SCAMS . . .

The number of email scams is proliferating. The most common of these are the attempts to gain access to our banking accounts. Most start with some type of warning that if you do not do as they say you will no longer have access to your account or may incur losses.

For example,

"Note that this activation is free and compulsory, failure to do this will result in suspension of your account as (Insert Bank Name Here) will not be liable if money is taken from your account without your knowledge."

Other common subjects are:

- Switch: Payment Notification
- Payment Notification (Head Office)
- Payment Confirmed.
- Rejected ACH payment
- Online Service Notice
- Banking Service Notice
- New Message
- Secure your account
- Online Upgrade Notification
- Release/Transfer Notice for your due Funds (US$3,500,000:00)
- Congratulations!! We are happy to announce that you have won an Email lottery jackpot prize.

The common thread is that all these types of scams try get you to click on a link in the email, leading you to a copy of the bank's web page. This web page will look exactly like the banking site and all info you input will be visible to the scammers. When you have put in the verification number you will be directed to a "this site has encountered a temporary problem, please try again later" page. In the mean time the scammers will try to drain your account, often changing SMS notification details etc. The banks will not be held liable in any way as you have given away your access details.

The second type of scam doing the rounds is far more personal. You will receive a phone call from somebody who says they are a Microsoft partner or some such and they are receiving messages from your computer that is about to fail or is infected with viruses. They will direct you to open the system management console error log, which will be used as proof that the PC is indeed about to collapse. The next step will be an attempt to get you to download some software so they can remotely access your PC to fix the problem and thirdly you will be told that you need to buy some software to fix your PC and prevent this happening in the future.

Things you should know

1. Microsoft will never ever call you unsolicited, nor will any major vendor.
2. No legitimate company anywhere in the world will gather information from a private source without their consent. They would be sued into oblivion.
3. The management console is a diagnostic tool and records thousands of transactions. Each time you turn your PC on it will result in 50 or so new entries into the log. Due to the complexity of the hardware and software in a computer, errors are expected. 99.9% of these errors are caused by a momentary conflict when 2 pieces of software try occupy the same space at the same time. When this happens Windows retries until it succeeds. Imagine 2 people trying to fit through a narrow door, they both head in and stop (error, error), perhaps they both half start to do door and stop again (error, error), one says "You first" and person proceeds (error resolved) and then 2nd person proceeds (error resolved). The logs are vitally important when tracking unresolved errors that may cause a PC to hang or crash, but unless you actually know what is it is and what you are looking for, it can appear alarming. This is what the scammers rely on.
4. The remote access software is legitimate and is something we IT people often use to save on a call-out to a client or for other remote maintenance. In the wrong hands it gives somebody full access and control over your PC.
5. The software they propose that you purchase, is completely malicious and will cause your PC to become unusable, they will charge you about R900 for this software.

Internationally the scammers success rate is about 1 in 7 with an average cost to consumer of $825

I suspect that a service provider or two have had their databases hacked giving the scammers access to your contact details, as most of the people I have spoken to about this scam seem to be from the same ISP.

There is a 2nd part to this scam and it involves either ignorant technicians or profiteers in IT service. These technicians when contacted to fix the problems resulting from people being duped, hugely overcharge or inform the person that the only way to fix it is to totally reformat the hard drive. One person I spoke to was charged R1200 to have her drive reformatted and in the process lost all her data as the technician said they could not back it up.

There are subtle variations of all the above scams. The golden rules are:

- Beware of any unsolicited email or phone calls especially if it supposedly comes from a big company,
- Do not click on links embedded in an email, open your browser and type the address in,
- Read the messages your operating system / anti-virus generates when downloading or installing software, don't click blindly.
- If it sounds or feels dodgy to you, trust your instincts and get a second opinion from a trusted source,
- If it appears to be too good to be true, it probably is.

I wish you all a happy and safe holiday season and hopefully the new year will better than the last.

Daryl Meyer

DataSafe Computing