Allianz Hot Topic: Vishing, April 2021

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or indeed transferring money to them. Vishing style fraud against both individuals and companies has seen increased media attention in recent times. We felt this would be a timely awareness reminder to advise what to do if Vishing is suspected. Guidance from the Garda and Europol is as follows:

- Beware of unsolicited telephone calls
- Take the callers number and advise them you will call them back
  - Don't validate the caller using the phone number they have just given you (phone numbers may be spoofed and voices disguised with readily available technology).
  - In order to validate their identity, look up the organisations phone number and contact them directly.
- Beware - hanging up a call initiated by another party may leave the call open.
  - If you can use a different phone to call back, or if using the same phone try wait 5 to 10 minutes after the cold call - just in case they waited on the line.
- Fraudsters can find your basic information online (e.g. social media). Don't assume the caller is genuine just because they have such details.
- Do not share your password, credit or debit card PIN number or online banking password.
  - <u>You should not be legitimately asked for these details by anyone.</u>
- Do not transfer money to another account or update bank transfer account details without independently legitimating the request.
- If you think it is a bogus call related to personal banking, report it to your bank.

Allianz