December 10, 2018

Beginners guide to practical Cybersecurity

Every 40 seconds, a company gets hit by ransomware, with hackers breaching up to 12 million files per minute.

Unfortunately, it's far more sophisticated and disruptive to your business operations. In this article we will look at the type of business records being hacked and the various ways in which the hackers get hold of information. Then we'll give a few easy tips on how to avoid cyber threats and how to protect your business's privacy.

What is the real extent of the problem?

In the new information age, hackers most often see potential for abuse because of greater visibility of private life. They retrieve data from various sources and access data which they can use for identity theft and hacking accounts.

- When logging onto a website, always look for the **“s”** and/or the lock in the link - http**s**:// - this indicates that your network is secure. The link will sometimes be displayed in green when the website is secure.
- Another tip is never to connect to public WiFi when having access to your company’s server or sensitive information, especially when a two-factor authentication password is not required.

What type of passwords can be used?

- The best password is one that even you don’t know. This is why you should use a security strategy with a password manager. However, for the passwords you do have to remember use long pass phrases or well-known phrases that are likely to be in a dictionary.
- The key is to mix things up as much as possible so that if someone does get into one of your accounts, they can't use the same information to get in everywhere else.

Conclusion

When you are aware of the risks, it may be much easier to protect yourself and your business from hackers, viruses and malware. Remember to install a good antivirus and anti-malware program on your computer and keep it updated. Never give out personal information to anyone who calls you on the phone. People can impersonate someone from a legitimate company trying to get information about your username and password and use that information to obtain information about your family and friends.

SERR Synergy assists businesses in compiling an Information Security Management Systems (ISMS) policy where the physical information and cybersecurity risks of organisations are identified and managed to maintain the confidentiality, integrity and legitimate availability of data.

Don’t miss the next part of our analysis and practical guide to ensure *cybersecurity* and learn how cybersecurity relates to all aspects of information compliance legislation in South Africa.

About the Author: Retha van Zyl completed her BCom Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title ‘Information Compliance Advisor’. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA manuals to the Human Rights Commission. She also compiles and implements ISMS policy to identify risks associated with information security in each department within an organisation.

Sources:

https://www.breachlevelindex.com/

https://www.theregister.co.uk/2015/11/12/snowden_guide_to_practical_privacy/

https://lifehacker.com/edward-snowden-explains-why-you-should-use-passphrases-1696958545

https://www.manageengine.com/products/desktop-central/secure-network-from-ransomware-and-cyber-attacks.html?network=g&device=c&keyword=cyber%20security&campaignid=45456045&cr294877362656&gclid=Cj0KCQiA8_PfBRC3ARIsAOzJ2urKYOZ58nS5-LHW1JKQUm1rIYWRMkRf-sXBRug_0xDlJ_zniZ7XzVIaAoXOEALw_wcB