WIRED for the FUTURE TECHNOLOGY INSIDER

JUNE 2024

Your monthly newsletter, written for humans not geeks

Out of sight, out of mind?

Having your employees work from home or their local coffee shop is the norm now. And while there are loads of benefits to this new attitude to work, it's easy to overlook a crucial aspect of keeping operations secure: The home set-ups of remote employees.

Here's the thing – neglecting remote security can lead to some serious headaches down the line. And you already have enough business headaches, right?

Imagine this: Your employee's laptop, which holds loads of sensitive company data, gets breached because their home Wi-Fi network wasn't properly secured.

Or worse, a malware infection spreads from their kid's device to their work laptop, putting your entire network at risk. That's scary.

A little vigilance and some regular checks can prevent these risks and keep your business and its data much safer.

So, let's talk about devices. Encourage your remote workers to treat their work devices like Fort Knox. That means regular updates and patches, robust protective software, and strong, unique passwords (password managers are your best friend for this). Remind them to avoid risky behaviors like downloading software from unofficial sources or clicking on suspicious links.

Next, address home networks. A weak Wi-Fi password is asking for trouble. Encourage your employees to set a strong password for their home network (again, a password manager can remove the hassle of this). And while they're at it, remind them to enable encryption and hide their network's SSID (Service Set Identifier) to add an extra layer of security.

And it's not just about devices and networks – physical security matters too. Use biometrics to protect logins. Remind your team to keep their work devices secure when they're not in use, whether that means locking them away in a drawer or simply keeping them out of sight from prying eyes. And if they're working from a shared space like a coffee shop, remind them to be cautious of public Wi-Fi and to keep an eye on their belongings.

Regular checks are key to staying on top of security. Schedule routine audits of remote set-ups to ensure everything gets a thumbs up. This could include checking for software updates, reviewing network configurations, and providing refresher training on best security practices.

Want a hand with that?
We can help – get in touch.

DID YOU KNOW...

Microsoft has a new email send limit?

Microsoft Exchange is cracking down on spam. Hooray! But if your business sends bulk emails, it might affect you.

From January next year, Microsoft will allow **no more than 2,000 external recipients of bulk emails.** It's to prevent people abusing the service, which wasn't designed for bulk mailing.

TechFacts

1. The internet weighs as much as a strawberry. That's according to physicist Russell Seitz. He says the combined weight of all the electrons in motion is about 50 grams.

2. The first computer bug was a real bug. In 1947, Grace Hopper and her team found a moth causing issues in their computer at Harvard University.

3. One Petabyte (PB) = 1,024 Terabytes = 1 million Gigabytes. To put this in perspective, a 50PB drive could hold the entire written works of mankind from the beginning of recorded history... in all languages

INSPIRATIONAL QUOTE OF THE MONTH

"You build your own strategy. You don't define it by what another competitor is doing."

Ginni Rometty, former CEO of IBM

Technology update

Install any website or web tool as an app in Windows 11

In Windows 11, you can install ANY website or web tool as a traditional app. They're known as Progressive Web Apps (or PWAs) and once installed, they'll appear on your Start menu like a normal app would. You can even pin apps to the Taskbar.

Why bother? PWAs use less resources than traditional apps, and you'll always get the latest version without having to run an update first.

All you do is visit the site, click on Settings, select Apps, and click "Install this site as an app." Easy.

June's fun tech quiz – June-o the answers to these?

1. The keyboard shortcut for copying information is Ctrl + C, but what's the shortcut to paste?
2. In 1999 Shigetaka Kurita invented what keyboard additions for phones that would get their own movie?
3. When a password is limited strictly to numbers, it's referred to as a PIN. What does that stand for?
4. What word is often abbreviated as Fn on a keyboard?
5. Which American tech company started with its founders' idea to rent out an air mattress in their San Francisco living room to travelers hoping to avoid the city's high cost of rent?

The answers are below.

1. Ctrl + V
2. Emojis
3. Personal Identification Number
4. Function
5. Airbnb

NEW TO

MICROSOFT

Microsoft Teams is becoming more inclusive

If you like to inject a little personality into your Teams chats, it's likely you use reactions from time to time. But until now, they've been a little restrictive.

This month, a small tweak is due to rollout which will allow people to select a skin tone for their reactions. Microsoft says, "This preference will be applied to all emojis and reactions in chats, channels, and desktop/web meetings, allowing users to express themselves more authentically in conversations."

Think about recovery BEFORE the attack strikes

Let us set the scene. It's an ordinary Wednesday. You're minding your own business, getting things done, and making boss decisions, then BAM... you get hit with a cyber attack.

Cue panic mode.

But here's the thing: These attacks happen more often than you'd think. And guess who the favorite targets are? No, not big multinational companies – SMBs like yours.

And the consequences? We're talking financial losses, data loss, reputation damage, the whole nine yards.

But it doesn't have to be that way. If you have a recovery plan in place you can turn a total nightmare into just "an annoying inconvenience".

So, what should your recovery plan include? Well, first things first, prevention is key. Invest in solid cyber security measures like firewalls, antivirus software, and regular security checkups. And don't forget to educate your team about the importance of good cyber hygiene (things like using strong passwords and not clicking suspicious links) – because human error is often the weakest link.

Next, have a game plan for when the inevitable happens. This means having clear protocols in place for how to respond to an attack, who to call, and what steps will minimize the damage.

Let's talk backups. Regularly backing up your data to a secure location can be a real lifesaver in the event of an attack. That way, even if your systems go kaput, you'll still have a copy of your important files to fall back on.

Finally, practice makes perfect! Regularly test your recovery plan to make sure it's up to the job. After all, you don't want to wait until disaster strikes to realize your plan has more holes than a block of Swiss cheese.

Cyber attacks may be scary, but with a solid recovery plan in place, you can rest easy knowing your business is armed and ready. Remember what they say: Fail to prepare, prepare to fail.

If we can help you create your recovery plan, get in touch.

Read this before it's too late

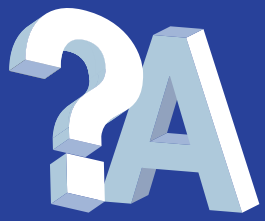
The worst time to decide how to deal with a cyber attack is when you're right in the middle of one.

Unfortunately, it's something you'll probably need to deal with eventually – SMBs are a prime target for cyber criminals.

It's a good idea to make a plan now, so that if the worst happens, you and your team are prepared to minimize the damage caused, the money spent, and the downtime suffered.

Our latest guide highlights 5 steps to stop a cyber attack causing the downfall of your business.

Download your free copy right now.



Q: Should I move my business data to the cloud?

A: The cloud brings many benefits such as zero storage limits and automatic backup. But it's important to choose the right provider. We can help – get in touch.

Q: How often should my team have cyber security training?

A: Since threats evolve at a rapid pace, regular training is important. Try to incorporate different methods each month, including simulation training.

Q: Can we use Microsoft Teams as a phone system?

A: Yes. And if you're already using Teams effectively, it could be a sensible solution. Get in touch and we can help you.

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