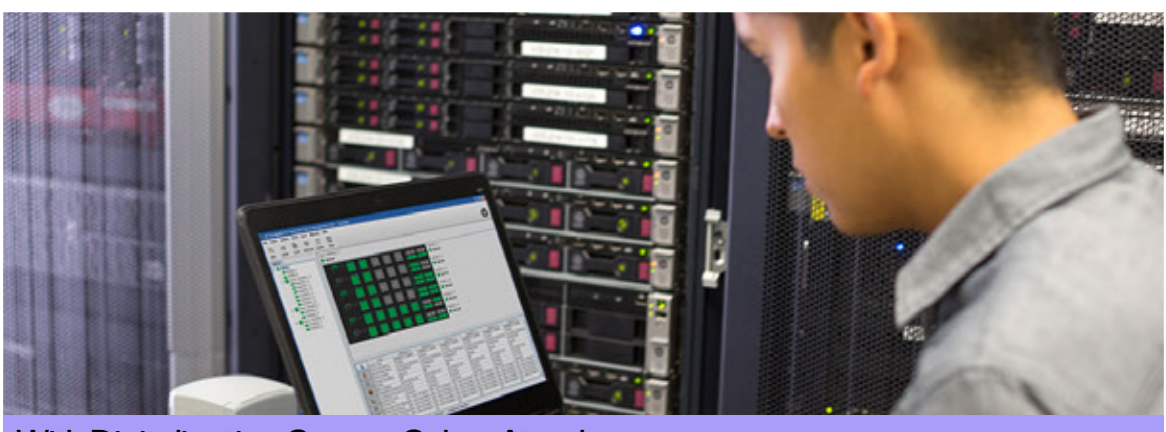
Is Your Online Business Safe from Cyber Criminals?

The digitalisation of the Philippines has grown rapidly over the past two years. To really benefit from the transformation, businesses must first make sure their digital presence is safe from cyber threats.

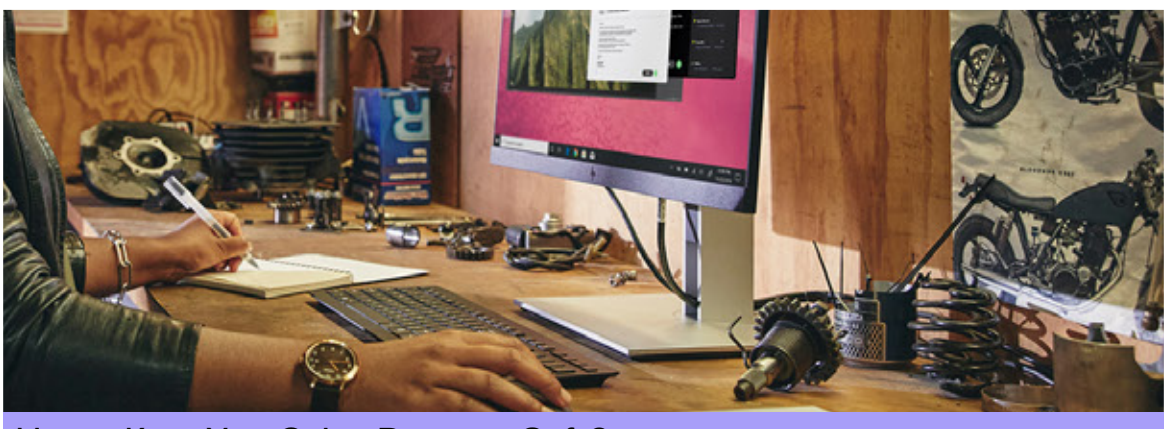


With Digitalisation Comes Cyber-Attacks

Digitalization in the Philippines is constrained by barriers, such as outdated policy and regulation, poor access to high-speed Internet connection, and lack of support infrastructure like logistics and digital payment.[1] However, with the pandemic and the lockdowns that followed, Filipinos had no choice but to quickly adapt to the digital world. And with that, it has unfortunately opened up doors to malicious cyber-attacks.

