JULY 2024

perigonone

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

Wallet? Check. Diary? Check. Laptop? Uh oh... laptop...? Laptop???

Picture this: It's a typical Wednesday evening, and your employee Jane is heading home after a productive day at the office. She's balancing her coffee cup, a shopping bag, and her work-issued laptop as she steps onto the train. It's only when she gets home that she realises, with a sinking feeling, that her laptop is nowhere to be found. Is it still on the train, maybe?

And then panic sets in as she remembers all the sensitive data stored on that device.

This scenario is a nightmare, but it doesn't have to turn into a full-blown crisis. Having a solid plan in place can mitigate the risks associated with a lost or stolen work device.

Here's what you should do if you or one of your team finds yourself in Jane's situation:

First and foremost, create an environment where employees feel comfortable reporting a lost or stolen device immediately. Jane needs to know that the sooner she informs the company, the better. Emphasise that there will be no blame or punishment – what matters most is safeguarding the data.

Ensure that all work-issued devices have remote wiping capabilities. This is your first line of defence. When Jane reports her laptop missing, your IT team should be able to remotely wipe the device, erasing all data to prevent unauthorised access.

Before a device is lost, proactive measures can make a world of difference. Make sure all company devices are encrypted. Encryption converts data into a code to prevent unauthorised access. Even if someone gets hold of Jane's laptop, encrypted data remains inaccessible without the proper decryption key. Most modern operating systems offer robust encryption options.

Always enforce strong password policies. Jane's laptop should have a complex password and, ideally, two-factor authentication (2FA). This adds an extra layer of security, making it harder for anyone to access the data if they bypass the initial password protection.

Regular training is vital. Employees should understand the importance of device security and the steps to take if a device is lost or stolen. Conduct workshops and send reminders about security protocols. The more informed Jane is, the quicker and more effectively she can respond to the loss.

Why are these steps so crucial? If Jane's laptop falls into the wrong hands, the consequences can be severe. Unauthorised access to customer files can lead to identity theft and loss of client trust. Exposure of financial data could result in significant loss and legal consequences. Proprietary information could be stolen and sold. It's a nightmare.

By implementing these strategies, you can sleep easier knowing that your company's data remains secure, even if a device goes missing. It becomes a minor annoyance not a disaster.

If we can help you create and implement a plan for this kind of scenario. Get in touch.

DID YOU KNOW...

Microsoft is SERIOUS about security?

Cyber security is crucial, and Microsoft knows that more than most. Now the tech giant has upped the ante, tying executives' pay to security performance. Basically, if it gets hacked, they don't get their bonuses.

This inspires confidence that Microsoft is really taking accountability for its security plans... but how do you think the executives feel about it?

TechFacts

1. On 30th April 1993 the directors of CERN released the source code of the World Wide Web into the public domain, making it freely available to anyone, without licensing fees. This was at the urging of its creator Tim Berners-Lee and allowed the web to flourish.

