PCWorld

Beware of this new phishing scam that could arrive in your mailbox

BY LAURA PIPPIG

Phishing scams don't just happen on the internet anymore.

If you think phishing scams only happen over the internet, you'd be dead wrong. In fact, there are many different types of phishing scams, including a recent type that occurs via traditional mail.

In Germany, the State Office of Criminal Investigation of Lower Saxony recently warned people about phishing attempts via mail in the form of fake letters that purport to come from their banks.

Some of these phishing letters look surprisingly close to the real deal, and some even contain personalized information. Complete with official logos, they give the impression that they're authentic.

Known cases have impersonated Commerzbank and Deutsche Bank, but any bank can be imitated—and it can happen all around the globe. Here's what you need to look out for.

HOW THIS MAIL PHISHING SCAM WORKS

The phishing letter informs you of "an important matter relating to [your] account," which can involve anything from keeping your data updated to scary warnings or threats that arouse panic.

Each letter is accompanied by a QR code and you're told to scan it if you want to move forward with a solution. You're led to think that this QR code is a convenient way to visit the bank's website.

But if you scan the code, you end up on a fake website that looks like the real website—and if you enter your details there, such as your login credentials, then your details

will end up in the hands of the hackers and fraudsters who sent you the phishing letter.

WHAT YOU SHOULD DO TO STAY SAFE

The German authorities recommend being particularly careful and suspicious of unexpected letters. When in doubt, you should call your bank to double-check whether the letter is legitimate.

Never scan unsolicited QR codes from anyone without verifying that they're trustworthy. Deactivate all options on your phone to "open links immediately" when scanning QR codes. This way, you can scan a QR code and see the destination URL before visiting, which can help you avoid deceptive websites masquerading as genuine.

If you end up falling for a QR code phishing scam (also called quishing scams), you should immediately inform your account provider (bank, credit card, online service) and have your account access blocked before changing all your passwords and restoring access.