Protecting your practice in a digital world: Knowledge is power

Hacking happens every second of every day. So reported Pieter Geldenhuys, Director of the Institute for Technology, Strategy and Innovation at a Glacier webinar titled Protecting your practice in a digital world. He offered some insights into what cybercrimes are trending and how you could beef up your digital security, which is the critical step in protecting your data and practice.

Knowledge really is power in the cyberwar

The first step to crime prevention is knowing who is likely to attack you and how they will do it. Pieter lists three types of hackers and many types of attacks.

White hats are hackers employed by a company or organisation to test their security by intentionally hacking and finding weaknesses. Gray hats are external hackers who create digital problems for the organisation and then offer their consulting services to fix the problem. Black hats are hackers with nefarious objectives and malicious intent.

The list of types of attacks is alarming and warrants attention. These include malware, phishing, password attacks, distributed-denial-of-service (DDOS) attacks and machine-to-machine attacks. One of the most common of these attacks is malware, which Google defines as a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network. Malware takes various forms – electronic worms, spyware and viruses, and obviously none of these are good news for your computer system or data. Pieter recommends the following ways to mitigate malware:

- router firewalls
- software updates
- computer firewalls
- anti-virus software.

To err is human

Pieter points out that the biggest threat on the dark web is social engineering, meaning that human error trumps firewalls, encryption and anti-virus software. If you are not on guard and consciously wiser than hackers and scam artists, your firewalls won't protect you, your data or your money.

Here are some of Pieter's tips to mitigate cybercrime:

1. Let's not go phishing. The point of phishing scams is to access your personal information like usernames and passwords, banking pins and so forth, with the simple goal, ultimately, to steal your money. This means that you need to be circumspect about the emails you open, the information you provide over the telephone to a supposed 'bank call centre' or a company you don't remember contracting with. Banks and companies will not ask you for pins and personal information over the phone. If you are their customer, they already have your information. Also, they will never ask you for the OTP that usually appears in an SMS on your phone. Regarding unexpected or unknown emails, check that the email address really is from the company you suppose it is.
2. Don't re-use passwords across the internet. This is the most common mistake and renders many scammers successful in accessing your data. Also, don't record your list of passwords on your computer. Passwords managers provide a safer way to save them.
3. If you're a company or online business, monitor and analyse your traffic. This also could mean limiting international hits on your website, which could mitigate denial-of-service attacks.
4. Check if you had a data breach at haveibeenpwned.com. Know if your passwords have been pwned by checking the lists of usernames and passwords on this website. There are billions of usernames and passwords that are 'open' for breach on the internet. Is yours one of them?
5. Make multi-factor authentication (MFA) your norm. Google defines MFA as a user having to provide two or more pieces of evidence to verify their identity to gain access to an app or digital resource. MFA goes a long way in ensuring access security.
6. Choose resilience over robustness in your digital security. Don't focus on one kind of security authentication methodology that offers 99.9% security. Rather use multiple methodologies that offer 90%.
7. Be aware of your vulnerability when using public Wi-Fi. Make sure that the website you log onto starts with https:// and use a virtual private network (VPN) that can be activated on your phone and that can encrypt your data.

Glacier Financial Solutions (Pty) Ltd.

A member of the Sanlam Group
Private Bag X5 | Tyger Valley 7536 | Email client.services@glacier.co.za | Tel +27 21 917 9002 / 0860 452 364 | Fax +27 21 947 9210 | Web www.glacier.co.za | Reg No 1999/025360/07
Licensed Financial Services Provider | Glacier Financial Solutions (Pty) Ltd. is also a Licensed Discretionary Financial Services Provider FSP 770, trading as Glacier Invest | Sanlam Multi-Manager International (Pty) Ltd. | A member of the Sanlam Group

Private Bag X8 | Tyger Valley 7536 | Tel +27 21 950 2600 | Fax +27 21 950 2126 | Web www.smmi.com *|*Reg No 2002/030939/07
Licensed Discretionary Financial Services Provider, acting as Juristic Representative under the Glacier Financial Solutions FSP 770
Glacier International is a division of Sanlam Life Insurance Limited
Sanlam Life Insurance Ltd. | Email life@sanlam.co.za | Tel + 27 21 916 5000 / 0860 726 526 | Fax +27 21 947 9440
Reg No 1998/021121/06 | Licensed Financial Services Provider