

What is Smishing?

Smishing is a form of Phishing. When someone tries to trick you into giving them your private information via a text or SMS message.

SMiShing is becoming an emerging and growing threat in the world of online security.



Smishing Attacks - Fraudsters

- *Credit card Fraud - Extortion*
- *'Bank texts' - Sensitive information*
- *'Breach' Threats - scare tactic*



Most people are aware of the security risks involved with clicking on links in emails. This is less true when it comes to text messages. Don't trust everyone.

How to prevent the attacks

In general don't reply to text messages from unknown sources.

Below are some specific steps to prevent smishing:

- Don't reply to text messages riddled with errors & mistakes.
- Don't click on any links or attachments within a text message.
- Never install applications that come through a text message, verify things first but always stick to the app store.
- If the preview looks dodgy, don't even open it, just delete it.



Almost all of the text messages you get are going to be totally fine. But it only takes one bad one to compromise your security. Not all texts are trustworthy.

ARE YOU CYBER SAFE?

How's your Network Security? Provide your business with peace of mind.

advoco-solutions.co.uk//it-services/network-security

ADVOCO
SOLUTIONS

Contact us:

contactus@advoco-solutions.com

0345 260 8801