NEWSLETTER

RJ2 Technologies Monthly Newsletter
October 2025

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

(847) 303-1194

www.rj2t.com

In this newsletter:

Worried About AI Threats? Here's What's Actually Worth Worrying About

AI is rapidly advancing – and bringing with it a whole new way to do business. While it's exciting to see, it can also be alarming when you consider that attackers have just as much access to AI tools as you do. Here are a few monsters lurking in the dark that we want to shine the light on.

Dopplegängers In Your Video Chats - Watch Out For Deepfakes

AI-generated deepfakes have become scarily accurate, and threat actors are using that to their advantage in social engineering attacks against businesses.

For example, there was a recent incident observed by a security vendor where an employee of a cryptocurrency foundation joined a Zoom meeting with several deepfakes of known senior leadership within their company. The deepfakes told the employee to download a Zoom extension to access the Zoom microphone, paving the way for a North Korean intrusion.

For businesses, these types of scams are turning existing verification processes upside down. To identify them, look for red flags such as facial inconsistencies, long silences or strange lighting.

Creepy Crawlies In Your Inbox – Stay Wary Of Phishing E-mails

Phishing e-mails have been a problem for years, but now that attackers can use AI to write e-mails for them, most of the obvious tells of a suspicious e-mail, like bad grammar or spelling errors, aren't a good way to spot them anymore.

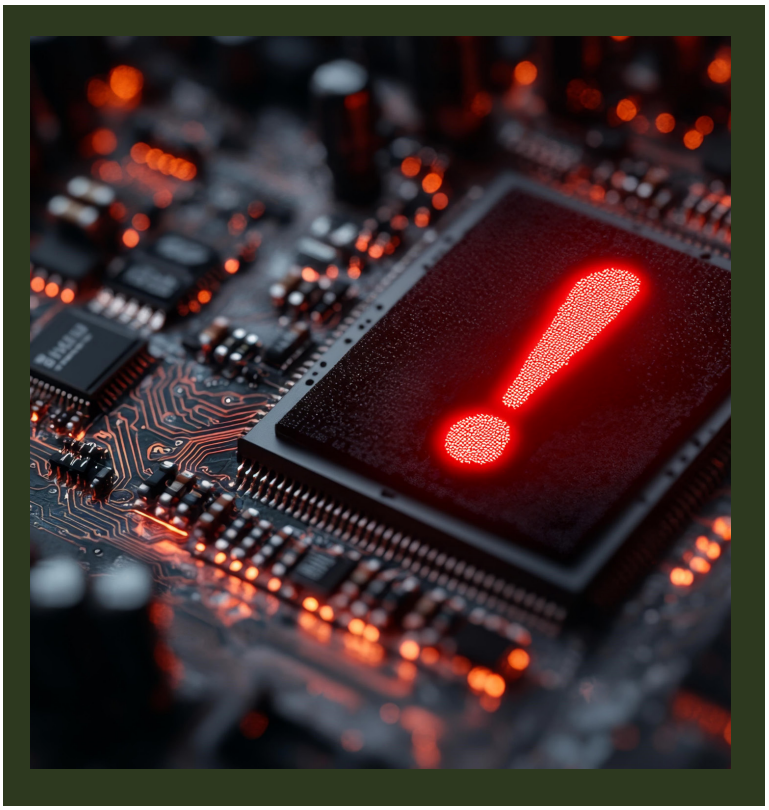
Threat actors are also integrating AI tools into their phishing kits as a way to take landing pages or e-mails and translate them into other languages. This can help threat actors scale their phishing campaigns.

However, many of the same security measures still apply to AI-generated phishing content. Extra defenses like multifactor authentication (MFA) make it much harder for attackers to get through, since they're unlikely to also have access to an external device like your cell phone.

Security awareness training is still extremely useful for reducing employee risk, teaching them other red-flag indicators to look for, such as messages expressing urgency.

Skeleton AI Tools – More Malicious Software Than Substance

Attackers are riding on the popularity of AI as a way to trick people into downloading malware. We frequently see threat actors tailoring their lures and customizing their attacks to take advantage of popular current events or even seasonal fads like Black Friday.



So, attackers using things like malicious "AI video generator" websites or fake malware-laden AI tools doesn't come as a surprise. In this case, fake AI "tools" are built with just enough legitimate software to make them look legitimate to the unsuspecting user – but underneath the surface, they're chock-full of malware.

