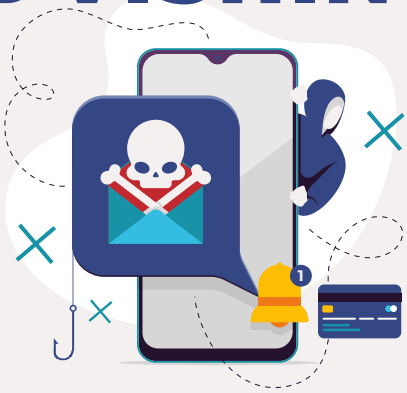
SMISHING AND VISHING

In today's modern world, it's more important than ever to keep your personal information safe and secure. Smishing and Vishing is when criminals send text or voice messages pretending to be from a legitimate organisation or from someone you know. Criminals use these types of attacks to try and gain access to your personal information.



Smishing and Vishing attacks

1. Verify who is making the request

Avoid providing personal information to anybody unless you are certain you know who you are dealing with. If you receive a suspicious message claiming to be from your bank, you should call the bank from a phone number you trust. This can be found by looking at the phone number on your bank statement or from the bank's official website.

2. Be wary of messages conveying a sense of urgency

If you receive a text message or a phone call that does not provide a lot of information and informs you that there is an urgent threat that must be addressed quickly this message is likely to be fake. Scammers will try to pressure you into taking a quick action without thinking. Always double-check that the request is genuine before proceeding.

3. Unexpected requests for personal information

A common sign of a vishing or smishing scam is a sudden or unexpected request for confidential information. In most cases a legitimate requestfrom a reputable organisation will not ask you to provide this information via text or from an unofficial number.

4. Avoid clicking on links within a message

Scammers do not always need you to reveal your sensitive information to gain access to your accounts. Sometimes their main goal is to trick you into clicking on a link and downloading malware or spyware onto your device. If your device is infected with malware, you can be susceptible to keylogging which will record your keystrokes and send confidential information to the scammer.

5. Treat messages with spelling and grammatical errors with caution

Legitimate organisations will hire experienced writers and editors to create and review messages before they are sent. If you receive a message with lots of errors or the message does not make sense this can be a sign of a scam.

6. Sharing personal information on social media can make you a target

You should be cautious about the information that you share online. It is common for people to post about travel plans, expensive purchases, and family members. A social engineer can use this information to create smishing and vishing attacks specifically for you. Before you post, think about what you are posting and who has access to it.