Do’s and Don’ts of Shared Printers

That often-frustrating machine down the hall may look like a mere printer to you—but it’s actually a powerful computer, and it’s chock-full of sensitive company/agency information.

Hackers can use printer vulnerabilities to capture old printer logs, which may contain sensitive information, experts say. They may also use printer security flaws to establish a toehold in an organization’s network, through which they can then move freely to gather data. With all these risks in mind, here are some Do’s and Don’ts to stay secure:

Do understand the nature of a modern printer. As noted above, it’s not just a box and ink; it’s a sophisticated, networked computer that probably has access to an astonishing trove of corporate data. Also, think of the shared printer as an internet of things device—and we’ve all been reading about the breaches caused by the IoT!

Don’t leave sensitive print jobs sitting around. This is another, far more basic, risk inherent in shared printers—people print documents but don’t pick them up promptly, leaving too much data available to prying eyes.

Do clear jams and settle other issues. It may be frustrating to take time to address printer trouble (out of paper, low toner, jams—you know the drill). The problem is that when a jam finally does get cleared, a bunch of jobs print all at once, leading to the risk described above.

Don’t hesitate to remind your co-workers. If you walk to the printer to fetch your own document, and you find a sensitive job left there by a colleague, it’s important that you walk their documents to their workspace. Remember, security is everybody’s job! You might even nudge them to pick up their print jobs promptly in the future.