NEWSLETTER

RJ2 Technologies Monthly Newsletter
July 2025

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

(847) 303-1194

www.rj2t.com

In this newsletter:

The Hidden Costs Of Waiting: Why You Can't Afford to Delay Your Windows 10 Upgrade

If you're still running Windows 10 on your business machines, let's cut to the chase: The clock is ticking.

On October 14, 2025, Microsoft is officially ending support for Windows 10. That means *no more security patches, no more bug fixes and no more technical support.*

But here's what business owners really need to understand: The cost of waiting isn't just about someday needing to upgrade.

It's about what waiting could cost you in the meantime.

"We'll Deal With It Later" Is An Expensive Strategy

We get it – upgrading every machine in your business isn't exactly your idea of a fun budget item. It feels easy to delay…until something breaks.

But here's what procrastination actually costs:

1 You're Operating Without A Safety Net

Once Microsoft discontinues Windows 10 updates, every new vulnerability becomes your responsibility.

Hackers love outdated systems because they're easy targets. It's like locking the front door but leaving the windows wide open.

One breach could cost you thousands – or worse, your entire business.

2 Software and Hardware Compatibility Issues

Many business apps, such as accounting tools, CRMs and industry-specific platforms, are already phasing out support for Windows 10.

If your systems stop working mid-project or crash during a client demo, what's that worth?

And it's not just software. New printers, peripherals and even security tools may stop playing nicely with your outdated OS.

3 Lost Productivity

Outdated systems are slower, they crash more frequently and they frustrate your team. Even small lags add up over time, dragging down efficiency, morale and your ability to compete.

If every employee loses 10 to 15 minutes a day to tech hiccups, what does that cost you over a month?

4 Emergency Upgrades Are Always More Expensive

Waiting until your systems crash or your team is locked out doesn't just create stress – it creates panic-spend mode:

- Emergency hardware orders
- Rush IT labor fees
- Business interruptions while machines are replaced

A little planning now saves a lot of scrambling – and money – later.

5 You're Risking Compliance Violations

If your business handles sensitive data or is subject to regulations (HIPAA, PCI-DSS, etc.), using unsupported systems could result in fines or lawsuits. Many regulatory frameworks require up-to-date security – Windows 10 won't meet those standards come October.

What Smart Business Owners Are Doing Now

They're getting ahead of the deadline, not just by upgrading devices, but by using this transition to:

- Audit what devices need to go
- Streamline tools and software
- Tighten up cybersecurity protections
- Plan smarter for IT spend in 2025

How To Make The Transition Smooth

Here's what we recommend:

- Run a compatibility check – Not all machines can run Windows 11. Find out which ones need to be replaced.
- Audit your apps – Make sure your essential tools are ready to run on Windows 11 or newer environments.
- Budget for hardware now – Don't get stuck in a supply chain crunch later.
- Partner with an IT provider – We can handle the transition from start to finish – no downtime, no surprises.

Don't Wait Until October To Panic

Waiting until the last minute will cost you more – in money, stress and missed opportunity. We're helping small businesses make the upgrade the smart way: planned, smooth and optimized for future growth.

Book a FREE Network Assessment and we'll help you identify what needs upgrading, what can stay and how to build a transition plan that won't disrupt your business before the deadline. For more information about Windows 11, **call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com.**

Get Fresh IT News Weekly with RJ2 Technologies!

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532

Your Vacation Auto-Reply Might Be A Hacker's Favorite E-mail

You set it. You forget it. And just like that, while you're packing for vacation, your inbox starts broadcasting:

"Hi there! I'm out of the office until [date]. For urgent matters, contact [coworker's name and e-mail]."

Harmless, right?

Actually, cyber criminals love these auto-replies. That simple message gives them valuable intel: your name, title, when you're unavailable, who to contact, internal team structure, and sometimes even travel details.

This provides two major advantages:

Timing – They know you're unavailable and less likely to catch suspicious activity.

Targeting – They know who to impersonate and who to scam.

This sets the stage for a phishing or business e-mail compromise (BEC) attack.

How It Happens:

- Your auto-reply is sent.
- A hacker impersonates you or your alternate contact.
- They send an "urgent" request for money, passwords, or documents.
- A coworker, trusting the e-mail, complies.
- You return to discover fraud or a breach.

Businesses with traveling executives or sales teams are especially vulnerable. Admins often field many requests, handle sensitive tasks quickly, and may trust a well-crafted fake e-mail.

How To Protect Your Business:

1. Keep It Vague

Skip detailed itineraries. Instead, say:
"I'm currently out of the office and will respond when I return. For immediate assistance, contact our main office at [info]."

2. Train Your Team

Educate staff never to act on urgent, sensitive requests based solely on e-mail. Always verify through another channel like a phone call.

3. Use E-mail Security Tools

Advanced filters, anti-spoofing protections, and domain monitoring reduce impersonation risks.

4. Enable MFA Everywhere

Multi-factor authentication across all accounts blocks hackers even if passwords are compromised.

5. Partner With A Proactive IT Provider

An experienced cybersecurity team can detect suspicious activity early and stop attacks before they cause serious damage.

Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com for more information.

Is Your Printer The Biggest Security Threat In Your Office?

If I asked you to name the biggest cybersecurity threats in your office, you'd probably say phishing e-mails, malware or weak passwords. But what if I told you that your office printer – yes, the one quietly humming in the corner – could be one of the biggest vulnerabilities in your entire network?

