Voice Phishing (Vishing)

Phishing is a technique used to gain information for malicious purposes. Often fraudsters use email to trick people into providing confidential information. However fraudsters also ring people to try and trick them and when they do, it is known as 'vishing'.

Vishing:

- Tricks people into sharing confidential information
- Calls appear to come from reputable organisations
- The fraudster sometimes tells you to an organisation on what looks like its usual number, but leaves the line open and intercepts the call, so all the information you think you're giving to the organisation is actually going to the fraudster.
- Fraudsters can mask the number that shows up on caller display so that the incoming call or text message looks legitimate

The Risk:

- Loss of information – customer, business, personal
- IT systems unavailable
- Financial impact to the business and to the individual
- Reputational damage

What to do if you receive a vishing phone call:

- Hang up and contact the organisation on a number you know to be legitimate on a different telephone line or allow at least five minutes for the line to clear.
- Phone the police non-emergency number 101 on a different telephone line or allow at least five minutes for the line to clear.
- Never give your PIN, bank card or bank details to anyone. Keep passwords and PINs safe – do not write them down and do not disclose them.
- The police and your bank will never ask for your PIN, bank details or cards. If you are contacted by someone who asks for these, hang up immediately.
- Ask for authentication e.g. ask the person at the other end of the line to verify a recent transaction you've made.
- Check statements regularly for transactions that you do not recognise.

What to do if you respond to a vishing phone call:

- If you have given away any of your company system usernames and passwords change your password immediately and let a member of the Information Security team know what has happened.
- If you have given away an online username and password contact the company (your bank, Amazon, Facebook, Twitter) immediately and tell them what has happened. If you use the same username and password for other sites change your password on those sites immediately.
- Report it to Action Fraud at http://www.actionfraud.police.uk/