YOUR MONEY SORTED

BEWARE OF CYBER CRIME

By LETITIA WATSON
Send suggestions for topics and requests for info to yourmoney@you.co.za.
We may answer your questions in this column but won't reply personally.

Remember: if something sounds too good to be true, it usually is

BE ALERT!

In just one week Your Money received the following "good news" emails: There's a lottery prize waiting for us in the UK; we're being compensated for ATM fraud; an "official" email from Absa, with an attachment; and an email from a destitute woman in Trinidad asking for help to access the millions of dollars she's entitled to. These emails have something in common – eventually they ask for your personal information and banking details. Don't miss the alarm bells, read on now!

PHISHING AND SMISHING

With the phishing scam someone, supposedly from your bank, calls you to persuade you to give them your personal information. But the "bank official" is a fraudster. The smishing scam uses the same technique but the fraudsters send you an SMS asking you to update your personal details. The SMS looks as if it's been sent by your bank and after receiving it the scamsters call and ask for details such as your ID number, account number and even your PIN. Never reveal your banking details in response to these attempts.

THE LOTTERY SCAM

You get an SMS or email telling you you've won a prize in a lottery and you're thousands of pounds, dollars or euros richer. But before you can get the prize money you first have to pay the "tax" or "an administration fee". Common sense would tell you that you can't win a lottery if you haven't bought a ticket. And no lottery will randomly contact you by SMS or email to tell you about your "unexpected windfall". Yet there are those who fall for this scam.

FAST-TALKING FRAUDSTERS

Fraudsters are usually good liars and manipulators. They may come across as very decent and even quote from the Bible. If for instance you get a message from someone asking you to help them access their "inheritance" or if they offer you a cut as compensation, don't fall for it! As with the lottery scam the fraudster will ask you to first deposit a sizeable amount into their account before "compensating" you. If you're taken in by this scam you can kiss your money goodbye.

Three groups spend other people's money: children, thieves, politicians. All three need supervision

– AMERICAN ECONOMIST AND POLITICIAN DICK ARMEY

5 QUESTIONS ABOUT ONLINE SCAMS

1. **What is phishing?** These are emails with links to websites or documents which appear to come from your bank. If you open the link or attachment it can download spyware on your computer. Delete these emails as soon as you receive them.
2. **How can I do online shopping safely?** Use only recognised online retailers. When doing a transaction the website address should change from http to https which indicates it's secure.
3. **What if I get a windfall?** If you get a message saying you've won something and it's from a well-known company first call them to confirm the win. Don't use the number provided in the SMS or email – go to the company's official website to ensure you have the correct contact details.
4. **Can bank officials ask me for my PIN?** No, your bank will never ask you for confidential information such as your PIN, username or password, online or telephonically.
5. **What about social media?** Don't share your physical address or personal information with people you don't know personally.

1 IN 214 EMAILS ARE SUSPECT

Statistics for 2014 show that on average one in every 214 emails sent and received in South Africa were fraudulent. And according to the internet security company Symantec's 2015 monitoring report SA companies were targeted more by worldwide phishing activity in 2014 than companies in any other country, with an overall average phishing rate of 1 in 568 emails.

TIP! Beware of prizes you've supposedly won without entering a competition.

GET MORE HELP HERE

- http://scambuster.co.za/
- http://cybercrime.org.za
- www.staysafeonline.org