2. The first wristwatch with the ability to make phone calls was the Samsung SPH-WP10, released in 1999.

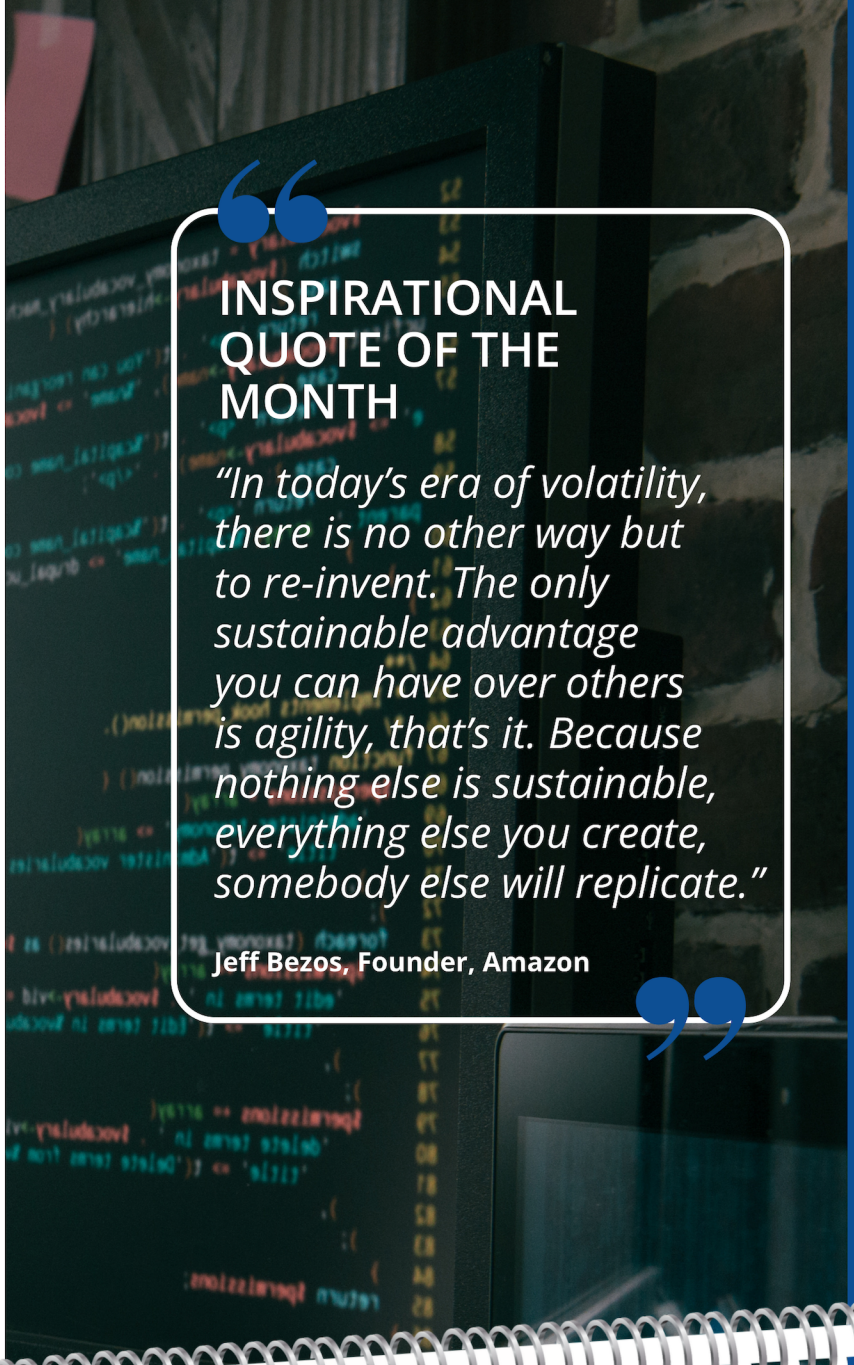
3. The first widely used web browser was Mosaic in 1993.

Technology update

Tech giants join forces to combat online scams

Some of the world's biggest tech companies, like Meta, Match Group, and Coinbase, have joined forces to form Tech Against Scams. It's a new cross-industry coalition to help reduce the amount of successful scams online.

And it has created a platform where people can share knowledge and best practice on how to fight common scams. Last year people were conned out of more than £1.5 billion.



INSPIRATIONAL QUOTE OF THE MONTH

"In today's era of volatility, there is no other way but to re-invent. The only sustainable advantage you can have over others is agility, that's it. Because nothing else is sustainable, everything else you create, somebody else will replicate."

Jeff Bezos, Founder, Amazon

It's time for July's fun tech quiz – who will be this month's quiz champ?

1. In an August 2021 blog post, CEO Ryan Roslansky approved permanent remote work for employees of which business-oriented social network?
2. What delicious computer term did web browser programmer Lou Montulli coin to refer to information that is sent from the browser to the web server?
3. What does "IoT" stand for?
4. What device was announced in 2007 with this slogan: "This is only the beginning"?
5. Wi-Fi is a family of wireless network protocols modelled after the IEEE 802 set of LAN protocols. What does LAN stand for?

