Cybercrime Fact Sheet: Telephone Scams (Vishing) and Text Scams (Smishing)

Background

Social engineering attacks by phone

- One simple method of social engineering based attacks is "**vishing**", which is phone phishing used to gain access to **personal and financial information** for the purposes of **committing fraud**.
- Vishing is **low cost to initiate**, requires **little technical knowledge** and can **reach large numbers of people** through auto dial programmes.
- **High volume vishing** campaigns focus on getting to as many potential victims as possible. The use of Voice over Internet Protocol and auto dial means thousands of people an hour can be contacted.
- **Common Vishing attacks** usually use **fear to drive a response** for example an automated message advising of fraud on your account and a false number to call. When the victim calls the number the automated responses directs the victim to enter their account/ card details as well as perhaps their PIN, CVV and date of birth.
- When targeting organisations the attacker can often pretend to be another employee requiring urgent assistance, impersonating another more senior employee. They are normally in a rush and try to take control of the conversation.
- **Smishing** is similar to vishing in relation to the benefits it provides fraudsters but instead of relying on phone calls it is a **text message** requesting immediate action from the recipient.
- **Smishing** has become **more popular than vishing** with higher success rates and victims being conditioned to not receiving spam texts on their phones, therefore believing the message to be legitimate
- **Spam filters** will stop many phishing emails for example being received in a recipient's inbox, but there is **no** mainstream **solution for stopping spam texts** reaching their intended target.

What do organisations need to do?

- Train staff never to share financial or company information with unknown/ verified callers.
- Implement a policy and process for reporting cases of Vishing or Smishing.
- **Raise awareness** of the threats and how they **impact your business.**

What are the risks?

- Responding to either vishing or smishing attacks can lead to **financial loss** and in some cases **identity fraud.**
- Following links found inside a smishing attack can lead to **malicious Trojans** being put on your PC or mobile phone to **steal passwords** and other high value data.
- Bank customers are also targeted by "**Smishing**" as more and more people access the internet and their banking through mobile phones.

Key tips

Learn to spot suspicious calls and texts and:

- Do not be rushed into making a quick decision in response to an urgent request, ask yourself does this make sense, would this company/ bank contact me in this way
- Where the attack is purporting to be internal to the organisation there can be obvious clues that it is not a genuine call such as:
    - Referring to the organisation by name on a supposedly internal call
    - Calling the UK from one country for information on another. This could take the form of calling the UK from an airport in Singapore for information on employees in Japan.
    - Being told how to use internal systems to provide information
- Never provide personal or financial information over the phone
- Use known numbers rather than those provided by the caller or in the text if you are requested to contact an organisation
- Never click on a link in a text message that you were not expecting