For instance, a TikTok account was reportedly posting videos of ways to install "cracked software" to bypass licensing or activation requirements for apps like ChatGPT through a PowerShell command. But, in reality, the account was operating a malware distribution campaign, which was later exposed by researchers.

Security awareness training is key for businesses here too. A reliable way to protect your business is to ask your MSP to vet any new AI tools you're interested in before you download them.

Ready To Chase The AI Ghosts Out Of Your Business?

AI threats don't have to keep you up at night. From deepfakes to phishing to malicious "AI tools," attackers are getting smarter, but the right defenses will keep your business one step ahead.

Protect your team from the scary side of AI... before it becomes a real problem. **Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com to learn more.**

4 Habits Every Workplace Needs

Most cyberattacks don't happen because of some elite hacker. They happen because of sloppy everyday habits – like an employee clicking a bad link, skipping an update or reusing a password that's already been stolen in another breach.

The good news? Small changes in your daily routines can add up to big protection.

Here are four cybersecurity habits every workplace needs to adopt:

1. Communication

Cybersecurity should be part of the conversation, not just something IT worries about. Talk with your team regularly about the risks they might face and how to avoid them.
For example:

• A short reminder in a staff meeting about how to spot a phishing e-mail.
• Sharing news of a recent scam in your industry so people are on alert.
When security becomes a normal part of the discussion, it feels less like "extra work" and more like second nature.

2. Compliance

Every business has rules to follow, whether it's HIPAA for health care, PCI for credit card payments or simply protecting sensitive customer information. Compliance isn't just about avoiding fines, it's about protecting trust.

Even if you're not in a highly regulated industry, your customers still expect you to safeguard their data. Falling short can damage your reputation just as much as it can hurt your bottom line.
Make sure to:

• Review your policies regularly to ensure they match current regulations.
• Keep records of training and system updates.
• Make compliance a shared responsibility, not just an IT checkbox.

3. Continuity

If your systems go down tomorrow, how quickly can your business get back up and running? Continuity is all about being prepared.
Always:

• Make sure backups are running automatically and tested regularly.
• Have a plan in place for what to do if ransomware locks up your files.
• Practice your recovery steps before you need them.

Even a simple test, like restoring one critical file from backup, can prove whether your plan really works.

4. Culture

At the end of the day, your people are your first line of defense. Building a culture of security means making good cyber habits part of everyday work.
Some ways to make that happen are:

• Encourage strong, unique passwords (or, even better, password managers).
• Require MFA (multifactor authentication) on all accounts that support it.
• Recognize employees who catch phishing attempts.
This reinforces good habits and makes security a team win.

When security feels like a team effort, everyone gets better at it.

Security Is Everyone's Job

Keeping your business safe isn't just about software or hardware – it's about people. By building strong habits around communication, compliance, continuity and culture, you're not just avoiding threats, you're creating a workplace that takes security seriously every day.

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

Vendor Partner Highlight - Axcient

This month we are excited to highlight Axcient, a platform that provides managed service providers (MSPs) with business continuity and disaster recovery (BCDR) solutions. By utilizing Axcient's solutions, MSPs are able to protect their client data and ensure productivity while generating growth and profitability.

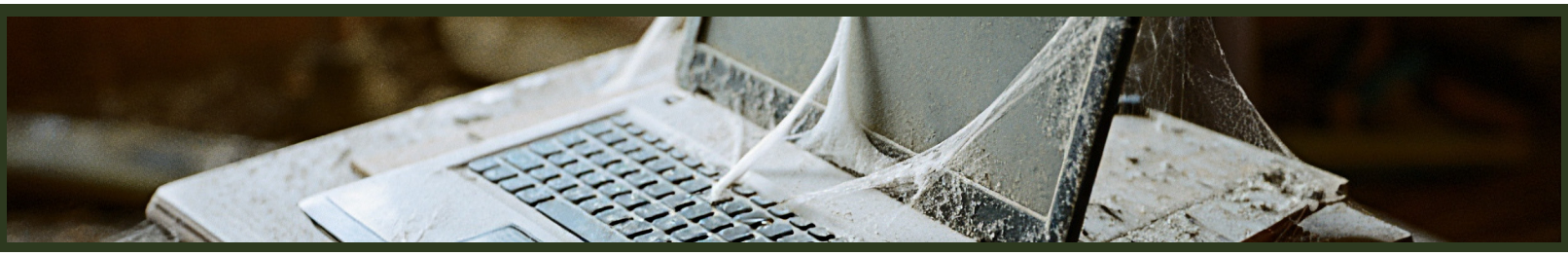
RJ2 Technologies utilizes x360Cloud and Office 365 Backup, effective solutions that automatically backs up data so that it can always be located, restored, and audited for uninterrupted business continuity after a data loss incident. Data is backed up to the encrypted, tamper-proof Axcient Cloud so clients can sleep soundly knowing the data is always available for recovery. **To learn more about this partnership please call RJ2 Technologies at (847)-303-1194 or email marketing@rj2t.com.**

