What is phishing?

Phishers fish for information of value.

Through fake emails, they try to fool you into

- **revealing your passwords or credit card data**
- **downloading a computer virus**

STOP | THINK | CONNECT™

Protect yourself!

- Never answer email requests for passwords, security codes, pin codes, etc.
- Only open email-attachments sent by addresses you trust.
- Be suspicious of any email that requires ‘immediate action’.
- Don’t trust emails with a general address, such as ‘Dear Customer’ or ‘Dear Sir or Madam’.
- Be suspicious of any email with grammar or spelling mistakes.
- Don’t trust emails that come from someone you know, but from an unusual email address.
- Is there a link? Hover your mouse over it and discover the true destination of the link.

Have you detected a phishing mail or website? Help make the internet a safer place and report the address to: **https://www.antiphishing.ch**

Cyber security is a shared responsibility!
https://www.stopthinkconnect.ch

UNIVERSITÉ DE GENÈVE · UNIVERSITÉ DE FRIBOURG UNIVERSITÄT FREIBURG · UNIVERSITÄT LIECHTENSTEIN · UNIVERSITÄT BERN · Hes·SO GENÈVE Haute Ecole Spécialisée de Suisse occidentale · FFHS Fernfachhochschule Schweiz Zürich | Basel | Bern | Brig Mitglied der SUPSI · Universität Konstanz · HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL FHO Fachhochschule Ostschweiz · Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN FH Zentralschweiz · SWISS INTERNET SECURITY ALLIANCE · EUROPEAN CYBER SECURITY MONTH · global IP action · Internet Society Switzerland Chapter · open systems · APWG www.apwg.org · SWITCH · STOP | THINK | CONNECT™ · eBanking but secure!

What is phishing?

The term ‘phishing’ comes from the word ‘fishing’. In contrast to fishers, phishers are not fishing for fish. Phishers fish for information of value. By definition, phishing is the attempt to steal sensitive data through tricking a person into revealing passwords or credit card data, or downloading a computer virus. It is a double loss, as the victim loses both their data and money.

Phishing attacks start with an email. A phishing mail may submit a tempting offer or demand immediate action to make you

- fill in a fake form
- click the link to a fake website
- open a malicious attachment

Often, they use logos of well-known companies to gain the recipient’s trust.

Be suspicious of any email that requires ‘immediate action’.

You might receive emails that tell you your (email, bank or any other) account will be deleted if you do not change your password immediately. And it’s easy – you can just use the form attached. Phishers try to build up pressure to trick you into taking an impulsive action. Remember, never answer email requests for passwords, security codes, pin numbers, etc.

Don’t trust emails with a general address, such as ‘Dear Customer’ or ‘Dear Sir or Madam’.

Phishing mails do not usually attack a single person – one email is sent to thousands of addresses to increase the chances of reaching someone who will fall into the trap. So most phishing mails start with a general greeting. Just keep in mind that if you are already a customer of a company or bank, it knows your name and would address you personally.

Is there a link? Hover your mouse over it and discover the true destination of the link.

Most phishing mails use a fake link to lure you into visiting a fake website or to install a virus on your computer. Those links are usually very long and often do not lead to the website the email indicates.

In order not to arouse suspicion, phishers use short links or a different link text. Thus, the real link is not visible – use your mouse to hover over it (do not click on it!) and the true destination of the link will appear. Check if it leads you to the website you actually want to visit.

Did you fall for a phishing attack?

Don’t panic – it can happen to anyone. Depending on the information revealed, you have some options:

- Get in touch with your bank and block your credit card or any transactions on your account.
- Contact the company or institution from which the phishing mail claims to be sent.
- Change all passwords that might have been stolen. If, for example, your email password has been phished, try to think which other passwords the phisher could discover with access to your email.
- Observe the actions on all your online accounts, such as Amazon, Facebook, etc, and report any suspicious events. Changing the passwords is always a good idea.
- Make sure your anti-virus program is up to date and initiate a virus scan on your computer.

Never answer email requests for passwords, security codes, pin codes, etc.

Neither your bank nor any other reliable company will ask you to send your password, security code or pin number via email. If you are not sure whether the sender is who they pretend to be, you can verify the request by

- calling the company or bank
- simply walking by
- sending an email to a known address (do NOT respond to the email in doubt)

Only open email attachments sent by addresses you trust.

Some files can install a virus on your computer just by opening them. So be careful not to open files attached to emails that seem suspicious. You may get an email with a bill for something you never ordered or a pick-up ticket for a ‘surprise’ parcel. Phishers know how to lure you into opening the attachment.

Be suspicious of any email with grammar or spelling mistakes.

General phishing attacks go for quantity instead of quality. Therefore, most phishing mails are not worded carefully. Some contain obviously bad translations and some just have spelling mistakes. Don’t forget that your bank and most companies are unlikely to send an email with poorly written text.

Don’t trust emails that come from someone you know but from an unusual email address.

Some phishing mails use a disguise to get through to you. You may see the logo of your bank or favorite brand. But is it the same email address that the bank or company usually uses? Check the sender’s address and compare it with the addresses you know.

Test your anti-phishing-skills with the phishing quiz from ‘eBanking - but secure!’ on

https://www.ebas.ch/phishingtest

Have you detected a phishing mail or website? Help make the internet a safer place and report the address to

https://www.antiphishing.ch

Cyber security is a shared responsibility!

https://www.stopthinkconnect.ch