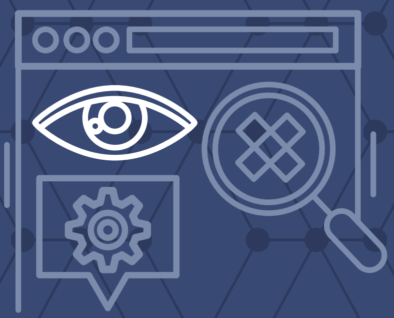
ATTENTION! *CYBERCRIMINALS CAN INTERCEPT YOUR DIGITAL INFORMATION*



CYBERSECURITY IS CRITICAL TODAY.

The advent of digital technology has brought us many advantages, but it has also created opportunities for cybercriminals, who can intercept, access or modify your digital information to perpetrate fraud or for ***extortion*** and/or ***ransomware attacks***.

Recent examples are WannaCry and Petya, known as ***ransomware***, malicious software that blocks access to a victim's data and threatens to delete or publish it until a ransom is paid.

BOTH YOU AND/OR YOUR BUSINESS COULD EXPERIENCE

- Loss of access to operating systems and/or data
- Threats to publish your data
- Data deleted until a ransom is paid

Once a ransom has been paid to the cyber actors, there is still no guarantee that the decryption key will be released!

---- DID YOU KNOW? ----

Even more scary, is that fraudsters are able to use malware to steal your credentials and impersonate you online. No one would be any the wiser, and they could clean out your bank account!

WHY IS IT GETTING WORSE?

- Lack of awareness about cyber threats
- Lack of sound cyber hygiene
- Lack of employee awareness within an organisation
- IT security not enhanced
- Security updates on computers and operating systems not conducted frequently enough.

HOW CAN YOU PROTECT YOURSELF AND YOUR BUSINESS?

- Avoid using public Wi-Fi hotspots for online banking.
- Don't send passwords or account login credentials over public or unsecured Wi-Fi networks.
- Use different passwords for different systems (don't have the same password for Facebook as your online banking).
- Use complex passwords changed every six months (8 character or more, a mix of upper and lower case, symbols and numbers).
- Install mobile security and antivirus software from a trusted security vendor.
- Change Wi-Fi passwords regularly.
- Use a two-factor authentication system whenever possible.
- Use secure web sites with 'https' and a "padlock" icon in the address bar.
- Instead of clicking on the link in the email provided, manually type the website in question into the URL bar of the browser and proceed from there. A malicious site is not able to recreate the legitimate HTTPS indicator.

> ***"While new technologies such as apps and Wi-Fi spots have made banking easily accessible to the public, they also carry certain risks. Consumers must be aware of these risks and take steps to safeguard themselves."***
>
> ***Kalyani Pillay***

SabricZA @Sabric SabricZA www.sabric.co.za

sabric

Making South African banking safe, secure and fraud free