

Europol Vishing Scam

Voice phishing, or “vishing”, is a phishing attack conducted by phone. Vishing is a classic tactic that cybercriminals continue to use today. Recently, cybercriminals launched a vishing attack that impersonates Europol, the law enforcement agency of the European Union (EU). Using advanced techniques, cybercriminals disguise their phone numbers to display as an official Europol number on your caller ID.

The call starts as an automated message, stating that your personal data has been compromised and to press the 1 key to continue. If you press 1, you’re greeted by a real person who sounds polite and professional. The caller offers to help, as long as you give them information such as your name, address, and identification number. Any information you provide will be delivered straight to the cybercriminals.

Follow these tips to stay safe from similar scams:

- Never trust your caller ID. Cybercriminals can spoof phone numbers to look like a familiar or safe caller.
- If you did not initiate the call, do not provide personal information over the phone.
- If you’re not sure if a call is coming from a legitimate organization, hang up. Then, find the official phone number for the real organization and call them directly. Don't call the suspicious phone number again.