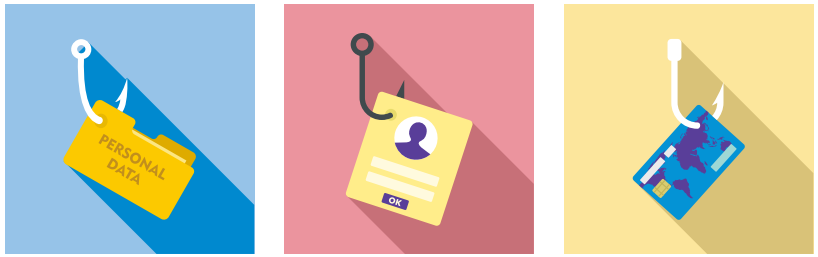
Phishing emails
Don't let them get you!



nixu cybersecurity.

Detect – 6 signs

1. A general greeting
If the message is addressed "dear customer" or in any other non-personal way, then be extra careful.

2. Bad spelling
Having unusually bad spelling errors can be a sign. Attackers don´t seem to care about grammar.

3. Weird sender
When in doubt check if the sender has a complete and active email signature.

4. Urgency
A sender who is demanding urgent action might push you to respond before thinking of the risk.

5. Asking about you
No serious companies ask for your personal information via email. If they do, call and double check that the request is legit.

6. Link or attachment
A phishing email usually has a link or an attachment that the attacker urges you to open.

Act – 4 steps

1. Take it easy
Usually, things go wrong if you're in a hurry. So take a minute to breathe and read the email carefully.

2. Hover, don't click
Hover over links before clicking. The infection may start when you click on the wrong thing.

3. Move to junk
If you are asked to send any critical or sensitive information by email, you can immediately trash the message.

4. Report IT service desk
Report every suspicious email to your company IT service desk. There are no unnecessary reports in this area.

Remember

- When your computer or other device is asking to be updated, do it! The more up to date your device is, the harder it is to attack it.
- Don't believe it just because you see it. If it seems phishy it might be just that.