

23.01.2026

Telephone phishing

Telephone phishing, also called “vishing” (voice phishing) is turning into an ever bigger challenge both for private individuals and companies. While Internet users are familiar with phishing e-mails or attempts at text message fraud, many underestimate the dangers posed by direct telephone calls.

What is telephone phishing?

Telephone phishing is a type of fraud where criminals contact victims by phone purporting to be employed by banks, authorities or well-known companies. Their aim is to obtain sensitive data such as passwords, online banking credentials, credit card data or TAN codes. To do so, the perpetrators use psychological pressure and frequently also “emergency” scenarios to trick victims into reacting on the spot. They tell some well thought-out stories to inspire confidence and then obtain confidential information that way.

How do these fraudsters proceed?

Modern attacks are often of a quite professional nature. They allow fraudsters to react in real time and inspire confidence. Their methods far exceed those of classic e-mail phishing attacks. The following approaches have been known to be used:

- **Fake phone number:** The number shown on the phone display appears legitimate, for instance your own bank’s telephone number (so-called “call ID spoofing”).
- **Fake identity:** Perpetrators pretend to be employed by banks, telecom operators, security departments or official authorities.
- **Authentic-looking scenarios:** It is for instance claimed that a fraudulent transaction needs to be stopped. To this end, you will have to disclose confidential data or visit a fake website.

Why is telephone phishing such a growing problem?

In accordance with the Bundesamt für Cybersicherheit (BACS), phishing incidents via the telephone have significantly increased in Switzerland. It is the combination of online data previously obtained via phishing, social engineering or data leaks with direct telephone contact which makes telephone phishing particularly dangerous.

This is how to protect yourself:

- **Do not disclose any confidential data over the phone.**
Account numbers, banking credentials, TAN codes or passwords should never be provided over the telephone.
- **Don’t react to the tyranny of urgency.**
Reputable companies will never ask you to make immediate decisions.
- **Check numbers.**
Never rely on the number displayed alone. Call back using known official contact numbers if in doubt.
- **Use official channels.**
Only ever contact your bank via the numbers quoted on your bank statements, their website or app.

Conclusion

Telephone phishing is no longer a future phenomenon, but reality. Your prudent behaviour though will ensure risks are significantly reduced. Remain vigilant, critically challenge any unexpected calls and only ever pass sensitive data on via secure, officially verified channels.

You can find further information on this topic in our article on [fraudulent support calls \(https://www.ebas.ch/en/fraudulent-support-calls\)](https://www.ebas.ch/en/fraudulent-support-calls).