The answers are below.

1. LinkedIn
2. Cookie
3. Internet of Things, such as your fridge and Alexa
4. iPhone
5. Local Area Network

NEW TO

MICROSOFT

You can block employees taking screenshots in Edge

Data privacy for your business is critical. But it's not only cyber criminals you need to be wary of. Sometimes, your staff could be (intentionally or unwittingly) sharing your confidential data using screenshots on their browser.

Microsoft is stepping in with screenshot prevention tools in Edge. You'll be able to tag webpages as protected, which will stop any unapproved copying of the data.

It's almost time to say goodbye (to Windows 10)

Microsoft announced that, come October 2025, Windows 10 will officially reach its end of life. This means no more updates or support, which could leave your business's systems vulnerable. It's a significant shift, but you have a few options to manage the transition smoothly and make sure your operations stay secure and efficient.

Option 1: Ignoring the inevitable
You could choose to do nothing and keep using Windows 10. However, this "ostrich" approach could expose your business to serious risks. Without updates, your systems become perfect targets for cyber attacks. The data you handle daily – customer details, financial information, and more – could be at risk. Not the best idea, right?

Option 2: Upgrade to Windows 11
The logical next step is to upgrade to Windows 11. Before you jump in, it's crucial to check if your current hardware can support it. Windows 11 comes with higher system requirements, so you may need a compatibility check (there are tools available for this). The benefits of upgrading are plenty - enhanced security, a more intuitive interface, and new features designed to boost productivity. Windows 11 is a great way to enhance how you work.

Option 3: New hardware
If your current devices don't meet the requirements for Windows 11, it might be time for an upgrade. Don't look at

investing in new hardware as a cost; it's an investment in your business's future. New devices are faster, more efficient, and come with better security features right out of the box. It's an opportunity to streamline operations and maybe even reduce your long-term costs.

Option 4: Pay for Extended Security Updates
If upgrading isn't an option right now, Microsoft offers Extended Security Updates (ESUs) for Windows 10. This means you can still receive critical security updates, but at a cost. For the first year, the price is manageable, but it doubles each year after that. While this can keep your systems secure a little longer, it's a temporary solution with escalating costs.

While autumn 2025 might seem far away, starting your transition plan now is wise. Deciding whether to upgrade, update, or overhaul your systems takes time. Early planning helps minimise disruption and spreads out the costs associated with transitions.

If you're feeling overwhelmed by the choices or just need some expert advice tailored to your business needs, we can help – get in touch.

Jason Willison, CEO Recommendation

Therabody SmartGoggles

I received the Therabody SmartGoggles as a birthday present, and they have been fantastic. These goggles are designed to provide relaxation and relief through a combination of heat, massage, and vibration. The SmartGoggles are particularly effective for easing eye strain, reducing headaches, and promoting overall relaxation.

The build quality is excellent, and they feel comfortable to wear for extended periods. Pairing them with your phone and their app has some really cool sessions curated with some great soundscapes. Love the heat pads that provide a soothing sensation.

$299 from Therabody.

Q: Which is the best browser to use?

A: It comes down to personal preference, but check your chosen browser is secure, has tools that work for you, and can be as private as you need it to be.

Q: What's the difference between 2FA and MFA?

A: 2FA (two-factor authentication) requires two types of authentication – say, a password and a onetime code. MFA (multifactor authentication) requires at least two, or more types of authentication.

Q: Which is best?

A: The answer depends on how your business works and what you're securing. Ideally, you'd use the method with the highest security standards yet the lowest amount of effort. We can help you figure this out.

perigonone

NOT ON THE EMAIL LIST ALREADY! GET A COPY OF TECHNOLOGY INSIDER EVERY MONTH...
To be added to the mailing list click here

CALL +61 8 6146 3582
EMAIL reachout@perigonone.com.au
WEBSITE www.perigonone.com.au