•**TSB Phishing Attacks**There has been a sharp rise in fraudsters sending out fake text messages (smishing) and phishing emails claiming to be from TSB. The increase in the number of reports corresponds with the timing of TSB's computer system update, which resulted in 1.9 million users being locked out of their accounts. Opportunistic fraudsters are using TSB's system issue to target people with this type of fraud.Fraudsters are commonly using text messages as a way to defraud unsuspecting victims out of money. Known as smishing, this involves the victim receiving a text message purporting to be from TSB. The message requests that the recipient clicks onto a website link that leads to a phishing website designed to steal online banking details. Although text messages are currently the most common delivery method, similar communications have been reported with fraudsters using email and telephone to defraud individuals.Protect Yourself:

- •Don't assume an email or text is authentic - always question uninvited approaches in case it's a scam. Phone numbers and email addresses can be spoofed, so always contact the company directly via a known email or phone number (such as the one on the back of your bank card).
- •Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected text or email. Remember, a genuine bank will never contact you out of the blue to ask for your full PIN or password.

If you have received a suspicious TSB email, please do not respond to it, report it to us www.actionfraud.police.uk/report_phishing and also forward it to emailscams@tsb.co.uk If you have been a victim of fraud or cyber crime, report it to us online or by calling 0300 123 2040.