Safeguarding Against Fraud

Phishing

Phishing is the **FRAUDULENT PRACTISE** of sending e mails purporting to be from reputable companies in order to induce individuals Into revealing personal information, such as passwords and credit card numbers.

How is it done?

These **DIGITAL THIEVES** will “phish” for your card details online and by sending e mails which *appear* to be from a trusted payment source. When in reality it is the “phishers” attempting to obtain your personal details in any way or form they can!

The communication will often claim to be from banks providing a link to click on or from a well-known organisation claiming that if you click on the link you will win various items ranging from holidays to I Phones...All of which is untrue and just a trick to **GET YOUR ATTENTION** and your personal information.

It is also not uncommon for the scammers to claim that your computer has a virus and they need to take “remote control” and “add software” in order to combat this virus… This “software” does not combat anything apart from them **GETTING YOUR PERSONAL INFORMATION.**

How can I prevent this?

BE AWARE that banks or large organisations will never ask you to reveal your personal details over e mail. Although an e mail may appear to be from a genuine sender it is possible to spot the fakes if you know how!

Phishing e mails will often start with http:// instead of https:// which means it is a secure site. Banks or the Police will never ask you to withdraw or transfer money as part of an investigation.

Safeguarding Against Fraud

The thought of a free gift card is enough to stir anyone's interest but remember these large companies often have large budgets to cover their advertising campaigns meaning they do not need to come pleading to the general public to help them out! It helps to remember that there is no free gift card and this is yet again **JUST ANOTHER SCAM.**

BE AWARE OF POOR SPELLING AND GRAMMAR and remember that businesses and organisations will not use web based e mail addresses such as Gmail or Yahoo. Ensure that your spam filter is set on your e mails so you can mark any suspicious e mails as spam which will keep out similar e mails in the future.

Choose, use and **PROTECT PASSWORDS CAREFULLY.** It is paramount that electronic devices are kept up to date with the latest software in order to deflect viruses but never trust a source you have not verified.

BE AWARE that there are many scammers out there who will appear to have your best interests at the forefront of their minds especially when it comes to protecting your devices from malware attacks but the reality ,is that it is just a trick to convince you. Never under any circumstances click on that dodgy link no matter how may tempting it may be to do so…**IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT PROBABLY IS!**

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