BIZCOMMUNITY

Tools built specifically to keep your laptop and files in it safe

Issued by ASUS

7 Dec 2022

Security has become an increasingly essential part of our daily lives, and its continued relevance is becoming more apparent. Similar to how you would secure your physical property using risk management tools and security services, corporate and personal data and files should ideally be secured using a handful of tools and strategies.

Sometimes these safety methods aren't evident. But the truth is, that tech companies and hardware manufacturers typically build robust security features into most consumer and commercial devices. This is done both on a hardware level and a software level - and if you're not using all of these you could be putting yourself at risk.

Office computers will already be protected against many threats, with firewalls keeping out hackers and security software blocking malware before it even attempts to infiltrate its magnesium-alloy body.

There are a few additional tools and features that daily users can utilise to ensure even more security at the office and elsewhere. How do you best protect them?

Physical protection

Any business notebook worth its salt has several physical protections built in. For starters, there's the all-important TPM (Trusted Platform Module) chip, which provides the necessary cryptographic technology to secure key hardware components.

When combined with Windows' BitLocker encryption, not only is a laptop password-protected at the initial startup (before Windows itself starts to load), but the hard drive is fully encrypted to protect sensitive data. It's imperative that the entire drive – not just selected files or folders – is encrypted, and BitLocker makes that a simple process.

BitLocker can also be used to encrypt removable drives, so if your staff needs to carry sensitive files on a USB stick, make sure they've spoken to IT about getting it encrypted before they travel.

Certain models feature an NFC reader, which can be used to encrypt with a physical FID02 security key. This allows any user with a Windows Azure AD account the ability to sign in without the need for a password. Simply tap the NFC security card over the touchpad on the device and the login's complete.

Don't forget about the all-so-trusty fingerprint sensor. An integrated fingerprint scanner provides users with a safer and faster way to sign in, and it integrates with Windows Hello, which means you can configure it when setting up a device quickly and effectively.

User protections

Physical security is a good start, but of course, the weakest parts of any security system are its entry points. That's why it's imperative that each user exercises proper security and password protocol when setting up and using a notebook. Especially when that notebook holds important or sensitive personal information.

But a good rule of thumb is to learn these security tricks now and apply them to all your devices.

You've probably heard this many times over - but constructing a powerful password is an art. Capital, number, symbol - check, check, check. The real challenge is not forgetting this password, along with tens or hundreds of others. And no, a notebook labelled 'passwords' won't cut it this time.

It's essential to invest time (and sometimes money) into a good password manager. There are multitudes of these available on the internet, and it's worth reading online reviews and finding one that suits your particular needs. Features like multi-platform operability and creating folders are all available depending on the platform.
Another consideration when using a laptop outside of the office is the security of its internet connection. This is where a VPN comes in - its purpose, to safekeep your internet connection.

Its usefulness extends from the company server to wider internet access, thereby avoiding potential drive-by hackings on insecure public Wi-Fi networks.

It's worth looking at additional forms of physical authentication – such as two-factor authentication – to key internal and external services. So, if a laptop is compromised and a user's passwords are discovered, the hacker is still unable to gain access to critical information.

The role of IT

Business laptops remain the property – and ultimately responsibility – of the organisation, and they'll likely continuously remind you of this fact.

Here, the ASUS Control Centre comes into play. This gives the IT department control over how the laptop is set up, deployed and maintained. In addition, it allows it to perform emergency actions remotely in the case of an unexpected crisis – for example, performing an encrypted disk wipe to remove all traces of sensitive information.

IT has become an integral skill in almost every profession in the 21st century. We've all been subtly forced to understand how technology works in some form. Doing basic problem solving and fixes have become the responsibility of many non-IT business users in a variety of industries.

It's essential to understand exactly how you can keep your business and personal files safe in a notebook – wherever you may be.

- **Asus announces full ExpertCenter desktop lineup at CES 2024** 16 Jan 2024
- **Navigating the digital realm: Asus' role in South Africa's business evolution** 19 Dec 2023
- **Revolutionising medical imaging: Asus healthcare AI solutions unveiled** 19 Dec 2023
- **The impact of smart conferencing equipment on business collaboration** 18 Dec 2023
- **Tech trends shaping the future: The rise of AI in South African businesses** 11 Dec 2023

ASUS

ASUS offers the best mobile computing technology. No matter where you are on your professional journey, there's a notebook ready to expand your capabilities and streamline your digital life.
Profile | News | Contact | Twitter | Facebook | RSS Feed