# Phishing

**Attackers use phishing to obtain log-in data from unsuspecting Internet users, for instance to then access e-banking facilities or online shops. In the process, the attackers affect a fake identity, so exploiting their victims' good faith.**

**Protect yourself against phishing 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 TLS/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.

(https://www.ebas.ch/en/phishing-test/)

## A typical phishing attack

### 1. Contact

Criminals send out faked e-mails purporting to be employees of online service providers or financial institutions. The recipients of such e-mails are for instance informed that their account information or access data (e. g. user name and password) are no longer safe or up-to-date, and that they should be updated using the link stated in their e-mail.

### 2. Intercepting personal data

A link stated in their e-mail does not however lead to the original service provider page, but to a faked website, albeit a very authentic looking one. Personal information entered there, such as passwords, directly end up in the hands of the perpetrators.

**3. Gain**

Using the stolen information, the perpetrators then, for instance, carry out remittances from their victim's bank account, buy online at their cost or place faked offers with online auction houses.

For you to receive phishing mails, fraudsters have to know your e-mail address first. To reduce this risk and spam received into your inbox generally, it helps to follow some simple rules, to be found in our article on spam (https://www.ebas.ch/en/protection-against-spam/) .

Received a phishing mail?

Discovered a phishing page?

Report it now: www.antiphishing.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nationales Zentrum für Cybersicherheit
NCSC

(https://www.antiphishing.ch/en/)

*Phishing means the theft of information which is worthy of protection, for instance Internet user log-in information.*

*The term phishing is made up from the words "password" and "fishing".*

***Info sheet:***

Phishing

How to protect yourself against phishing attacks

Police and Swiss Crime Prevention –
an office supported by the cantonal
ministries of justice and police,
in co-operation with the University of
Lucerne and "eBanking – but secure!"

*(https://www.ebas.ch/wp-content/uploads/2019/10/phisingSKP_en.pdf)*

# Further information for anyone interested

### Classic phishing

With classing phishing, the attackers are trying to lure their victims to a counterfeit website with the help of a faked e-mail and to get them to enter their log-in information (for instance account number, password) there.

Alternatively or additionally, they may also add mail attachments containing a Trojan. Once this attachment is opened, it installs itself in the background, proceeding to capture Internet users' access details or directing them to fake websites.

Important to know: Financial institutions would never send out e-mails like that!

**Prevention**: Never click any links or attachments in e-mails, but always enter the financial institution's address into your browser manually, and check TLS/SSL connection and certificate (https://www.ebas.ch/en/checking-certificates/) .

### Spear phishing and dynamite phishing

In contrast to classic phishing which involves large amounts of e-mails randomly sent to a broad public, with spear phishing, recipients are specifically chosen and receive e-mails personally tailored to them.

Senders take the guise of a trustworthy person here, often posing as an acquaintance, employee or business partner of the recipient. The personalised e-mail contents seem credible and authentic and are therefore not even recognised by spam filters at times.

If such personalised e-mails are created automatically and sent out en masse, we also call this "dynamite phishing".

**Prevention**: Remain wary of unexpected e-mails or those with unusual contents, even if you think you know the sender. In case of doubt, contact the sender via a second channel, for instance by telephone.

### Smishing (SMS-Phishing)

SMS messages are increasingly used for phishing attacks, too. The perfidious thing about "smishing" is that most of the criteria suitable to recognise phishing e-mails cannot be used for SMS messages: There is usually no personal form of address. Language and design of these text messages are too simple and brief to allow any conclusions as to whether they are fake.  And on most mobile devices, it is rather difficult or unreliable to check the true sender and the link.  Many users are also used to receiving SMS messages to verify their e-banking log-in or before financial transactions are carried out.

**Prevention**: Never click on any links included in SMS messages, but manually enter the website address of your financial institution which you are familiar with into your browser. Then check there is a secure connection (lock symbol, target address). If you receive any unexpected SMS messages, contact your bank via the contact information you know (for instance their official telephone number) and have them confirm that they actually sent this SMS.

**Vishing (voice phishing or phone phishing)**

Vishing is the voice- or telephone-based version of phishing. Similar to classic phishing, a well thought-out story is employed to induce users to disclose confidential information, such as their log-in details for their e-banking facility.

**Prevention**: Never let other people know any of your confidential data, such as passwords. Immediately terminate any phone calls asking you for such details. Contact your financial institution only via their official telephone numbers.

**QR Phishing**

With QR phishing, attackers simply stick their own QR codes (Quick Response codes) over those displayed in frequently visited places and direct gullible users to a fake URL. This way, it is easily possible to execute scripts or show a faked financial institution log-in page, in particular on mobile devices.

**Prevention**: Never use any QR codes to log into any financial institution site. Before scanning any QR codes please check whether they have not been covered up by a fake one. Check whether the link points to your desired address.

**Phishing using websites in the attachment**

When phishing using websites, no link or document is included in the e-mail you receive – instead, there is simply an HTM- or HTML file containing a fake website in the attachment. Victims are fooled, since there is no link to click on. And at first glance, the attached file doesn't seem to be that dangerous either, as it isn't an actual document (Word, Excel) which could for instance run some macros.

But caution! HTM and HTML files can redirect victims straight to the attacker's server! Any log-in information then entered will end up in the wrong hands this way. In addition, such files can also contain scripts, which may just cause more damage.

Such redirects and scripts are blocked by the latest e-mail software for security reasons. If however you open such an HTM or HTML attachment, this is no longer controlled by the mail program's security settings. This is extra-perfidious, since even users aware of phishing in general are duped, since the browser address line "only" shows a local file path and not a dubious URL the way it is displayed with classic phishing.

**Prevention**: Please be wary of any HTM or HTML attachments in general. Don't click on any e-mail attachments, but always enter your financial institution's address into your browser manually.