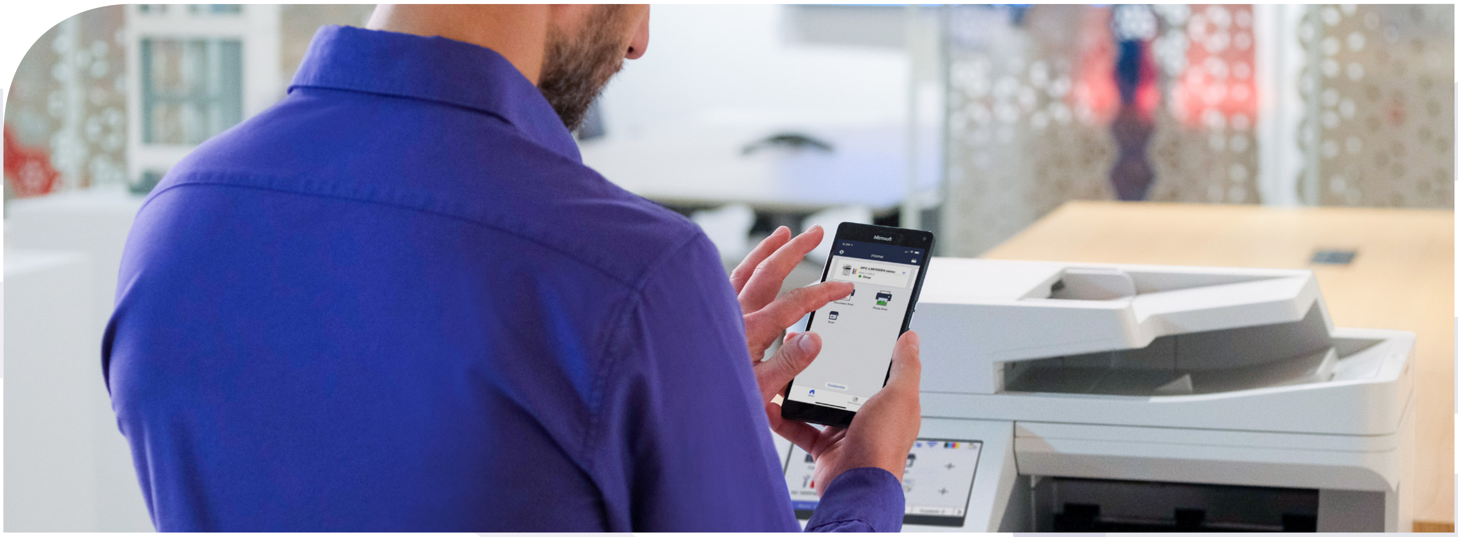
brother
at your side

Your Printing Isn't as Secure as You Think
(and what you can do about it)

Data is valuable, and therefore it's vulnerable. With high-profile breaches now increasingly common, the business world is generally aware of the importance of cybersecurity. And many, maybe even most, companies understand that because printers are part of the network, they are access points for hackers – and may be especially vulnerable in today's hybrid work environment.

Yet for too many companies, printing is not secure. Why not?



Lack of Accountability, Lack of Clarity

Because printing has not traditionally been recognized as a security weak point, responsibility often goes unassigned. This may be particularly true in organizations that are understaffed, where many employees are already tasked with multiple responsibilities. Moreover, the general awareness of print-related vulnerability seems not to have filtered down to specific practices and protocols.

Security threats often include:

- Printouts that are left unattended at the device
- Employees not logging out after printing confidential documents
- Lack of traceability for who has accessed documents

Finally, a common complaint among businesses is the way security-related information is itself communicated: the jargon may actually be adding to the confusion.

79% of companies say that print security is very important

Source: *IDC Infobrief I Defending Your Business Infrastructure with Print Security

7 Ways to Strengthen Print Security

1. Get the Board On Board

Print security is no longer just an IT issue. It must be strategically considered by both the Chief Information Officer and Chief Information Security Officer.

2. Conduct a Thorough Audit

Make sure that print infrastructure is included in regular security audits. This is particularly important for businesses with a mix of new and legacy devices.

3. Change Pre-Set Admin Passwords

Default admin passwords are weak points for print devices. The good news is that they can be changed quickly and easily to something more secure.

4. Make Sure Firmware is Up to Date

Potential security vulnerabilities can be significantly reduced by updating firmware and configuring print devices for automatic updates.

5. Protect Documents

End-to-end encryption of network traffic ensures secure transfer of print jobs to printers.

6. Monitor Devices

Devices generate a wealth of data, which can be used to identify security events and enable fast response. Monitoring software is available.

7. Train Employees

Many data loss incidents are caused unintentionally. Businesses must educate employees on the importance of protecting sensitive information.