SHARP

Be Original.

Simple printer security for small businesses

Index

Introduction

Peter Plested,
Director, Information
Systems at Sharp
Electronics Europe

Printers or multifunctional printers (MFPs) are a familiar fixture in most workplaces.

Used routinely every day, on the outside they may not appear to have changed much over the last ten or even twenty years. However, as IT administrators know, on the inside, MFPs have evolved to become sophisticated computer systems, connected to your business network and the Internet.

Even though nine out of ten office workers in Europe do not recognise printers or MFPs as a security risk, they are as much of a target for hackers as a laptop or a PC. They need to be protected through technology and safe user behaviour.

As a printer manufacturer, security is at the centre of our product development. We want to make sure that our products and services make people's working lives easier and more productive, while keeping data safe at the same time.

We wanted to find out people's attitudes towards printer security. Do those outside of our industry consider this a potential issue or risk?

We interviewed more than 5,500 office workers in small and medium sized businesses (SMBs) in Europe and found that almost half of people were unaware that hacking a printer was even possible.

Our research also highlighted a clear lack in formal training and advice when it comes to printer security. We aim to help fill this gap with technical advice and whitepapers available on our website, and with this guide, created with ethical hacker Jens Müller.

The guide presents a snapshot of office printing behaviour in Europe and offers some easy-to-follow security tips for those responsible for office technology in SMBs. We hope you find it useful and welcome your thoughts or experiences on the biggest hurdles you face in keeping your data secure.

Contact us @Sharp_Europe on Twitter and visit us at www.sharp.co.uk

Is your network secure?

Did you know that smaller companies are least likely to have printer security features in place?

62% of workers in companies with less than 49 employees say that anyone can use their printer or MFP. This figure drops to 43% for companies with 151-250 employees.

The risks of not controlling access to the printer range from malware being uploaded to the network via the printer, intentionally or unintentionally, to the leaking of confidential data left in print outs in the printer tray.

Research highlights

10%

Only 10% of office workers identified printers or MFPs as posing a security risk in their workplace.

21%

21% of office workers said they do not have any security processes in place for printers or MFPs in their workplace.

25%

25% of office workers said they have found confidential or personal information on the printer tray that was not intended for them, a data protection breach.

28%

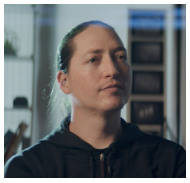
28% of office workers have used a work printer to print a personal document that they have created at home, outside of the business' security environment.

14%

14% have used their office printer to print a document they have downloaded despite a warning that the file may be insecure, exposing the business network to a potential threat.

Research was conducted for Sharp by Censuswide. 5,514 office workers in companies with 10-250 employees from seven European countries were surveyed , including the UK, Germany, France, Italy, Netherlands, Sweden and Poland.

An expert's view



Jens Müller
Ethical hacker

Jens Müller, ethical hacker, explores the implications of Sharp's research findings and the potential risks to SMB data security posed by printers and MFPs.

Sharp's research found that nine in ten European office workers do not perceive their printer or MFP to be a potential security risk to their organisation. After all, why would someone want to hack a company's printer or MFP? How profitable would it be to them?

Firstly, printers are everywhere. Every company has one, they're connected to the network and they can be easily targeted by hackers if they are not secure.

Secondly, printers and MFPs can contain valuable information, so there is a lot of motivation to hack into a printer. Companies should ask themselves how valuable the information is that they are printing and scanning. In an era when the General Data Protection Regulation (GDPR) puts the onus on companies to protect personally identifiable data that they hold on individuals, the printer or MFP could be an expensive weak spot.

Typically, there are two types of hacker – kids that want to have fun and test their hacking skills out of curiosity, and then there are the more sinister characters whose objective is corporate espionage. While we don't know how big the problem of security breaches via printers and MFPs is currently, we do know that there are tens of thousands of printers available for hackers to access, so the potential problem is huge.

It would be a mistake to think this is solely an issue for the enterprise, as SMBs are just as vulnerable, especially if their work is of interest to criminals who could benefit from stealing their data or disrupting their business, for example, if they are a supplier to a government organisation. And this is an issue because, as Sharp's research highlights, smaller companies have less ability and resources to tackle cybersecurity than enterprise organisations.

Therefore, educating staff is important. Just in the same way that SMBs train staff about important security threats like phishing, they also need to understand the security risks around printers and MFPs, and how to mitigate them. And yet we know that 40% of office workers in Europe have never received training or advice on how to print securely.

What are those risks? Not only can printers and MFPs provide access to sensitive printed, scanned and faxed documents, there is also the risk of printers being abused to escalate into a company's network or to perform distributed denial of service (DDoS) attacks. We saw this with the Mirai botnet in 2016, which compromised devices around the world – including printers – and performed the largest DDoS attack in history. Hackers will always look for the weakest link, which could be the printer.

