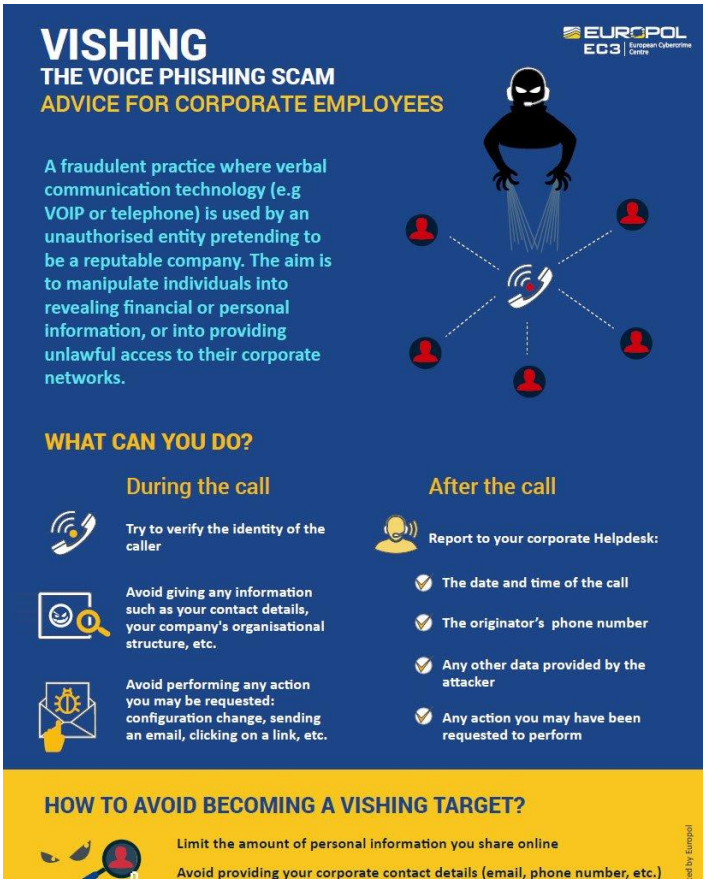
BEWARE OF "Vishing Scam"



Voice phishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward. It is sometimes referred to as 'vishing' a portmanteau of "voice" and phishing.

Vishing is a socially engineered technique used for stealing information or money from consumers using the telephone network. The term comes from combining "voice" with "phishing," which are online scams that persuades people to give personal information

If you ever receive a vishing call from someone claiming to be an employee of your bank, credit card company, or any other business - hang up. Then call the actual business immediately to report the incident. Be sure to call using only a reliable telephone number obtained from your local phone book or from your paperwork with that business.

The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account,

mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone,

What can consumers do to protect themselves?

- Be suspicious of all unknown callers. People should be just as suspicious of phone calls as they are of e-mails asking for personal information.
- Ask questions. If someone is trying to sell you something or asking for your personal or financial information, ask them to identify who they work for, and then check them out to see if they are legitimate.
- Call them back. Again, if someone is selling you something or asking for information, tell them you will call them back and then either verify the company is legitimate, or if it's a bank or credit card company, call them back using a number from your bill or your card. Never provide credit card information or other private information to anyone who calls you.

Things you and your business can do as well to fight back against vishing:

- Don’t answer your phone when you receive phone calls from unknown numbers.
- Don’t respond to unsolicited sales, marketing, or outreach messages.
- Don’t call phone numbers that are provided in online ads, pop-up windows, emails, etc.
- Register with a paid robocall blocking service.
- Educate yourself, your loved ones, and your employees about potential threats and scams. Teach them to hang up and call the person, department, or company directly using official phone numbers (such as from an official directory).
- Inform your company’s IT department about any potential scam calls or emails.

References:

https://en.wikipedia.org/wiki/Voice_phishing

https://www.pricecountywi.net/729/Phishing-Vishing-Smishing

https://www.cnet.com/news/protecting-yourself-from-vishing-attacks/

https://www.zdnet.com/article/protect-yourself-from-vishing-attacks/

https://www.thesslstore.com/blog/what-is-vishing-how-to-recognize-voice-phishing-phone-calls/