Your Mobile Phone - Cybercrime and Smishing

Smishing is when someone tries to trick you into giving them your private information via a text or SMS message. The use of Smishing is soaring and is more of a danger than 'fishing' by email.

The reason? People trust text messages more than they do email, so they are more likely to succumb to the scam. Smishing has been around for years but because consumers have wised-up to email tricks and, in fact, are using email less and less for simple messages, scammers have switched their focus to SMS texts to target their victims.

The text usually contains a link that downloads malware, which steals as much data as it can find. And therein lies the threat: Your smartphone knows a lot more about you than your PC, so an installed piece of malware might steal the phone numbers in your contact list and spread the virus in hopes to exponentially multiply. Even important bits of personal data, like banking credentials or your tracking location, can be at risk.

Scammers are also using texts to pose as tax authorities. The tactic creates a false sense of realism because many people don't realize that text messages can be a threat. They say that the user is due a tax refund or needs to provide more information. Basically, they try to get users' information, and that can be used for stealing their money.

Research suggests as many as one in three smartphone users had been targeted by a Smishing attempt in just six months last year, although the actual number is likely to be higher since most people don't report scam attempts.

What to Do

The best thing you can do to avoid falling victim is to never click on a link inside a text message.

Certainly, you should never respond to a request for a password or other confidential information. Instead, visit the real website of the organization that seems to be asking and check if it's a genuine request.

You should also use extreme caution even if the message asks you to send the word "Stop" to stop receiving messages, as many do, unless you're 100% sure that it's genuine.

Sending a "Stop" message may not land you in immediate trouble but it signals to a scammer that there's a bite on the line.

In fact, for the same reason, you should never reply to text messages from someone you don't know. It simply opens the door for an onslaught of spam.

Block the sender if you can. But otherwise, just delete the message. And don't share your cell phone number on social media.

In addition, it's wise to install an anti-malware app on your phone.

To learn more about **Smishing**, and cybercrime prevention see www.getsafeonline.org

For further advice or if you believe that you have been a victim of fraud or cybercrime contact

Action Fraud on 0300 123 2040 or www.actionfraud.police.uk

Source – Based on an article from: www.scambusters.org