Fake letters from financial institutions

Time and again, fraudulent letters are circulating, purportedly sent by your bank and looking astonishingly authentic. But there are ways to unmask such fakes.

The most important points to remember:

- Always use your financial institution's official website or mobile banking app for all e-banking transactions.
- Verify the authenticity of letters received in the post – the same way you do for electronic communications – and report suspicious letters to your financial institution.
- Check the Internet address of any QR codes scanned in via your mobile phone camera before actually opening the link.

Fraudsters take great care to design fake letters to look as authentic as possible, complete with a correct-looking logo and professional layout. Their objective: To obtain sensitive information or credentials from their unsuspecting victims, for instance to then use them to unlawfully profit from logging on to their e-banking facilities.

A typical scenario: A QR code displayed in a letter leads to a fake website which looks just like your e-banking log-in page. You are then asked to enter sensitive information such as your credentials there. Criminals subsequently use this to obtain access to your accounts.

This approach mirrors the classic phishing (https://www.ebas.ch/en/phishing/) method, with one difference: Instead of sending an electronic message (such as an e-mail, text or Messenger post), they are mailing out physical documents. They frequently also put pressure on victims, for instance by pretending that their account is to be blocked unless they immediately carry out the action allegedly required to avoid this.

From an attacker's viewpoint, the use of QR codes offers the one big advantage that victims cannot at first glance see what kind of Internet address is behind the link coded into the mosaic image. Otherwise, their fake would be recognisable as such immediately.

You can unmask this scam by checking the Internet address shown after scanning the QR code with your mobile phone camera before proceeding to the actual website. Even better, you could always enter your financial institution's Internet address into your browser's address line manually or start your mobile banking app itself – which will ensure for certain that you end up with your bank's real e-banking facility.

Criminals fake written documents by reputable companies, for instance those sent by financial institutions, with sometimes very authentic results. Such letters will ask end customers to take some security-relevant actions. In this way, fraudsters are trying to obtain their victims' sensitive information or credentials.