It sounds ridiculous, but hackers love printers. And most businesses don't realize just how much of a security risk they pose – until it's too late. In 2020, Cybernews ran what they called the "Printer Hack Experiment." Out of a sample of 50,000 devices, they successfully compromised 56% of the printers, directing them to print out a sheet on printer security. That's nearly 28,000 compromised devices – all because businesses overlooked this "harmless" piece of office equipment.

Wait, WHY Target Printers?

Because printers are a goldmine of sensitive data. They process everything from payroll documents and contracts to confidential client information. And yet, most businesses leave them wide-open to attack.

Here's what can happen when a hacker gains access to your printer:

Printers store sensitive data – Every time you print, scan or copy a document, your printer keeps a digital copy. Many printers have built-in hard drives that store years' worth of documents, including payroll files, contracts and employee records. If a hacker gains access, they can steal or even reprint those files without your knowledge.

Default passwords are a hacker's dream – Most printers come with default admin logins like "admin/admin" or "123456." Many businesses never change them, making it ridiculously easy for cyber criminals to take control.

They're an open door to your network – Printers are connected to your WiFi and company network. If compromised, they can be used as an entry point to install malware or ransomware, or steal data from other devices.

Print jobs can be intercepted – If your print jobs aren't encrypted, hackers can intercept documents before they even reach the printer. That means confidential contracts, legal documents and even medical records could be exposed.

They can spy on your business – Many modern printers have built-in storage and even scan-to-e-mail features. If a hacker compromises your device, they can remotely access scanned documents, e-mails and stored files.

Outdated firmware leaves the door wide-open – Like any device, printers need security updates. But most businesses never update their printers' firmware, leaving them vulnerable to known exploitations.

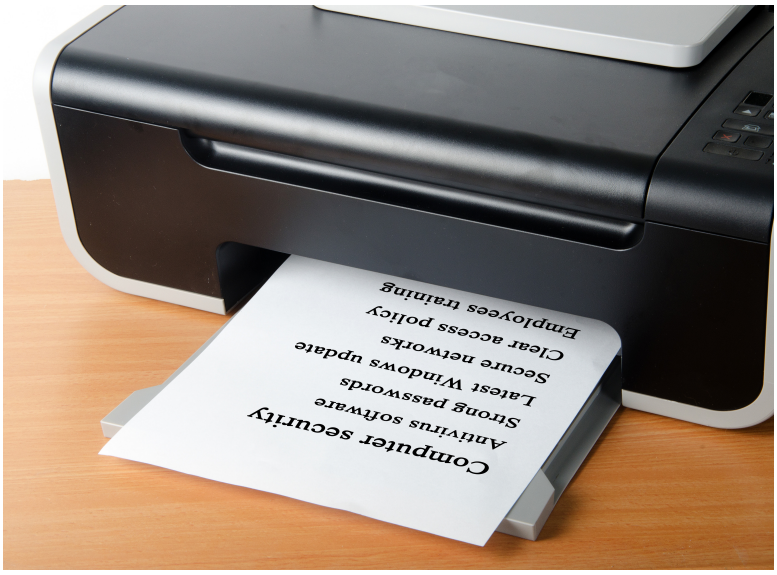
Data mining from discarded printers – Printers that were improperly disposed of can be a goldmine for cyber criminals. Residual data stored on discarded printers can be mined for sensitive information! This can result in potential security breaches. Printers need to have their storage wiped clean to avoid being vulnerable to data breaches and legal liabilities.

How To Protect Your Printers From Hackers

Now that you know printers can be hacked, here's what you need to do immediately:

1. Change The Default Password – If your printer still has the default login credentials, change them immediately. Use a strong, unique password like you would for your e-mail or bank account.

2. Update Your Printer's Firmware – Manufacturers release security patches for a reason. Log into your printer settings and check for updates or have your IT team do this for you.



3. Encrypt Print Jobs – Enable Secure Print and end-to-end encryption to prevent hackers from intercepting print jobs.

4. Restrict Who Can Print – Use access controls so only authorized employees can send print jobs. If your printer supports PIN codes, require them for sensitive print jobs. You can also add a guest option.

5. Regularly Clear Stored Data – Some printers let you manually delete stored print jobs. If yours has a hard drive, make sure it's encrypted, and if you replace a printer, wipe or destroy the hard drive before disposal.

6. Put Your Printer Behind A Firewall – Just like computers, printers should be protected by a firewall to prevent unauthorized access.

7. Monitor Printer Activity – If your IT team isn't already tracking printer logs, now is the time to start. Unusual print activity, remote access attempts or unauthorized users printing sensitive documents should be red flags.

Printers Aren't Just Office Equipment - They're Security Risks

Most businesses don't take printer security seriously because, well, it's a printer. But cyber criminals know that businesses overlook these devices, making them an easy target.

If you're protecting your computers but ignoring your printers, you're leaving a huge hole in your cybersecurity defenses. **Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com for more information.**

Vendor Partner Highlight - cisco Meraki

This month we are excited to highlight Cisco Meraki, a leader in cloud-managed IT solutions that are transforming the way organizations connect, secure, and scale their networks.

RJ2 Technologies is proud to be partnered with Cisco Meraki because of their security-first design and their real time analytics. From small businesses to global enterprises, Cisco Meraki continues to be a trusted partner in building resilient, future-ready networks.

To learn more about this partnership please call RJ2 Technologies at (847)-303-1194 or email marketing@rj2t.com