13.03.2026

Beware of HTML phishing

There is currently a particularly treacherous type of phishing doing the rounds – HTML Phishing. Unlike classic phishing attacks, the faked login-page employed is embedded directly into an HTML attachment.

This is how HTML phishing works

In contrast to an usual phishing attack, e-mails contain an attached HTML file in these cases. Once opened, your browser will display a professionally designed and very credible-looking website. Users are then asked to enter their credentials here. In reality though, data are transferred straight to the attackers. In addition, such HTML files might contain scripts causing additional damage to your device.

HTML phishing is particularly dangerous because the fake website is opened locally and there is no typical web address shown in the browser bar. Many security filters have difficulty recognising HTML attachments, and their professional appearance considerably increases the message's credibility.

How to protect yourself

Make sure to always remain sceptical if you receive any unexpected HTML attachments. Credentials should only be entered on well-known, secure websites. In case of doubt, we recommend you check a message is authentic using official contact channels.

HTML phishing has been developed from classic phishing attacks and is particularly treacherous due to them combining visual authenticity with psychological pressure. Alertness, caution and consistent action are the most important means to preventing such attacks.

Further information (on other phishing variations, too) can be found here (https://www.ebas.ch/phishing) .