If the printer or MFP has no password, then that's an issue. We also know that across Europe more than half (52%) of office workers say that no authentication is required to use any function of their printer or MFP. Older devices can be more susceptible as their security will not be up to date, in much the same way that old Windows devices are often the way in for viruses or cyberattacks. The vulnerabilities of outdated software were highlighted dramatically by the WannaCry outbreak in May 2017 and these same risks apply to printers too.

So how does an SMB protect itself from a printer or MFP vulnerability? Well, defence is harder than offence; hackers just need to find one way in, while the IT manager (or whoever takes responsibility for IT in a company) needs to think about every potential weakness. Security is a recurring cost to admin, which puts pressure on the SMB's bottom line and probably explains why it drops down the priority list. It's also difficult to prioritise investment in something which is working and doing its core job well (i.e. printing or scanning documents).

And it's not just about printing. The scanner can be a weak point too and scanned documents can easily be leaked by a hacker. SMBs should consider PDF document encryption and check their email scans sent from the MFP are secure.

There is of course a lot of focus on data but SMBs must never overlook the 'analogue' threat of information held on paper. Hackers have in the past found sensitive information in the rubbish. It can be easy to access the printer and any hard-copies that might have been left in the paper tray, as they are often situated in open areas of the office and shared across departments.

While the risk can feel overwhelming, it's easier than you might think to stay on top of printer security. There are simple ways to mitigate risks and most don't require any extra investment, apart from your time. Read my tips for IT administrators or those in charge of office technology.

Printer security tips

These tips relate to any printer or multi-functional printer that is connected to your company network. Some relate to settings that you can change yourself as an administrator, some may require you to get help from the company that supplied your printer or maintains it.

Change default passwords

Don't let hackers take control of your printer. Set a strong password for the administration control panel webpage immediately upon setting up your device. Printers are commonly deployed with a default password which is publicly available and therefore known by hackers. Hence, it is essential for IT administrators to actively set a password for each of the printers in your office.

User authentication

Make sure your MFP only accepts print jobs from authorised personnel. Set it up so that users must authenticate themselves before they can print any documents. User authentication can be enabled in the printer's administrative panel. Limiting access to whitelisted users should be central to your security strategy to exclude attackers and therefore prevent undesired printouts and more sophisticated attacks.

No bypassing

Make sure that no other possibility exists to print and therefore bypass access controls and perform unauthenticated printing. Do not guarantee visitors even temporary access to your devices, instead use guest segregation: if guests need to print, provide a separate device not connected to your organisation's network.

Disable unnecessary print services

Only run what you really need. Disable all other network and local print services to minimise the opportunities for attacks. Once you have figured out which protocols are really used in your setup, disable all other unrequired services. For example, if you print via IPP there is no need to keep the raw port 9100 printing service open. If you print via LAN only, there is no need for the printer to act as a WiFi/Airprint hotspot.

Network security

The Internet can be a dangerous place. Make sure your printers are not directly exposed to the public Internet to prevent unsolicited printouts and to limit the opportunities for more sophisticated attacks. While this sounds obvious, right now there are tens of thousands of printers directly accessible over publicly routed IP addresses. You can enhance your internal network security further, using IP or MAC address filtering.

Physical security

Unauthorised users can find gaining physical access to printers and MFPs easier than accessing servers or workstations and launching a malicious print job from a USB drive can take only a matter of seconds. As a countermeasure, control by authentication or disable all physical ports such as un unauthorised printing via USB (frontside), parallel or USB cable (backside), NFC and Bluetooth.

Do not locate printers in public places, make sure that printer maintenance is only undertaken by authorised staff, and train your employees to approach suspicious or unknown people.

Do not leave confidential documents on the printer tray. Enable Secure Print Release (also sometimes called “Pull Printing,” “Follow Me Secure Print” or “pick up protection”) based on PINs or ID cards to approve the document.

Firmware updates

Over the last decade printers have evolved from mechanical devices with microchips to full blown computer systems. Therefore, it is essential to treat them like other components in your IT system: Always make sure to keep up with the latest security patches and firmware updates.

The most recent version is the most stable and secure. It guarantees to be running the latest security features and protection mechanisms. Schedule a fixed, regular appointment to roll out firmware updates or do so when it is available from your authorised dealer.

Enable monitoring

What happens if you had a breach or detect suspicious activity within your organisation’s network? Log files may reveal information about what exactly happened, keeping digital evidence of intrusion attempts such as malicious print jobs (remember to enable user authentication).

IT administrators can enable email notifications to keep themselves aware of critical issues and security violations

Secure disposal

Don’t just trash it. Past security breaches occurred because hackers obtained discarded printers and got access to their hard disks or non-volatile memory (NVRAM). If the device had been integrated into the organisation’s network, it may hold sensitive data. On decommission, ensure any memory or HDD is cleared. If the device is to be returned to the company you bought it from, use the end-of-lease features to ensure that all confidential data is overwritten before the device leaves the facility.

