firewall and disable remote firmware uploads on exposed printers.

Go Millions of Printers Open to Devastating Hack Attack Researchers Say (MSNBC)

Go HP Refutes Inaccurate Claims, Clarifies on Printer Security