M.M.WARBURG & CO
BANK

Cybercrime warning

Fraud attempts via digital communication channels are continuously increasing and therefore still require a high level of alertness.

Last updated:
18/09/2024

Cybercriminals are increasingly adapting to technical, regulatory and application-specific underlying conditions in a rapid manner.
The constant use of new methods, sometimes based on spying on personal behavioural patterns or data, necessitates a prudent and vigilant approach to digital channels and the required login data at all times.

Phishing: access data captured via email

Phishing involves, for example, a link in an email or text message redirecting targets to an authentic-looking website that sends their data straight to the fraudster once it has been entered or a message that asks you to send sensitive data by email to a fake email address.

Spear phishing and pharming: phishing 2.0

Further developments of this method include even more effective spear phishing, in which deliberately incorporated personal data of the target person and possibly the insertion of a fake email thread are intended to dispel doubts about the authenticity of the input interface, and pharming, which is based on the targeted manipulation of domain names in Web browsers.

Search engine phishing: remain vigilant when performing familiar steps

Search engines can also be manipulated and can lead unsuspecting users to fake pages, sometimes with the first hit. This often results in purported blocking messages or a prompt to reinstall. Here, too, sensitive data may be revealed and later misused. You should therefore always check the address of your online banking platform very carefully or bookmark it from the outset.

'Godfather': entire fake websites

In addition, the German Federal Financial Supervisory Authority (BaFin) warns Android users of malware called Godfather, which records data entries from banking or crypto applications. Godfather also makes use of professionally fraudulent websites and also sends fake push messages to gain access to authentication codes. It is not yet known exactly how the software reaches the end devices.

Fraud over the phone via grandparent and CEO scams

The popular grandparent trick (calling a supposedly close relative asking for short-term assistance in an emergency) and variants of the same are also still being perpetrated. The CEO scam is also repeatedly tried: here, a supposedly high-ranking/important person puts you personally under pressure to disclose data and 'not to ask stupid questions now.' Even fake bank employees or police officers appear again and again, urging targets, for example, to hand over cash and valuables for 'safekeeping'.

Current warning: 'booking not successful'

Beware of this current scam: after booking a hotel or ticket on a portal, customers are contacted with a deceptively genuine message claiming that there have been problems with the selected payment method. A link is also sent to enable the user to re-enter payment details, or the commu-

nication is redirected to a messaging service such as WhatsApp. The user is simultaneously put under time pressure: you are told that if you do not respond within a certain period of time, the booking will be cancelled. Caution: the link leads to a fake page, and the messages come from scammers. In this way, criminals try to get payment details or induce the customer to make a payment. Alternatively, it may be claimed that the payment method needs to be 'verified'. However, if the target follows the instructions, they actually trigger a payment directly to the fraudsters.

Only ever make payments via the platform through which you booked. Do not allow links to direct you to another website. The name is often very similar, but does not exactly match that of the original provider.

Do not respond to messages from strangers that you receive via messaging services. When you receive such a message, be aware that this is not the usual way for the company to contact you.

Current warning: reversal of a payment

Fake cancellation websites lurk for new victims with the following scam: if someone wants to cancel a booking and searches for information via a search engine, they are taken to a fake website. If you call the number provided there, you are taken directly to fraudsters, who pretend to be employees of the company and often ask for more sensitive information. In addition, you are instructed to download a specific application and enter the desired data there for a payment reversal. Instead of a cancellation and refund, however, further payments are actually triggered.

Current warning: update TAN procedure

Bank customers are increasingly being deceived by fake text messages instructing them to update their TAN procedure. A text message sent by fraudsters claims that the registration for the TAN procedure of a real bank has expired. The message contains a link for the alleged update of their registration. In reality, this link leads to a phishing website where customers are asked to enter their login details for online banking or TAN app, which will end up in the hands of the scammers. A bank will never send a request to update the security procedure by text message.

Current warning: QR code phishing bypassing security software

Quickly scanning a QR code (quick-response code) will take you straight to the menu in a restaurant, the login screen for booking a ticket or an invoice form. Caution: QR codes can also be misused for phishing attacks.

Cybercriminals, for example, send an email asking you to scan a QR code in order to open a document or invoice. The link then leads to a fake page, with the aim of intercepting personal data. Pressure to act quickly is often exerted here, too. IT security software, such as antivirus programs or the firewall, do not detect such phishing messages. QR codes are not recognised as attachments, but as images.

However, the following also applies to QR codes: only scan them from trustworthy sources and, if in doubt, do not open the link or enter the required data. If you are unsure, contact the sender by another means.

