OCTOBER 2021

WHERE TO START
TECHNOLOGY SOLUTIONS

CELEBRATING 20 YEARS 2001-2021 IN BUSINESS Anniversary

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans, not geeks

Software Updates: Your business's secret data security weapon

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

What's worse is that when you're working on your computer, the software pops up a message saying it needs to be updated. At least the phone apps don't take long and typically do not interrupt you that much. But, unfortunately, it's too easy to hit "remind me later" on your computer and forget about it until it is too late.

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 the operating system, the developers work fast to create a minor update - a.k.a. a patch that should address the vulnerability. However, this is like a Band-Aid until the full update is released and applied.

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

The fact that they're still in the top 4 proves that many businesses are skipping updates, and the bad guys know this is the case.

The answer is quite simple: Have your IT partner ensure ALL your software is always kept up-to-date. This is typically done remotely, in the background, and with minimal disruption to you and your team.

Instantly your business will be more resilient because of it.

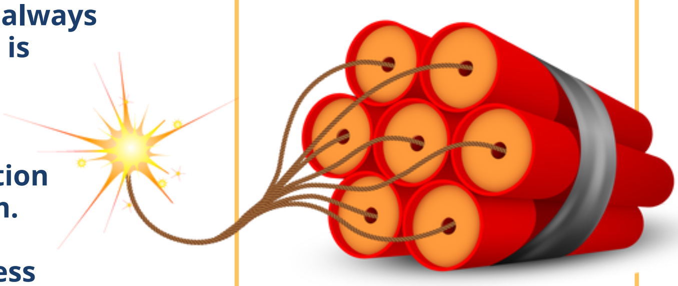
DID YOU KNOW?

Did you know... about dynamite phising?

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 as well as staff training to stay protected.



Technology update

With many 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 waiting for data theft. So any data sent over public Wi-Fi (especially those that don't need a password to gain 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 fraudulent wi-if networks to be wary of. You think you're connecting to the coffee shop's Wi-Fi… but how do you know isn't it a fake version of the real thing?

As soon as you log on, they can capture your credentials and potentially other personal data on your device. If members of your staff are using public Wi-Fi regularly, a best practice is to use a VPN (Virtual Private Network) to keep the data safe.

A VPN acts as a private tunnel for your device to connect to your company network, keeping your info safe. Your IT service provider can recommend an appropriate solution based on your unique situation. NOTE: Many of the consumer VPN services will do little to nothing to protect your company data.

Or better yet, bring your cellular hotspot (a.k.a. your cell phone) and use its data plan—nothing extra to carry, configure, or to charge.

FUN TECH QUIZ

Test the staff on your next Zoom call

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) Mother-board

INSPIRATIONAL QUOTE OF THE MONTH

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

Bill Gates

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 emails

MICROSOFT 365 TIP

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

- Bring up 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

IT WON'T BE LONG BEFORE YOU WILL BE TARGETED BY RANSOMWARE if you have not already been so...

Here's a scary thought: The fastest-growing cyber-crime is Ransomware, and it's a "big" business. But, unfortunately, it's businesses exactly like yours that make that possible.

Simply put, Ransomware is where your data is encrypted until you pay a ransom. It's terrifying to see and very hard to undo once an attack has launched. And yes, it DOES have a long-term impact on the business.

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

True, it only takes one click on one bad link to let a criminal into your system. And once in, they will spend weeks hiding in the background, secretly preparing the attack by learning about you, the business, and whom you do business with.

One of their primary goals is to stop your IT partner from kicking them out once they have landed and established a foothold.

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

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

So, the question you need to ask yourself is. Do you know how resilient your business will be when it is hit with Ransomware? We can tell you.

Let's jump on a 15-minute video chat where you can talk to our chief security expert, Alan Helbush, who will ask you a few questions about your business, its technology, and as your staff.

No tech talk, we promise—just a good and worthwhile conversation about protecting your business.

Set up video chat with Alan today at www.WTSci.com/AlanHelbush or download the guide at www.WTSci.com/RansomwareResiliency

Let's talk on a video chat

But first, I have three questions for you:

1. Do you currently have an IT support company?
2. How happy are you with them?
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 to see how we can help.

It's true, the events of the last few years has taught businesses just how important it is to get proactive and responsive IT support when you need it.

And, we're taking on new clients again.

Set up a 15-minute exploratory video chat at
www.WTSci.com/AlanHelbush

WHERE TO START
TECHNOLOGY SOLUTIONS

Alan's Calendar

How you can get in touch with us:

CALL: (844) 727-6448 | **EMAIL:** hello@WTSci.com
WEBSITE: www.WTSci.com

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 much storage space my apps are taking up?

ANSWER

Sometimes if your computer is running slowly it's a good idea to remove the 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