The Hidden Cost of Neglected IT Maintenance—and How to Avoid It

While cybersecurity and innovation often steal the spotlight, routine IT maintenance quietly plays a critical role in business continuity. Neglecting it can lead to performance issues, security gaps, and unexpected downtime—all of which cost time and money.

Why Maintenance Matters More Than You Think

IT systems are like vehicles: they need regular checkups to run smoothly. When updates, patches, and hardware checks are skipped, small issues can snowball into major disruptions. For example, outdated firmware might expose a network to vulnerabilities, or a neglected server could fail during peak business hours.



Common Areas That Get Overlooked

Software Updates & Patch Management
Delaying updates can leave systems exposed to known threats. Automating patch management ensures critical fixes are applied promptly without disrupting workflows.

Hardware Health Checks
Aging hardware can slow down operations or fail unexpectedly. Regular diagnostics help identify components nearing end-of-life before they cause problems.

Backup & Recovery Testing
Backups are only useful if they work when needed. Routine testing ensures data can be restored quickly and accurately in case of an incident.

License & Subscription Reviews
Unused or expired licenses can lead to compliance issues or unnecessary costs. Periodic reviews help optimize spending and ensure proper coverage.

What This Means for Your Business

Neglecting IT maintenance may seem harmless in the short term, but it can quietly erode performance, security, and profitability. By prioritizing routine upkeep, businesses can avoid costly surprises and maintain a stable, secure environment. Whether you're managing a small office or a growing enterprise, proactive maintenance is a smart investment—and one that MSPs are uniquely positioned to support with efficiency and expertise.

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

Recycle Your Assets and Plant a Tree

This November, we are excited to highlight one of our solutions to address both concerns of innovation and care. We are highlighting our electronic hardware recycling program, designed to help organizations responsibly decommission outdated hardware while contributing to a greener planet.

As technology evolves, companies often face the challenge of safely disposing of old servers, laptops, desktops, and other electronic devices that can hold sensitive data. Improper disposal not only harms the environment but also poses serious risks to data security. RJ2 Technologies' new recycling solution offers a secure, affordable, and environmentally responsible way to manage this process.

One of the key features of this program is our certification of destruction for hard drives. We understand that many of these devices contain sensitive company data, and ensuring that information is permanently destroyed is critical. We are to committed our process to securely wipe data and destroy physical drives, giving you peace of mind and helping you meet compliance standards.

But our commitment doesn't stop at secure disposal. We're also focused on making a positive environmental impact. For every device recycled through our program, RJ2 Technologies will plant a tree in partnership with reforestation initiatives. This means that your company's decision to recycle not only helps clear out old hardware - it also contributes directly to restoring forests and improving the health of our planet.

This initiative reflects our broader mission to support sustainable business practices. By choosing RJ2 Technologies for your hardware decommissioning needs, you're joining a movement towards eco-conscious IT management. Whether you're upgrading your infrastructure, downsizing, or simply clearing out unused equipment, our solution makes it easy to do so responsibly.

We've designed this program to be cost-effective and hassle-free, ensuring that companies of all sizes can participate. With our streamlined process, we will deliver real value - both for your business and for the planet.

At RJ2 Technologies, we believe that technology and sustainability can go hand in hand. This recycling solution is just one of the ways we're helping our clients modernize their operations while reducing their environmental footprint. We're proud to offer a service that not only protects your data but also supports global reforestation efforts. We invite you to be part of this exciting initiative. Let's work together to build a future where innovation and conservation go hand in hand.

If you are interested in recycling your IT assets and want to learn more about this solution, please 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