WIRED for the FUTURE

DECEMBER 2024

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

The number one threat to your business? **Ransomware**

Imagine this: You're starting a normal day, coffee in hand, ready to tackle your to-do list. Suddenly, a red screen flashes on your computer, and a message pops up: "Your files have been encrypted. Pay up to get them back."

That's ransomware, a cyber attack that's fast becoming the number one threat to businesses worldwide. It's become a top choice for cyber criminals because it's profitable, easy to deploy, and very effective.

Cyber criminals get their ransomware software onto a computer, often from something as simple as a link in a phishing email (that's an email pretending to be from a trusted source). When clicked, it installs software that gives them access.

They lock your files, making them unreadable. The cyber criminals demand payment, usually in cryptocurrency, and promise to return access once they're paid. Some even threaten to leak sensitive info if you don't comply.

It's scary and the consequences for any business are huge. It's not just the loss of data, it's expensive, time consuming, and could break the trust you enjoy with your customers and suppliers.

So, how do you keep your business safe?

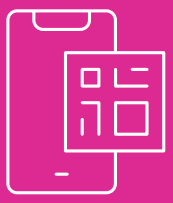
The good news is that basic security practices can go a long way. Start by training your team not to click on suspicious links or open unexpected attachments. Regularly updating applications and security software is also crucial, as it closes security gaps cyber criminals might try to exploit.

Most importantly, create a reliable backup system. Set up isolated, "cold" backups that are disconnected from your main system. So, if an attack hits, your data remains untouched. Regularly test these backups to make sure they work when you need them. In a ransomware attack, being able to restore your data from a safe backup can save your business from costly downtime or ransom demands.

Ransomware is serious, but a proactive approach can make all the difference. With the right prep, you can keep your business running smoothly. **If you'd like help with that, get in touch.**

DID YOU KNOW...

Now PDFs are being hijacked



Cyber criminals have another new trick: Hiding malicious QR codes in PDF attachments.

Instead of putting them directly in emails, scammers slip these codes into PDF files to bypass email security filters and lure people into scanning them on their phones (which often have weaker security).

They'll pose as big brands and send "urgent" emails about invoices, deliveries, or payments to push people into opening the file and scanning the code.

Be cautious and don't scan QR codes unless you're certain they're genuine.

Need new hardware? **Here's where to start...**

When your team's computers or internet start lagging, it's often a sign your hardware needs an upgrade. But with so many tech options, you may want some help knowing where to start. Allow us...

First, think about what your team needs. Office-based teams might need powerful desktops, while mobile workers may benefit from lightweight laptops. Make sure the hardware can handle your daily tasks comfortably – more complex tasks like graphic design will need more powerful machines. Ergonomics matter too, so consider comfortable screens, keyboards, and portable designs if they're on the go.

Next, look beyond computers to your network setup, like routers and switches. Even the best devices won't work well if your network equipment is outdated. Investing in quality network gear, like routers with strong Wi-Fi coverage and built-in security, keeps everything connected smoothly.

To stay future-ready, pick hardware that can grow with you. For example, choose computers with upgradeable storage or memory and network equipment that can handle more devices. Cloud solutions can also be a flexible option, letting you expand storage or services as you need them.

Finally, focus on durability and security. Good hardware should last and protect your business.

When you're making big decisions like this, it's a good idea to consult with experts – like us – who can guide you on cost-effective options and can make sure your technology will meet today's needs and tomorrow's growth.

If we can help you with that, get in touch.

Q: Should I embrace AI like Copilot?

A: Technology is advancing and it's important to keep up, but if you're unsure, take some expert advice and guidance before you start.

Q: How do we switch to passkeys?

A: These are replacements for passwords. You'll need to change your security settings within individual apps, but a little time now is certainly worthwhile for better security. If we can help, get in touch.

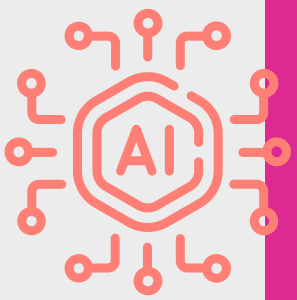
Q: How can I make sure employees aren't fooled by phishing emails?

A: Invest in regular cyber security awareness training for everyone. This can be interactive and doesn't have to be classroom-style (or boring!).

MICROSOFT

You can create a custom AI with Microsoft... soon

Microsoft is introducing a way for businesses to create custom AI agents in Copilot Studio, which can automate tasks and save time. Unlike basic AI tools that respond to direct commands, these AI agents can be set up to act automatically – doing things like checking customer details or inventory when an email arrives.



Microsoft is rolling out ten ready-made agents in Dynamics 365, which can be customized for tasks like sales and case management. These agents are designed to be easy to set up without coding, making automation accessible for all businesses.

Right now, this tool is only available in a public beta, but we expect to see a rollout soon.

This is how you can get in touch with us:

CALL: 416.572.3805 | **EMAIL:** info@wiredforthefuture.com
WEBSITE: wiredforthefuture.com

WIRED for the FUTURE