BIZCOMMUNITY

7 steps to keep your SME cyber safe

Cybersecurity for small business has come to the fore as more SMEs shifted towards digitalisation to survive in the unstable by Covid-19 circumstances. Yet, a whopping two out of five companies in the US and the United Kingdom with 50 or fewer employees do not have any type of cybersecurity defence plan in place, according to research from IBM and the Ponemon Institute released in 2020.

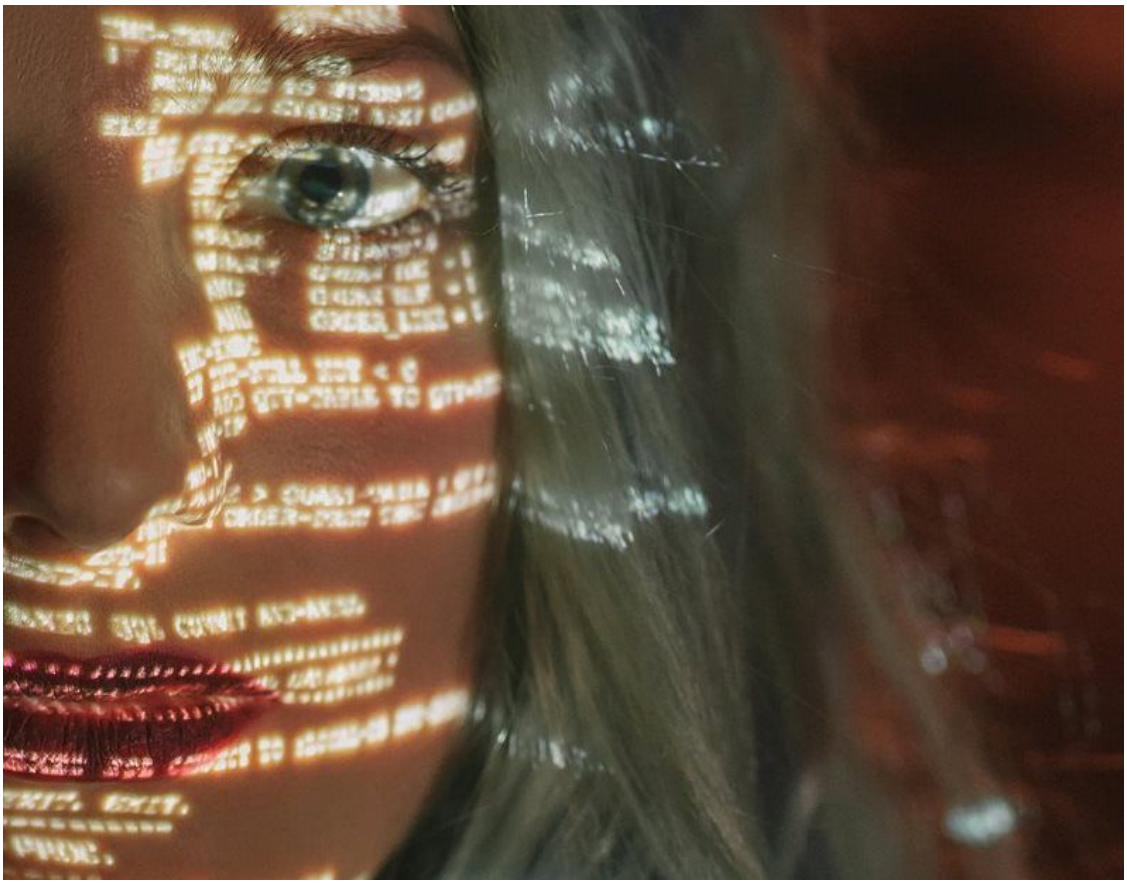

Photo by cottonbro from Pexels

Cybersecurity experts at Enhalo, a full-circle cyber defence group, offer seven steps to keep your SME cyber safe in 2021:

1. Education must be a priority

An educated workforce has to be a top priority. The truth is, many cyberattacks target a business where it is most vulnerable: the employees. Therefore, educating staff on the type of threats and how to deal with them must take centre stage on your cybersecurity awareness plan.

Each security incident should be an opportunity to educate, test and reinforce details on what the business is protecting and why it's important to behave in a certain way.

Human fallibility remains the weakest link in cybersecurity

Yash Pillay 19 Jan 2021

Once your staff understands what the business is trying to protect, and buy into the importance of following secure behaviours, they become accountable and actively participate in creating a secure environment.

2. Backup data and restore quickly

Having your data backed up and restored effectively is the foundation of cybersecurity. Data that cannot be restored to its original state is useless, so you need to consistently back up and check the reliability of the data once restored.

Backup systems can be automated with a minimal time investment required. In fact, this process can take only 15 minutes a month. Checking that your data can be fully restored using only three hours a year, is the best security investment you can make.

3. Defend with multifactor authentication

Every small business should be using Multifactor Authentication (MA) as the first line of defence because it is difficult for cyber attackers to get around. Multifactor authentication is simple and available on most cloud platforms at no or a low cost.

Think cybersecurity is expensive? Just wait until there's a breach...

Lukas van der Merwe 18 Dec 2020

4. Encrypt remote access to your network

Protecting and encrypting remote access on your internal network is a critical layer of cybersecurity because employees and third parties can log into your system remotely using their phones or other devices.

Using VPN encryption or SSL/TLS level security to protect access to your network, adds a layer of assurance as employees and third parties may not have adequate security from their end.

5. Rule of least privilege

This is a simple step to implement, yet many small businesses are not vigilant about who gets access to what. Your people should only access what they need for their role and level. Also, when roles change, access should be reviewed using this principle.

Systems should be treated like people; they should also only have access that is essential for their function. If a computer or device does not need access to a server, then don’t give it access.

For example, mobile or IoT devices such as kettles or fridges should not be on the same network as your file server containing your critical business data. Such devices should be on a separate network so that if compromised, cybercriminals can't use them to gain access to your confidential files.

6. Reduce the attack surface area

Not everything has to be online, that is on the cloud or on a computer connected to the internal network. Something that cannot be accessed is essentially an impenetrable vault; hackers can't attack something that they can't reach.

7. Patch management is a must

Software is being updated all the time to address any security vulnerabilities as well as providing new features. Regularly check for software updates to make sure you are on the latest, stable and tested version. Remember that patching does not only apply to operating systems and applications but also to the firmware for all devices such as routers, firewalls, and printers.

While there is some automation in patch management, this is not a step you can leave to vendors to control. It requires hands-on diligence and because hackers know it is the one area that is often neglected by small business, they easily exploit this space.

If you follow these cybersecurity steps for small business, bearing in mind the principles of simplicity, access control (AC), confidentiality, integrity, availability (CIA) and layering, you will be able to build a more secure and resilient company.