09.12.2021

Christmas time is phishing time

Extra caution is always required towards the year end. There's a long tradition of phishing mails over Christmas in particular. Due to COVID-19 and digitalisation, these are now even more wide-spread than ever.

Cybercriminals use phishing to obtain your access data, for instance for your e-banking facility or online shops. Protect yourself by ...

- never using any links you receive by e-mail, SMS or messenger services, and never scanning in any such QR codes to log into your financial institution facility.
- never filling in any forms received by e-mail and asking you to enter log-in information.
- treating any attachments received with e-mails and text messages with great caution.
- never disclosing any confidential information, such as passwords, during telephone calls.
- always entering the address for your online service provider or financial institution's log-in page manually via the browser address line.
- checking there is an SSL connection (https://, lock symbol) when calling up a log-in page, and verifying that the Internet address shown in the address bar of your browser actually indicates that you have reached the correct page.
- contacting your financial institution if you are not quite sure or something is not completely clear.