STAPLES
Business Advantage®

Do You Know the Three Ds of Print Security?

As technology advances, printers are looking and acting more like PCs, which means they are susceptible to the same security issues that PCs have. However, many IT professionals don't have near the same level of security concerns for their printers as they do for their devices and servers. The truth is that printers are vulnerable too and as many as 64% of IT managers have reported some form of printer malware on their machines and 60% have reported having a printer data breach.*

It's more important than ever to make sure all of your devices – including printers - are protected. Printer protection can be as simple as remembering the three Ds of print security: **DEVICE, DATA, DOCUMENTS**. Read on to understand the risks….

DEVICE

Top Risks	Pro Tip
The average MFP has **250+ security settings** that create easy access points into the network	Partner with an IT vendor that provides **security software solutions** that monitor and manage printer settings and firmware notification upgrades automatically
Open access to **control panels** or **USB ports** that don't require authentication create weak links	Implement **authentication protocol** for printers so that only authorized users can change settings and disable all USB and open ports to prevent walk-up and mobile access
Loading of fictitious firmware often occurs during **reboot or restart** which is when printers are most vulnerable	Consider technology that has **built-in controls** to prevent access during reboot/restart, allowing access for this only to IT staff

Continued on second page

Do you know the three Ds of print security?

Continued from first page

DATA

Top Risks	Pro Tip
MFPs are the **most common** data input and output devices which means data can be at risk during transit	Implement **data encryption processes** to avoid data breaches while content is being transmitted
Printers/MFPs can allow access to company sensitive data and personal information by sending sensitive documents to any **email or fax** via basic multifunction capabilities	Ensure access to your printers/MFPs are limited to those with **access codes** or other authentication processes to prevent entry point into your network where sensitive data resides
Compliance standards from the government as well as corporate and healthcare regulations can be difficult to keep pace with	Work with an IT vendor for your hardware and software settings that ensure company and government compliance for **data security**

DOCUMENTS

Top Risks	Pro Tip
Sensitive information is often printed and left sitting in the **output bin** of the printer which makes it accessible for anyone to see	A short **training session** for employees to remind them of the importance of securing printed data can alleviate sensitive documents getting into the wrong hands
Open access to various **paper trays** that may contain specialty templates like company checks, prescription forms, blank invoices and shipping labels are often left in the trays for others to access	Utilize the latest printer/MFP technology that allows for **locking of paper trays** and limits access to only authorized personnel
Documents that are sent to **folders or email**, regardless of encryption, are often targets for those looking to steal confidential information or records	Working with an **MPS provider** can help secure documents in transit with multiple encryption levels that utilize technology that **incorporates metadata** for audit tracking and sender verified credentials

Don't let a print data breach happen to you. Learn how Staples Business Advantage can partner with you to alleviate risks. Visit us at **www.staplesadvantage.com/MPS** or call **844-243-8645**

* Ponemon Institute, "Insecurity of Network-Connected Printers," October 2015.
Ponemon Institute, "Annual Global IT Security Benchmark Tracking."

STAPLES Business Advantage