In late November 2021, more than 20,000 Philippine customers were notified that their personal details had been compromised in a ransomware attack on a big membership store.[2] Cyberattacks do not discriminate. Whether it's individuals, SMEs or large corporations, cyberattack is a risk to everyone. OpenGov Asia reported that a UK-based cybersecurity firm found that Philippine organisations have spent an average of $820,000 (approximately P40 million) to recover from these attacks – costs that cover the ransom paid, and the costs incurred by the downtime.[3]

With these drastic effects, businesses are starting to take cyber threats more seriously than ever.



How to Keep Your Online Business Safe?

In order for businesses to thrive safely online, robust security systems need to be in place. Here are some helpful tips to create and maintain a secure work environment, especially when remote or hybrid work is here to stay.

1. Set Up Effective Endpoint Management System

It is crucial for your business to put up protective measures the moment they begin incorporating digital tools, and ultimately bridging the virtual and physical realms of your operations.

For one, it is highly recommended to establish security protocols at the frontline of your business. You can do so with the help of endpoint security management systems.

Endpoint refers to the entry points accessed using end-user devices such as laptops, PCs, and mobile phones. It is also where cyber criminals frequent as they usually take advantage of unsuspecting end users to hack into your organization's digital space.
Having an endpoint security management system gives you the ability to protect your workflows and information with endpoint devices connected with your network.

2. Boost Your IT Team's Capacity to Safeguard

Business owners should also take note that relying on traditional anti-cyberattack strategies is not enough to keep everything safe. For company IT teams to fully do their job in protecting the company from cyber threats, they must be equipped with the right tools and programs to help anticipate, contain, and prevent cyberattacks from breaching into your company's digital ecosystem.

3. Only Trust Reliable Devices

One of the most basic and simple steps in making sure your business is safe from cyber-attacks is to trust reliable devices. Your employees must be provided with devices that can enhance their productivity anywhere and anytime, and at the same time, give you peace of mind.

Trustworthy devices for work are such as the latest laptops or PCs running on up-to-date software programs. Outdated technologies and applications are prone to cyberattacks due to the fact that they no longer have the

HP Solutions

Providing SMEs a Safe Journey to Digitalisation

Keeping your online business safe should be done without disrupting its digital transformation, and ultimately its growth. This is why you should build your cyber security defenses with the help of innovative solutions and technologies.

Endpoint security solutions that can counter aggressive and unknown cyberattacks such as HP Wolf Pro Security can also act as your IT team's extension. With its enterprise-grade security features, HP Wolf Pro Security can provide a multi-layered defense for your company without putting additional workload on your IT staff. From self-healing firmware and in-memory breach detection to threat containment via isolation, HP Wolf Security reduces the addressable attack surface and enables remote recovery from firmware attacks.

Boosting performance of your workforce

As mentioned, equipping your team with the right devices is crucial for performance. Allow your team to master cloud-based computing and tasks with top-of-the-line business laptops, such as HP ProBook 440 G9. These laptops powered by the latest generation of Intel Core processors and Windows 11 Pro are designed to boost performance of your workforce, all while you work at ease knowing that the safety and privacy of your company will not be compromised.

HP Probook G9 series

LEARN MORE

HP ProBook 440 G9 and HP ProBook 450 G9

LEARN MORE

HP Wolf Security

HP WOLF SECURITY

LEARN MORE

Sources

1. Secure Connections (2022, March). Cybersecurity In The Philippines: Global Context And Local Challenges. Asia Foundation. Retrieved April 21, 2022, from https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

2. Felix Kim, (2021, December 19). Philippines tightening cyber defenses as attacks surge. Retrieved April 21, 2022, from https://ipdefenseforum.com/2021/12/philippines-tightening-cyber-defenses-as-attacks-surge/

3. Aineena Hani (2021, September 29). Strengthening Cybersecurity Readiness in the Philippines. OpenGov Asia. Retrieved April 21, 2022, from https://opengovasia.com/strengthening-cybersecurity-readiness-in-the-philippines/