Phishing e-mails checklist

GENERALI

How to protect your personal details

E-mails from fraudsters who want to get their hands on your personal details, such as passwords, PINs and other ways to access your accounts, often look so much like the real thing that you get taken in. With a little care and the right knowledge of what to look out for, you can often recognise phishing e-mails from criminals for what they really are.

1. Be especially careful if you get an e-mail that you weren't expecting.
2. Phishing e-mails ask you for confidential details such as passwords, TANs, PINs, customer and access numbers associated with your own account number.
3. The e-mail is written in different fonts of differing sizes.
4. The e-mail has grammatical and spelling mistakes.
5. Accents are used wrongly or missed out altogether (in German names and words, for example, umlauts may be missed out, so you will see ae, oe, and ue).
6. You're addressed in an impersonal way (Dear customers of ABC Bank).
7. The concluding salutation is impersonal (Your ABC Bank).
8. A phishing e-mail is not addressed to you personally, but to a collective e-mail address (kunden@abc-geldhaus.ch).
9. The e-mail contains threats (e.g. of the account being blocked).
10. The e-mail has a form attached to it or contains a link to a form, in which you are called on to enter personal details such as your PIN, TAN, account number, customer and access numbers.
11. The e-mail contains a link which at first sight appears to be genuine, but some elements of the URL are written unconventionally or wrongly, which indicates that the website address is fake

Other things to look out for:

Never use a link sent to you in an e-mail, or a QR code that needs to be scanned in, to log on with a bank.

Always enter the address of your bank's signing-in page manually.

Don't fill in forms that are sent to you by e-mails asking you to enter signing-in information.

Don't divulge any confidential information during telephone conversations.