Voice Phishing

8 Warnings to Be Careful About

	① An unsolicited call	② A fake Caller ID	③ An immediate action required	④ An unsettling scenario
Stop.	Unsolicited calls can be malicious. Attackers often pretend to be from IT, HR or a person in authority.	Caller IDs can be fake and easily be spoofed to display a phone number of a genuine government, company or known person.	Scammers can use phony threats, and false promises to pry information from you in order to steal your identity or valuable information.	Attackers create scenarios to prey on emotions.
Think.	Be suspicious, especially if you don't know the caller and if he wants to help you by fixing an issue.	Be skeptical and evaluate the purpose of the call, especially if the caller is an unknown person claiming to be from IT, HR or a person in authority.	If it seems too good to be true or if you feel pressure to take an action, it most likely is an attempt to fraud you.	If the caller tries to stress or scare you, there is nothing to be shy about verifying the validity of their call (e.g., did you really forget to complete something, is there a problem with your computer or is a loved one truly in danger).
Act.	Be alert and don't give out any information. Take the time to verify the caller's identity by asking questions; legitimate callers will always answer your questions and give you time to reconsider a situation.	Be cautious, don't give out any information and take the time to verify the caller's identity.	Resist! Don't give out any information and take the time to question the legitimacy of the call. Report the incident immediately if you were victim of a threat or if you released personal or corporate information.	Don't get carried away by the stories and don't give out any information. Take the time to verify if it's true, and then answer or call back the official at a known and published number.

	5 A silent call	6 An unrecognizable voice	7 A recorded message	8 A request for access
Stop.	Silent calls are when the phone rings, you answer, and there's no one on the other line, and one-ring calls are when your phone rings once. By answering or calling back, you're confirming the validity of your phone number, making it ready for an attack.	Criminals can use voice changing tools to pose as a former colleague or a long-time friend who needs your support.	Robots send instructions, such as "Press 1 to speak to an operator" or "Press any key to be removed from the call list» to confirm that your phone number is valid. If you do so, it can lead to more automated calls and attacks.	Don't open the door to the scammers. If a caller insists that you enter your BDC credentials on a website provided over the phone or asks you to give them remote access to your computer, you are in essence divulging your password to a cybercriminal.
Think.	If the caller isn't talking right away or didn't leave a message, ask yourself if it's safe to take action to try to know who called you and why.	If the voice of the caller doesn't match the one you remember or if there is background noise making it difficult to recognize the caller, be vigilant! Don't forget that there is a lot of information available on social media that can be used to trick you.	Be suspicious and ask yourself if it's safe to follow instructions provided by a robot on an unsolicited call.	Think twice before agreeing to any unsolicited and unusual requests. We are all responsible to protect our credentials.
Act.	Hang up immediately and do not call back.	The best defence is to not automatically trust the caller and verify their identity. Call back the person using the known number.	Do not follow instructions and simply hang up or delete the voice message.	Ask to receive a ticket number by email (without providing your email) and wait to receive it from our usual BDC ticketing system before continuing the discussion, and don't provide information while you wait. Hang up and call back. If you provided your information, contact IT Service Desk and change your password right away.

Don't forget!

Be careful when responding to any type of request for information – what you provide may be the exact information needed by cybercriminal to perpetrate their next attack.