Other Common Attack Types

Vishing, Telephone Scams

Phone scams, or vishing, are when a fraudster calls pretending to be your bank or another trusted organization. Nowadays with Artificial intelligence (“AI”) technology (e.g. Deepfake), image can be synthesized to create falsified videos. Besides, Deepfake has extended its application to sounds in which your voice can be mimicked by deep fake technique to create different conversations by capturing your voice of 5 seconds. With deepfake images and sound, one can fabricate videos that never exist. Fraudsters can even make their call appear to come from a number you know and trust or impersonate the voice of someone you know to direct your company to transfer money to a third person bank account. This is known as Phone Number Spoofing.

They can sound very convincing and may already know some of your personal information, such as your account number or address. If you feel uncomfortable, or sense something is wrong, don’t be afraid to end the call.

You can always call the organisation on a number that you know, such as the number on the back of your bank card.

Fraudsters can keep the line open and even spoof a dial tone, so try to use a different phone, or wait at least 30 seconds before making your call.

Typical examples include:

- ‘Your bank’ advise you that your account is at risk, and you need to move your money to another account to keep it safe.
- ‘Your bank’ needs your help to investigate a fraud.
- Your internet or mobile provider calls you to fix a problem you haven’t reported.

A bank can already transfer funds at your request and would never ask for your passwords, PIN, any One Time Passcodes or secure key code.