Safeguarding Against Fraud

Smishing

In computing SMS Smishing is **A FORM OF CRIMINAL ACTIVITY** using social engineering techniques. Smishing is the act of attempting to acquire personal information such as passwords and credit card details by masquerading as a trustworthy entity. This form of electronic communication will usually come via SMS and it is a type of **PHISHING ATTACK.**

How is it done?

This is a tactic which will leverage your trust in order to obtain information which once obtained will allow the "smisher" to use **YOUR** personal information to **THEIR** advantage.

A text will often include a link for you to click on and/or include a warning that if you do not take action then you will incur charges on a daily basis. In reality this is a tactic used to encourage you to respond immediately therefore removing any opportunity for you to assess the request fully.

The scammers may be attempting to obtain your details in order to **STEAL YOUR IDENTITY.**

Texts can also come from numbers which look to be genuine mobile numbers. It is also possible messages to come from numbers which do not look like phone numbers such as "5000". This means that the text message is actually just an e mail sent to a Phone. In reality this means you are simply just a number which reaffirms that this was not just intended for you…This is someone just trying their luck!

How can I prevent this?

BE WARY OF CLICKING ON ANY LINKS received in a text message even if it appears to have come from a friend. It may be they do not realise it is a scam.

Safeguarding Against Fraud

WATCH OUT for any form of contact which does not use your name but instead refers to you as a “valued customer”. This suggests that the contact has been made with many people and not just you.

Never install an app from a text message. If it’s a genuine App then it will be available from the official app store which means it will have to go through meticulous testing prior to being approved to be sold on there.

REAL BANKS WILL NEVER CONTACT YOU ASKING FOR PASSWORDS. They belong to you and should be kept private and confidential. No such occasion should arise where you need to reveal your personal passwords to anyone….**EVER!**

VICTIMS FIRST
Care | Empower | Recover

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Useful contacts

www.thamesvalley.police.uk Tel: 101 / 999
www.victims-first.org.uk
www.getsafeonline.org
www.actionfraud.police.uk Tel: 0300123 2040
www.ageuk.org.uk
www.cyberaware.gov.uk
www.citizensadvice.org.uk
www.nationaltradingstandards.uk

Please contact Thames Valley Police for more details via telephone dialling 101, or visit our website at www.thamesvalley.police.uk

STRONGHOLD
Fighting Organised Crime in Partnership

Protect Your World
STAY SAFE ONLINE

Produced by Thames Valley Police Economic Crime Unit