JULY 2024

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

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 realizes, 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. Emphasize 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 defense. When Jane reports her laptop missing, your IT team should be able to remotely wipe the device, erasing all data to prevent unauthorized 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 unauthorized 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. Unauthorized 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?

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 fall 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 minimize 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.

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.

Business gadget of the month

Jabra Stealth Bluetooth headset

If you take a lot of calls but you're also always on the go, a Bluetooth headset could save you time (and arm ache). You don't need to stop what you're doing to answer the phone each time a call comes in. And if you spend a lot of time in noisy places, it'll help cancel out that background noise and give you a better call quality.

The Jabra Stealth Bluetooth headset not only looks great, but it's a light and comfortable option too. It also comes with additional ear cushions and hooks so you can get a truly personalized fit.

$145.98 from Amazon.

This is how you can get in touch with us:

CALL: (408) 559-2800 | **EMAIL** info@trutechnical.com
WEBSITE: www.trutechnical.com

TRU Technical Partners
IT SUPPORT & CYBERSECURITY