INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

SMISHING: NOW ON YOUR PHONE

According to McAfee SMiShing is:

"... a version of phishing in which scammers send text messages rather than emails, which appear to have been sent by a legitimate, trusted organization and request that the recipient clicks on a link or provide credentials in a text message reply. The term is a condensed way of referring to “short message service phishing,” or “SMS phishing.”"

Over the past few years, we've learnt not to trust emails, fearing we'll become victims of phishing fraud. Most people by now know not to click on links in emails. With SMS's you can't preview links as in emails, which increases the possibility of clicking on it out of curiosity. Unfortunately, human behaviour is the greatest threat to cyber security and it's something that cannot be controlled by IT security staff.

Criminal hackers had to find another way to trick users into revealing personal information. As we start using more and more mobile devices, the potential for possible platforms increases. Additionally, if you use your devices at home and at work, you also put the university at risk when you are a victim of either phishing or smishing. At the university, there are thousands of staff and students using various devices, all at risk of being infected.

How do they do it?

Hackers have access to software that generates cell phone numbers based on area codes, they then plug into a cell phone service provider's extension and generate the remaining numbers with the software. By means of a mass email text message service, messages are distributed. Text messages will contain a link which installs keyloggers or link to malicious websites which harvests your personal information. Other text messages trick the receiver into calling numbers, leading to outrageous phone bills. (Also see the latest Wangiri scam) Yet another type will trick you into thinking you've subscribed to a service. When you try to unsubscribe, you'll be billed for using the service. Some text messages will download spyware which can see everything you do on your phone.

How to avoid it

1. Know how this kind of scam works. You'll be able to recognise it easier.
2. Don't reply to text messages from numbers you don't know, especially if it asks for personal information.
3. Even if it's a message from a friend, make sure it's legitimate. Your friend could have been hacked. Check with them first.
4. Install security on your phone, for example, a VPN, anti-virus and spyware.
5. Never install apps from text messages. Rather go to the app store where you know the software has been tested and verified. (e.g. Google Play)
6. If you're unsure if a text message is safe, don't open it.
7. If you didn't sign up for a service, ignore the message.

'Smishing' scams target your text messages. Here's how to avoid them from CNBC.

[SOURCES: www.webopedia.com; CNBC; www.bbc.com; www.norton.com; www.consumeraffairs.com; www.mcafee.com]

Posted in:Communication,Security | Tagged:Smishing | With 0 comments