Email Phishing

8 Things to Consider

	1 Sender	2 Salutation	3 Urgency	4 Content
Stop.	Knowing the person whose name is on the email doesn't make it safe. Faking a name is easy and a common tactic of cyber attackers.	If emails say "Sir, Madam / Dear Client" instead of using your name, watch out! This can be a sign that the sender doesn't actually know you and that this is part of a phishing scam.	By providing a seemingly important reason (e.g. your account will be blocked, this offer is for a limited time only, your computer is vulnerable and needs an update), scammers try to create a sense of urgency to make you act rather than think.	Scammers can ask you for personal or financial information, or even your password—something no legitimate organization would ever do. Others will try to create an official-looking email by including logos of legitimate companies.
Think.	Does it sound legitimate or is it trying to mimic someone you know? Check the email address to confirm it's really from that person.	A sender who knows your identity should be sending you a personalized email and calling you by your name. Pay attention! Information from social media accounts leaves a digital footprint that criminals can use to appear convincing.	Be suspicious of words like "update quickly," "send the information within 24 hours" or "you have been a victim of a cybercrime." Don't fall for that! 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.	Is the design what you'd expect? Pay attention and look for errors! Also, ask yourself why you would receive such an unusual request by email.
Act.	Be alert and verify the sender's identity. Report the email as phishing if it seems to be fraudulent. If the sender pretends to be someone you know, inform this person. Avoid forwarding the email: if you need to transfer it to a colleague, send a picture of the email instead.	Verify twice and report suspect emails as phishing. They are either marketing or scam emails.	Don't give out any information and take the time to question the legitimacy of the email. Report the incident immediately if you were victim of a threat or if you released personal or corporate information.	Be cautious and don't click. Clicking is giving out sensitive information. If the request comes from a known organization or person, call the official number to verify the legitimacy of the request.

	5 Link or button	6 Attachment	7 Contact information	8 Report when in doubt
Stop.	Phishing emails usually contain a link or a button that, if clicked, will take you to a fake website or install malware.	When you open a scammer's attachment, you open the door to malware that can wreak havoc on your computer or even BDC's entire network. Some phishing emails may contain viruses disguised as harmless attachments that are activated when opened.	The contact information in scam emails can be fake, incomplete, or missing. Sometimes, only minimal information is provided to make you think they are legitimate.	Criminals send phishing emails to millions of people asking for sensitive information or containing links to fraudulent websites. Some may contain viruses disguised in attachments.
Think.	If it's unusual to receive a link from a specific sender, you can verify where it leads you by moving your mouse pointer over the link to show its full address.	Are you expecting to receive this attachment from this sender? If you aren't, even if you know the sender, it can be a phishing attempt.	Be skeptical and look for official contact information. Legitimate businesses always provide their corporate information in their signature.	If it seems unusual or too good to be true or if you feel pressured to take an action, it most likely is an attempt to fraud you.
Act.	Unless you can confirm the legitimacy of the link, don't click on it, and report the email as phishing. Best practice to access a website is to type its official address in a browser and then add it to your Favourites bar and access it from there.	Don't open it before verifying its authenticity. You can call or text the known sender, who will either confirm they sent it to you or realize they have been hacked.	If you don't know the sender, verify the contact information provided in the email by visiting the business's official website before dialing its number or responding to the email.	Trust your gut! Don't give out any information and take the time to question the legitimacy of the email. If you have doubts, report the email as phishing by using the *Report Message* button located on the right-hand side of the Outlook toolbar.

Don't forget!

- → Do not forward phishing emails to avoid increasing the risks.
- → Report phishing emails by using the *Report Message* button located on the right-hand side of the Outlook toolbar.
- → Be careful when responding to any request for information—what you provide may be the exact information needed by the cybercriminal to perpetrate their next attack.