Many of you have probably come across a story of someone falling victim to cybercrime. Five years ago, this might have been unusual, but more and more this is a reality and someone we know personally has been affected.

One of the main challenges with cybercrime is the fact that the schemes are constantly changing. The criminals are continuously working to find new ways to defraud unsuspecting customers. This means that no one ever knows enough, and no one is ever safe.

To give an idea of the damage caused by cybercrime we can share the following stats:

- In 2018 there were 23,466 incidents of banking-related cybercrime reported by SABRIC, costing consumers R262 million. This was an increase of 75% in the number of incidents from the previous year.
- In 2018 there were 7,445 banking application incidents costing consumers R104 million. This was an increase of 55.4% in the number of incidents from the previous year.
- In 2018 there were 3,900 Online Banking incidents costing consumers R129 million. This was an increase of 37.5% in the number of incidents from the previous year.
- In 2018 there were 12,121 Mobile Banking Incidents costing consumers R28 million. This was an increase of 110.4% in the number of incidents from the previous year.

There are, however, a few things you can do to minimise your risk:

- Make sure your PC and Mobile Phone have up-to-date antivirus software.
- Use strong passwords for each of your online accounts. Passwords should be at least eight characters long, and a combination of letters, numbers and special characters are recommended.
- Do not use public computers to access your bank account or emails.
- Never give out confidential information; banks will never ask you to confirm your information over the phone.
- If you receive a phone call requesting confidential or personal information, do not respond and end the call.
- Do not click on links or icons in unsolicited emails.
- Do not blindly believe the content of unsolicited emails. If you are worried about what is alleged, use your own contact details to contact the sender to confirm.
- Type in your online bank website address in the internet browser.
- Check that the banking website certificate is valid.
- If you think that you might have been compromised, contact your bank immediately.
- Always verify bank account information in person with your Trust Officer.

At Personal Trust, our clients are known to us by name. In line with our philosophy of personal service, we do not have a call centre. This means that you will never be called by a stranger about your investments with us, nor will you ever receive an email asking you to insert or verify your credentials.

Should you receive any suspicious communication, do not hesitate to contact your Trust Officer or their Assistant to verify.