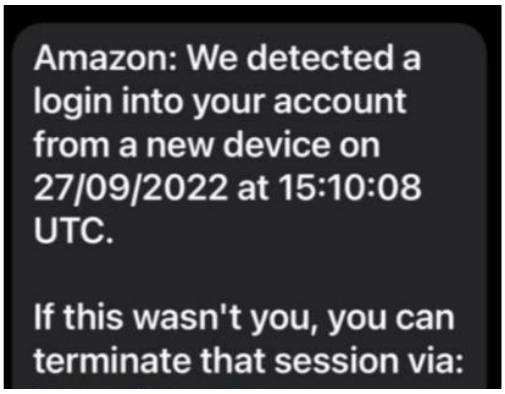
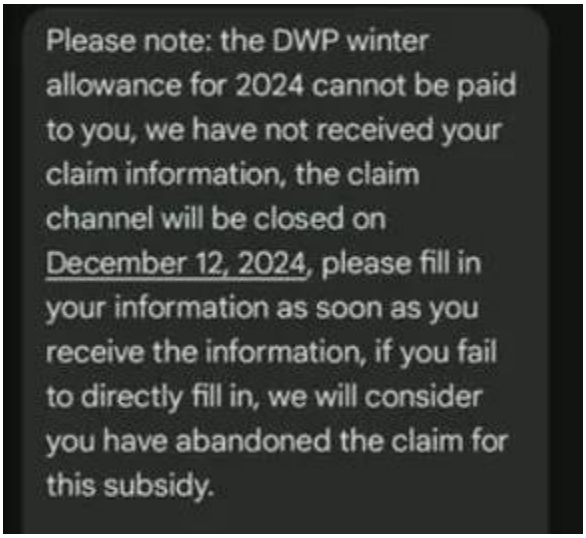
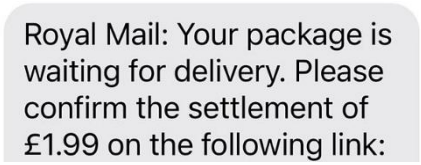
Beware of phishing texts and emails

This month, Fraud Protect Officers from Avon and Somerset Police want to make people aware of phishing texts and emails. Fraudsters can pretend to be anyone over text or email and they are often influenced by current affairs, such as Covid and the cost of living crisis. Here are some text message examples below where we have removed the links, but these could also come through via email.







When the victim follows the link, they will be asked for personal details such as bank/card information and passwords. However, just clicking on the link alone can result in malicious spyware or viruses being downloaded onto the victim's device.

Unfortunately, there is often a secondary part to these phishing texts, which is particularly sophisticated. It is known as "transfer into a safe account" fraud. The victim, maybe even a few days later, might be contacted by a fraudster, purporting to be from their bank. The fraudster will know who they bank with, along with other personal details, from the information harvested from the phishing text. They will claim that there has been fraud on their account and their funds are at risk, often referring to the phishing text. The victim, remembering the recent phishing text, is often convinced by the fraudster, feeling panicked by the thought of their funds being at risk. The fraudster explains that, to protect their funds, they need to transfer them into a "safe account". The bank details provided simply belong to the fraudster.

REMEMBER:

- Stop and think before responding to any email or text message
- Don't click on links unless you can verify where they came from
- Never provide information to anyone who contacts you out of the blue – take time to verify their credentials through a trusted source
- Just because a text or email purports to be from a government agency or organisation doesn't mean it is
- Forward scam text messages to 7726 (SPAM) and emails to report@phishing.gov.uk