APRIL 2024

modernnetworks

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

It's Time to Fix Your RISKY Password Habits

We all know how important it is to keep our data safe, but sometimes our best intentions fall short. And when you have employees, you're at an increased risk of security threats and bad habits creeping in.

Here's the deal: Even if you invest in cyber security training, changing long held password habits can be a tough nut to crack. People love convenience, and remembering a ton of complex passwords just isn't their idea of a good time.

Your employees are juggling dozens of passwords for work and personal use. It's a lot to handle, and sometimes they slip up and reuse passwords across different accounts. It's a familiar story, right? And it's where the trouble starts.

When passwords are reused, it's like leaving the front door wide open for cyber criminals. If the password is breached on one site, they will try it to access other sites.

Here's how you can make sure your team stays on top of their password game.

Password audit: Ask your IT partner to do an audit of passwords and look for weak ones that should be changed.

Block weak passwords: Ask your IT partner to implement a password policy that stops common passwords from being used.

Scan for compromised passwords: Even strong passwords can be compromised. Stay one step ahead by scanning for breached passwords and prompting employees to change them.

Use password managers: Password managers securely generate then store a unique password for every different account… and fill them into the login box so your team don't have to.

Multi-Factor Authentication (MFA): Add an extra layer of security with MFA, where you get a code on a separate device. It's like putting a deadbolt on your front door – double the protection, double the peace of mind.

With the right tools and guidance, password security doesn't have to be hard work. If we can help you with that, get in touch.

IN THIS EDITION

HAVE YOUR SAY

Help us improve our communications by taking our short survey.

CLICK HERE

Why Your Office Printer Might Be A Stealthy Cybersecurity Threat

In the fast-moving world of cybersecurity, where our attention is often drawn to firewalls, antivirus software, and data encryption, there exists a hidden vulnerability that many overlook—the humble office printer. Despite its innocuous appearance, this seemingly mundane device can serve as a clandestine gateway for cyber mischief, harbouring more secrets than one might imagine. Let's delve into the intriguing realm of **managed print solutions (MPS)** and their pivotal role in safeguarding organisations against this overlooked threat.

The Unassuming Printer: A Hacker's Backdoor

Imagine a typical day at the office—you're printing out a routine report on the office printer. What could be more innocuous than the office printer? But behind the paper trays lies a vulnerability that hackers are all too eager to exploit. Printers, like any network-connected device, can possess vulnerabilities ranging from unpatched firmware to weak passwords and outdated security protocols. That makes them low-hanging fruit for cybercriminals seeking to access your confidential data.

The Silent Intruder

Consider this scenario: A hacker exploits a printer vulnerability to infiltrate your network, gaining access to sensitive documents, email addresses, and even login credentials. The printer, seemingly harmless as it sits in a corner, unwittingly becomes the gateway to your organisation's most sensitive data.

Print Jobs on the Loose

Have you ever sent a job to the office printer only to forget to retrieve it? Those forgotten pages could contain sensitive information that any unauthorised person might pick up and walk out the door with.

The Rogue Print Server

Print servers, responsible for managing print jobs across an organization, become potential points of vulnerability if intercepted by rogue actors. Your confidential data could be left exposed, awaiting exploitation.

Real-World Printer Shenanigans

- In March this year, Anycubic, a popular brand of 3D printers, suffered a worldwide hack. The hacker was able to exploit a critical security flaw in the devices, and added a file that warned users of the vulnerability that could allow attackers to take control of their printers. The hacker urged the users to disconnect their printers from the internet and also called upon Anycubic to open-source their 3D printers. **This message was downloaded by almost 3 million devices.**

- **A teenager from the UK managed to hack approximately 150,000 internet-connected printers across the world.** After gaining control of these devices, he began printing ASCII art and messages to notify their owners that their machines were now "part of a flaming botnet." The hacker signed off his work using the name "Stackoverflowin."

- **CyberNews conducted an experiment where they hijacked close to 28,000 unsecured printers worldwide** and forced them to print out a guide on printer security. This was done to raise awareness about printer security issues.

NEXT

Enter Managed Print Solutions (MPS)

Thankfully, managed print (MPS) emerges as a beacon of hope in this digital minefield, offering comprehensive solutions to mitigate the risks posed by office printers.

Security Patch Patrol

MPS providers like Modern Networks diligently monitor printer fleets, ensuring that security patches are promptly applied to mitigate vulnerabilities and enhance overall network security.

Secret Handshakes at the Printer

Secure print release systems require authentication before documents are printed, reducing the risk of accidental data leaks, and stopping a stranger from walking off with your company's crown jewels.