Enable encryption

Your data is valuable. If not encrypted then every document that is printed on a network printer is transmitted in plaintext over the wire – allowing everyone “in the middle” to access print jobs. To enable in-transit encryption, IT administrators basically have two choices: Transport layer encryption (TLS/SSL), and IPSec, which will encrypt the whole network traffic.

If you need to send confidential files such as scanned documents over insecure channels, use S/MIME end-to-end email encryption based on certificates or use PDF encryption with a strong password. To guarantee secure storage of documents on the printer or MFP, enable the printer’s hard disk encryption feature.

Jargon buster

Authentication
Unique identification, typically through two pieces of information such as a username and password.

Ports
Ports are used by networked devices (PCs, servers, printers etc.) for communication with each other (e.g., a workstation connecting to a printer). Unguarded open ports and services can be used as an attacker vector, for example, to upload malware.

Protocols
A protocol is defined as a set of rules and formats, permitting information systems to exchange information. In a network context, for example, IP and TLS/SSL are protocols.

Transport Layer Security (TLS/SSL)
A type of technology that encrypts data when it is being transported or transferred between one device and another to prevent eavesdropping. TLS/SSL is common for websites but can also be used to protect other services.

Internet Printing Protocol (IPP)
A network printing protocol capable of authentication and print job queue management. IPP is supported and enabled by default on most modern printers and MFPs.

IP addresses
Every device connected to the internet must have a unique number (IP address) to connect with other devices. There are currently two versions of IP addressing: IPv4 and a later upgraded version called IPv6.

IPsec (Internet Protocol Security)
A suite of protocols for securing Internet Protocol (IP) communications at the network layer. IPsec also includes protocols for cryptographic key establishment.

S/MIME (Secure/Multipurpose Internet Mail Extensions)
A set of specifications for securing email. Secure/Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding security through digital signatures and encryption.

MAC addresses
A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC). This means that a network connected device can be uniquely identified by its MAC address.

IP or MAC address filtering
IP and MAC addresses are unique numbers used to identify devices on the Internet (IP) or on a local network (MAC). Filtering ensures that IP and MAC addresses are checked against a 'whitelist' before devices can connect to your network.

Network services
Network services facilitate a network's operation. They are typically provided by a server (which can be running one or more services), based on network protocols. Some examples are domain name system (DNS), dynamic host configuration protocol (DHCP), voice over internet protocol (VoIP).

Whitelist
A whitelist is an exclusive list of people, entities, applications or processes that are given special permissions or rights of access. In a business sense, this could be for example the staff of an organisation and their rights to access the building, the network and their computers. In a network or computer sense, a whitelist may define applications and processes that have the rights to access data storage in secure areas.

DoS/DDoS
A Denial of Service (DoS) is a type of disruptive attack where normal operation or service provided by a network or device is blocked or disrupted. A Distributed Denial of Service (DDoS) is a type of DoS attack using multiple (numerous) attacking systems to amplify the amount of network traffic, thereby flooding and perhaps swamping the target systems or networks.

Phishing attack
Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Spoofing attack
A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.

Man-in-the-middle attack
A man-in-the-middle attack (MITM) is where the attacker secretly sits between two parties who believe they are connected directly and privately communicating with each other. The attacker eavesdrops and may also alter the communication between the parties.

Malware attack
Malicious software (malware) can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet..

Sharp security features

Sharp provides a suite of integrated security features to help protect businesses' information and documents from a multitude of threats.

Sharp's latest ranges of A3 MFPs* and A4 MFPs** are its most secure to date. Sharp offers a unique 360-degree approach to security, giving SMBs the tools to control and manage their print policies and help them protect their confidential information whether it is being printed, copied, scanned, faxed, stored or shared over their network.

From Network Security, which covers all business networks and all connected peripherals, to Output Security to control and track access, through to Document Security, which protects both digital and physical documents, Sharp has a simple solution for you.

For more information about these topics, visit our White Paper library or the Information Security section on our website: https://www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security-new---mainpage.htm

- Network Security
- Output Security
- Document Security
- GDPR compliance

This comprehensive security approach ensures that your organisation also benefits from the highest level of compliance with the latest security regulations, including the General Data Protection Regulation (GDPR).

To discuss your security requirements in more detail, please contact us.

Sharp takes care of security so you can take care of your business.

* A3 models: MX-6071, MX-6051, MX-5071, MX-5051, MX-4071, MX-4061, MX-4051, MX-3571, MX-3561, MX-3551, MX-3071, MX-3061, MX-3051, MX-2651.
** A4 models: MX-C304W, mX-C303W

www.sharp.eu

SHARP

Be Original.