CYBER SECURITY AWARENESS

#BeCyberSmart

CGM CompuGroup Medical

Content

Do your part #BeCyberSmart

Cybersecurity starts with YOU and is everyone's responsibility. There are currently an estimated 5.2 billion Internet users - over 65% of the world's population. This number will only grow, making the need to #BeCyberSmart more important than ever.

Cybersecurity starts with you.

Everytime you use the Internet, you face choices related to security. Friends can be selected, links clicked, websites accessed, and wireless networks can be joined.

Your security depends on making secure online decisions. Making the Internet more safe and secure requires all of us to take responsibility for our own cybersecurity posture.

For more information on Cybersecurity visit **www.cgm.com/za-becybersmart**

Cybersecurity: What is it?

Cybersecurity is the art and science of protecting networks, devices and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity and availability of information.

Cybersecurity is making sure that your online presence, your smart devices, your information in cyber space stays safe and out of the hands of the wrong people.

For more information on Cybersecurity visit **www.cgm.com/za-becybersmart**

Poor Cybersecurity?

Just like with most things, being online has inherent risks. Some are more severe than others. But poor cybersecurity can make you, and often those you connect with, more vulnerable to those risks. Your computer can be vulnerable in many ways.

A malicious attacker can hack into your system and change your files, or you can be attacked by malware. Even if you take the best precautions, you can't always prevent these things, such as:

- Exposure of the customer data and the associated costs.
- The cost of litigation
- Ransomeware incidents - if paid, ransomware can cost tens of thousands of rands.

For more information on Cybersecurity visit **www.cgm.com/za-becybersmart**

Sobering Cyber Stats.

1 RANSOM ATTACK every **11 SECONDS** globally.

Malicious emails are up **600%** due to **COVID-19.**

The largest ransomware payout was **$40 MILLION** setting a **WORLD RECORD.**

Out of **1,086 ORGANISATIONS** whose data had been encrypted, **96%** got their data back.

The average downtime a company experiences after a ransomware attack is **21 DAYS**.

In **SEPTEMBER 2020** alone, cybercriminals infiltrated and stole **9.7 MILLION** medical records in the USA.

Source: https://www.varonis.com/blog/ransomware-statistics-2021/

For more information on Cybersecurity visit **www.cgm.com/za-becybersmart**

Potential threats.

Phishing: Phising attacks use emails and malicious websites that appear to be trusted organisations, such as charity organisations or online stores, to obtain user personal information

Malware: A computer can be damaged or the information it contains harmed by malicious code (also known as malware). A malicious program can be a virus, a worm, or a Trojan horse. Hackers, intruders, and attackers, all of whom are in it to make money off these software flaws. Despite their benign intentions and curiosity, their actions are usually contrary to the intended uses of the systems they exploit.

Identity Theft and Scams: Identity theft and scams are crimes of opportunity, and even those who never use computers can be victims. There are several ways criminals can access your information, including stealing your wallet, overhearing your phone call, dumpster diving (looking in your trash) or picking up on a receipt that contains your account number. While you cannot guarantee that you will not be victim of identity theft, you can lower your risk with a few simple tips...

Simple Tips for Cybersecurity.

AT HOME

- Have separate devices for work and personal use.
- Connect to Ethernet (wired) or at least WPA2 (Wi-Fi Protected Access 2) for a secure wireless connection.
- Use a VPN (Virtual Private Network) whenever possible to access employer systems/data.
- Keep router and modern firmware up-to-date.
- Secure IoT devices (smart speakers, appliances, etc) - use strong, unique passwords whenever possible.

TRAVELLING

- Don't use public Wi-Fi when accessing confidential info. Use a personal hotspot instead.
- Keep devices secure and accounted for at all times.
- Disabled automatic bluetooth pairing.
- Don't allow your devices to auto-join unfamiliar Wi-Fi networks.
- Don't use borrowed chargers or public charging stations.

PHYSICAL SECURITY REMINDERS

- Never use unknown USB devices.
- Always lock your workstation.
- Keep confidential information secure - use privacy screens and headphones if necessary.
- Implement a clean desk policy by removing business documents, notes, etc.
- Don't allow unauthorised individuals to tailgate.

AT HOME

- Enable multi-factor authentication (MFA) that requires a separate device when possible.
- Practice good password hygiene.
- Never save passwords on your browser.
- Keep work-related communication to systems and approve by organisation.
- Check privacy/location/security settings on apps and restrict any unnecessary access.

Read more about the importance of backing up your data here >

#BeCyberSmart

CompuGroup Medical SA (Pty) Ltd.

Block 3 · Upper Ground Floor · 1 Waterhouse Building · 4 Waterford Place
Century City · Cape Town · 7441 · South Africa
P: 0861633334 · E: hello.za@cgm.com · www.cgm.com/za-becybersmart
Directors: Christo Groenewald · Thorsten Kollet
Company domiciled in: Cape Town
Company Reg. No. 2005/023029/07 · VAT ID: 432 022 6063

Synchronizing Healthcare

CGM CompuGroup Medical