Office Printer Encryption Magic

MPS encrypt data as it travels between office printers and servers, rendering it indecipherable to unauthorised parties and thwarting potential hacking attempts.

Role-Based Access Control

By implementing role-based access control, only authorised personnel are granted access to certain printer functionalities, reducing the risk of unauthorised data access or manipulation.

In Conclusion

It's important to keep in mind that even the most ordinary devices, such as the humble office printer, can pose a major threat to your organisation's security if not properly protected. By using managed print solutions and implementing robust security measures, you can enhance your defences against potential cyberattacks. It's easy to forget, but your office printer is more than just a combination of plastic, ink, and paper; it can also serve as a digital backdoor to your company's network. Therefore, it is crucial to take the necessary steps to protect it at all costs.

DID YOU KNOW... Managed Print Can Save You Money

Do you want to learn more about the benefits of managed print such as reduced waste, lower energy consumption and lower costs?
Get in touch today.

NEW TO

MICROSOFT

Say hello to perfect photos with Windows

Microsoft is bringing the best feature from the Google Pixel phone to Windows 10 and 11. The AI-powered 'generative erase' tool removes imperfections and unwanted features. It can even replace them with AI-generated images, such as removing people from backgrounds or replacing the background entirely.

It promises a user-friendly, impressive editing experience that will improve your website images, presentations, and loads more.

Cyber-attacks: Stronger, Faster and More Sophisticated

A new security report has revealed some alarming trends.

First off, cyber-attacks are becoming faster than ever. Breakout times (that's the time it takes for a criminal to move within your network after first getting in) have dropped significantly. We're talking an average of just 62 minutes compared to 84 minutes last year.

This is not good news.

Not only are these attacks faster, but they're also becoming more common. The report has identified a whopping 34 new cybercriminal groups, bringing the total to over 230 groups tracked by the company.

And guess what? These cybercriminals aren't sitting around twiddling their thumbs. They're getting smarter and more sophisticated. The report highlights a new record breakout time of just two minutes and seven seconds. That's barely enough time to grab a coffee, let alone mount a defence.

But here's the real kicker: The human factor is increasingly becoming the main entry point for these cyber-attacks.

They will try to get your people to click a link in a phishing email, which will take them to a fake login page. Once your employee enters their real login details, they have inadvertently handed them over.

Or they pretend to be someone your team trusts. This is called social engineering.

So, what can you do to protect your business from these cyber threats?

- **Educate your employees**

Make sure your team is aware of the latest cyber threats and how to spot them. Regular training sessions can go a long way in preventing costly mistakes.

- **Implement strong password policies**

Encourage the use of complex random passwords generated and remembered by password managers. Use multi-factor authentication for an added layer of security (this is where you use a second device to confirm it's really you are logging in).

- **Keep your systems updated**

Make sure all software and systems are up to date with the latest security patches. Cybercriminals often exploit known vulnerabilities, so staying current is key.

- **Invest in cyber security software**

Consider investing in reputable cyber security software that can help detect and mitigate threats in real-time (we can help with this).

- **Back up your data**

Regularly back up your data and store it in a secure location. In the event of a cyber-attack, having backups can help minimise downtime and data loss.

When it comes to cyber security, it's better to be safe than sorry. If we can help you to stay better prepared, get in touch.

DID YOU KNOW... you can snooze your emails?

Our inboxes can be relentless. Sometimes an email pings through that you don't have time to deal with, but you don't want to forget about either.

Instead of marking it as unread and leaving it to get lost amongst the scores of junk, if you use Outlook you can snooze it instead. That means it pops back to the top of your inbox at a more convenient TIME.

Simply right click the email, click Snooze, and set a time. Done!

Q&A

Q: The sidebar and sidebar button in Microsoft Edge is annoying. Is there a way to hide it?

A: Yes. Just go to the cog icon at the bottom of the sidebar and turn off the "Show sidebar button" setting. But make sure that Edge is updated to version 122 to use this feature.

Q: How do I know if I'm spending too much on technology?

A: It's unreasonable to believe your hardware will last forever or that your business software won't need upgrading, but you don't need all the latest tech and gadgets. We can help you set a realistic budget, get in touch.

Q: How can I tell if my passwords have been leaked?

A: Sites like haveibeenpwned.com allow you to search across multiple data breaches to see if your email address has been compromised. Alternatively, we can help – get in touch.

modernnetworks

To get in touch with us:
Call 01462 426500
Email info@modern-networks.co.uk
Web www.modern-networks.co.uk