Become more cyber smart in 2019

As we enter 2019 with a fresh outlook and practical New Year's resolutions, why not also add 'improving cyber skills' to your list of goals?

Source: pixabay.com

Given the importance of protecting yourself and assets in the online space, you should make 2019 the year you get on top of things making sure you have the digital skills to guard against criminal attacks.

“Being cyber smart is critical in the digital age when all of our personal data is online and mobile devices are the popular tool used to access online accounts,” says Junaid Munshi, Cell C’s chief commercial officer.

“We need to protect our online documents, passwords, and personal information and this means taking a few simple steps,” he adds.

“These measures don’t take long and the reward is ensuring your identity, data and money are safe, and that you and your family do not fall victim to cybercriminals.”

Here is a list of tips to help South Africans become more cyber smart in 2019.

1. Downloading apps from a trusted source

Make sure your apps are downloaded from a trusted source such as the App Store. You can also read the comments in the feedback section to help you ensure that the app is legitimate.

Be careful of downloading apps from a link sent to you in an email or SMS message. When downloading an app it is also important to review what type of access the app requires e.g. a gaming app that requires access to your location, contacts and gallery.

2. Avoid performing sensitive transactions over public WiFi

Don’t conduct any business or commercial affairs online over public WiFi. Rather use a trusted, secure network at home or the office. Public WiFi networks are not always secure and your credit card details, bills, documents and passwords can be obtained.

If you do use WiFi in a public area such as shopping malls or restaurants, make sure that you connect to the right network by asking personnel for the right name and password. Criminals set up their own networks that may look authentic, which they use to intercept your data when you connect to them.

3. Don’t let family and friends use your work cellphone

Anyone else using a device you use for work – be it a tablet, smartphone or laptop - could accidentally download a virus or spyware, deplete your data or accidentally delete important information. Remember, your banking app may also be on this device so ensure it is for your use only.

4. Don’t click on links from unknown sources

When you receive an email offering a great deal on an item you want, be extra cautious. Don’t click on the link in the email because it could be a scam designed to get your personal details. Rather shop online at trusted franchises. Also, move your cursor over the email address to check its validity. If it looks strange, delete the mail immediately.

5. Lock your device

This is a basic security rule. Ensure you have a strong password and don’t divulge it to anyone. To be even safer, change the password every month. If your device caters for the use of fingerprint biometrics or facial recognition, use that as an alternative security measure.

6. Download a security app

Download apps like ‘Lost’ and ‘Find my iPhone’. These allow you to remotely erase your personal information if your cellphone were to get stolen. These will also keep logins, accounts and passwords safe.

7. Install and update your anti-virus software

As with your computer, it is good practice to also have anti-virus software installed on your phone. Ensure your anti-virus software is consistently up to date and back up your important documents.

For more, visit: https://www.bizcommunity.com