WIRED for the FUTURE TECHNOLOGY INSIDER

SEPTEMBER/OCTOBER 2021

Your bi-monthly newsletter, written for humans not geeks

Software updates: Your business' secret data security weapon

You know that feeling when you look in your phone's app store, and there are 29 apps asking to be updated? Yes, everyone gets annoyed with this sometimes.

What's worse is when you're working on your work computer, and software pings up a message saying it needs to be updated. At least phone apps don't take long and don't interrupt you that much. On your computer it's too easy to hit "remind me later" and forget it.

Often these updates are known as patches and they're there to keep your business safe.

When a vulnerability is found in a piece of software or an operating system, the developers work really fast to create a small update – the patch – that fixes the vulnerability. This is like a Band-Aid, until a full update is created.

It's risky to ignore any updates. A recent study found that today's top 4 most exploited vulnerabilities were discovered between 2018 and 2020.

The fact that they're still in the top 4 shows that many businesses are skipping updates!

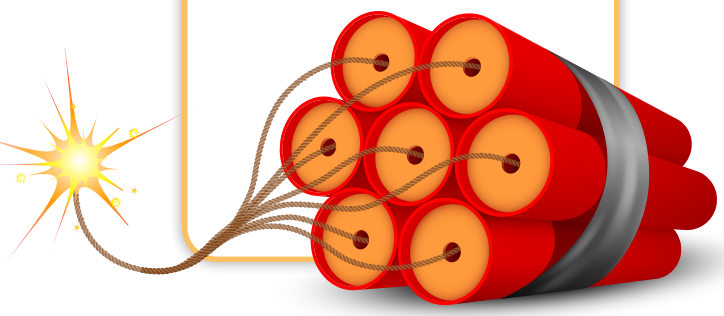
The answer is simple: Get your IT partner to make sure all your software is always up-to-date. This can be done remotely and easily with minimal disruption to you and your team.

DID YOU KNOW?

Did you know... about dynamite phishing?

Dynamite phishing is where "adult content" is emailed to you. The criminals behind it are hoping you'll click a link and give them access to your computer (that's what phishing is).

It's often aimed at male names, and there's been a **974% spike in it recently.** Use security software and staff training to stay protected.



Technology update

With more of us working remotely now, coffee shops are getting busier again as we look for somewhere other than home to work.

But while it can be great for getting rid of distractions, it's not so good for security.

That's because public Wi-Fi is a hotspot for data theft. Any data sent over public Wi-Fi that doesn't need a password to access is vulnerable to theft or manipulation from someone else using that network.

And it's not just other Wi-Fi traffic you need to consider. There are also fake networks to be wary of. You think you're connecting to the coffee shop's Wi-Fi... but how do you know it isn't a fake version with the same name?

As soon as you log on, they can suck up all of your credentials and any other personal data on your device.

If your team is using public Wi-Fi regularly, best practice is to use a VPN (Virtual Private Network) to keep your data safe. This acts as a private tunnel for your device to connect to a private network, keeping your info safe.

WIRED for the FUTURE
we make IT happen

Tech Fact#1

The name Google was accidental. It was a spelling error by the original founders who thought they were going with Googol

Tech Fact#2

Samsung is 38 years and 1 month older than Apple

Tech Fact#3

51% of internet traffic is non-human. 31% of that is spammers, and malicious phishing

FUN TECH QUIZ

Test your team at your next Zoom quiz

The loser buys the virtual beers…

1. What is OS an abbreviation for?
2. What kind of file does the .tmp extension usually refer to?
3. What was the first computer with a color display?
4. What was the name of the first computer programmer?
5. What is a computer's main circuit board called?

The answers are below.

1) Operating System
2) It's a temporary file
3) Apple 1
4) Ada Lovelace
5) Motherboard

MICROSOFT 365 TIP

Teams has been the breakout star of the last few years. Here are some Windows keyboard shortcuts for your next Teams meeting:

- Go to Search: Ctrl + E
- Turn your camera off: Ctrl+Shift+O
- Mute yourself: Ctrl+Shift+M
- Background blur: Ctrl+Shift+P
- Zoom: Ctrl+= to zoom in and Ctrl+- to zoom out
- Go to your files: Ctrl+6

INSPIRATIONAL QUOTE OF THE MONTH

"It's fine to celebrate success but it is more important to heed the lessons of failure."
Bill Gates

We're really looking forward to the launch of Windows 11 in the next few months. But are your devices ready for it?

Microsoft has changed the minimum system requirements needed to run its operating system if you're upgrading from 10 to 11 and that's created a headache for a lot of people.

On the plus side, the changes mean you'll get increased security, reliability, and compatibility. But it does mean that some of your devices might not be up to spec to upgrade.

Here are the minimum hardware requirements the new OS requires:

- An Intel Core processor from 2017 onwards.
  Or AMD Zen processors from 2019 onwards
- 4GB of RAM
- 64GB of hard drive storage
- Oh, and it all hinges on having a TPM (Trusted Platform Model) 2.0 chip

While Windows has required all its devices since 2016 to have the TPM chip, many of them haven't been activated. And that process is... technical, to say the least.

If that's all nonsense to you, contact us and we can check your devices for you. Just give us a call or drop us an email.

BEFORE LONG YOU WILL BE TARGETED BY RANSOMWARE

Here's a scary thought: As the fastest growing cyber-crime, ransomware is big business. And it's businesses like yours that are prime target.

Ransomware is where your data is encrypted until you pay a ransom fee. It's terrifying to see, and very hard to undo once an attack has launched.

Criminals are targeting small and medium sized businesses because many don't take cyber security seriously enough.

It only takes one click on one bad link to let a criminal into your system. Once in, they will spend weeks hidden in the background, secretly preparing an attack.

Their primary goal is to stop your IT partner from kicking them out once the attack has started.

Here's the answer: You need a blend of appropriate security software and staff training to protect your business.

You WILL be targeted at some point; this is a reality for all businesses in 2021. Whether or not your business succumbs to that attack depends on how prepared you are.

Do you know how resilient your business would be if it were hit with ransomware? We can tell you.

Let's jump on a 15 minute video call. You can talk to our chief security expert at Wired for the Future, who will ask you a short number of questions about your business and its IT.

No tech talk, we promise. Just a good productive conversation about protecting your business.

Visit
www.wiredforthefuture.com/cyber

Let's talk on a video call

Three questions for you:

1. Do you currently have an IT support company?
2. How happy are you with them?
3. 3. If the answer isn't "I'm so delighted, I daydream about them and write them little love notes", let's jump on a video call

The events of the last few years have taught businesses just how important it is to get proactive, responsive IT support.

We're now taking on new clients again.

Set up a 15 minute exploratory video call at www.wiredforthefuture.com/contact

Q A

QUESTION
Can I take a screenshot in Windows 10?

ANSWER
Yes! The easiest way to capture and save a copy of your entire screen is to hit the Windows key + Print Screen key. Your picture will be saved to the Pictures > Screenshots folder.

QUESTION
How can I see how much storage space my apps are taking up?

ANSWER
Sometimes if your computer is running slowly, it's a good idea to remove some apps you no longer use. To see how much storage space they're taking up, go to Settings > System > Storage. Then look at the drive you want to search (This PC, for example) and click Apps & Games.

QUESTION
Can I get rid of the ads on my Start menu?

ANSWER
Yep!
Go to Settings > Personalization > Start. Then turn off the *Occasionally show suggestions in Start* toggle switch

WIRED for the FUTURE

This is how you can get in touch with us:

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