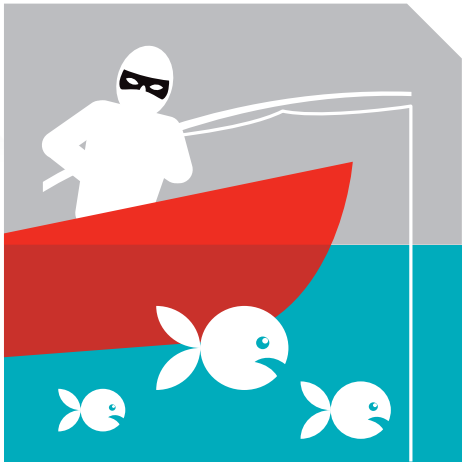
bsi. Phishing

Think before you click!



If it sounds too good to be true, it usually is.
Well-crafted phishing emails are designed to contain certain psychological triggers that encourage you to click

Be on the lookout for phishing themes
Cyber attackers love launching phishing campaigns based on current events. For example, tax season, major sporting events and the COVID-19 pandemic all saw huge increases in phishing traffic

Email tone
Phishing emails are designed to play on your emotions. Greed, urgency, curiosity and fear are all major motivators embedded in an effective phishing email

Do not click...
...on links, or open files attached to suspicious unsolicited emails. Always verify with the sender via phone

Be particularly aware...
...when files or email links direct you to websites requesting username and passwords, as these are often fraudulent and look extremely realistic

Impersonal phrases?
Does the email contain generic greetings?

Sender address looks odd?
Does the sender address match the name of the inferred reputable company?

URL too short?
Be aware that criminals use shortened URLs rather than using the exact URL – this makes the phishing URL less obvious. Roll the mouse over the link in the email to see the underlying URL.

Phishing awareness
Run regular phishing simulation campaigns for your employees

Configure your mailbox...
...so external emails are tagged with an "External Email" warning

Double check with your contacts
In the case of BEC (Business Email Compromise) attacks, it is important to verify requests for payments and updates to payment information.

Have you received a suspicious email?

If you do see any email that looks to be from an untrustworthy source, report it to your IT department and follow their advice. If you happen to click a link or download one, contact your IT department immediately as it will have protocols in place to remediate or solve the issue.