Current warning: cybercriminals using AI/vishing

Language programs that work with the help of artificial intelligence (AI), such as chatbots, can process text modules within seconds. Cybercriminals use such programs to correct phishing emails or adapt texts, making it even more difficult for the recipient to recognise their authenticity.

If in doubt, check the sender's email address for discrepancies. Alternatively, find the sender yourself via another access point on the official website or app. Make sure that the page starts with **https://** and that a website you already know is spelt correctly. Fraudsters often use a very similar Internet address to feign seriousness and trustworthiness. The fraudsters also use the capabilities of AI to mimic voices almost perfectly in the case of 'vishing' – a portmanteau of the terms 'voice' and 'phishing'. Such fake voice messages seek to deceive targets into divulging data or even transferring money directly to the criminals: 'I had a car accident, I need you to transfer money to me.' 'Your account has been hacked.' Here, you have to remember to stay calm and not reveal any personal details over the phone. If in doubt, ask for the telephone number and promise to call back. This buys time and allows you to check the phone number of the caller and the authenticity of the call.

Current warning: fraud attempts now also analogue/quishing

In what is known as 'quishing', you receive a deceptively genuine-looking paper letter that claims to be from your bank. The letter contains a QR code that you will be asked to scan to confirm your photo TAN procedure, for example. Again, your data can fall into the hands of fraudsters and, in the worst-case scenario, direct money transfers may result. Do not follow the instructions in these letters under any circumstances and, if in doubt, contact your client adviser.

Current warning: incorrectly displayed phone numbers/spoofing

In spoofing, attackers also try to create the appearance of trustworthy communication in order to gain access to personal data. In the case of 'caller ID spoofing', technical manipulation causes a different caller number to be shown on the display from the one used to actually make the call. This simulates a 'real' call, such as from your bank or an official body.

Don't let yourself be pressured on the phone! Your bank, the German Federal Financial Supervisory Authority (BaFin), Europol or the police will never press you to divulge personal data, such as bank account details, over the phone. You should end the call and then ring the bank and the police to clarify or report the matter. However, do not use the callback function of the phone, but manually dial the number you know. Also, do not accept offers for remote maintenance of your computer due to alleged threats or technical problems. You should also not comply with requests to pay money to a 'secure' account over the phone.

Current warning: fake social media messages

Anyone who has registered in a professional network knows the usual messages: 'You have been found in X number of searches' 'You have received a contact request or message'. These messages can also be replicated in a deceptively genuine way with the aim of gaining access to personal login details or redirecting users to a fake page.

Fraudulent emails can be identified by small errors, such as 'Linkedin' instead of 'LinkedIn', an unusual sender address or inaccuracies in text or logo. If you click on the fraudulent link, you will be redirected to a fake page that seeks to gain access to personal information such as your phone number. Once this is in the hands of the fraudster, an attempt will be made to obtain further personal data by means of targeted calls.

These scams can be transferred to other social media channels, whether Facebook, Instagram, X or messages from your email service provider. It should be kept in mind that every message may be a scam. And you should beware of clicking too quickly and carelessly.

Don't let yourself be pressured!

These fraud attempts often result in **artificial pressure being put on the user to act quickly**. Hybrid forms of cyberattacks and requests to call a supposed hotline are also becoming increasingly common. Professionally trained people then increase the pressure to disclose sensitive data in order, for example, to avert alleged damage.

Protect yourself and your data

Please always note that the bank and its employees will never ask you to disclose sensitive login data by email. Therefore, always be careful and follow the general security instructions for handling emails, e.g. at https://www.bsi.bund.de/DE/Home/home_node.html.

What to do if something has already happened

If in doubt or if you have already shared sensitive data, please contact your client adviser at the bank or via one of the following telephone numbers or email addresses immediately:

Online banking hotline (6 a.m. to 10 p.m. daily):
Free of charge throughout Germany: tel. 0800 72 33 982 / If calling from abroad: tel. +49 (0)40 3282 2332

General cross-bank girocard and Mastercard blocking hotline (around the clock):
Free of charge throughout Germany: tel. 116 116 / If calling from abroad: tel. +49 116 116

Email: service@mmwarburg-service.com

Please also note the following information/security recommendations:

Keep your devices up to date

Make sure that your firewalls and virus scanners are activated and always up to date.

Only download banking apps from authorised app stores

To download or update apps for your smartphone or tablet, please only use the authorised app stores (Apple: App Store / Android: Google Play Store). Do not follow prompts to download apps via email.

Do not store PINs, TANs or other login details

Passwords, personal identification numbers (PINs) and transaction numbers (TANs) should never be stored unencrypted in apps, the cloud or on your hard drive. Login details should also be changed regularly.

Check the bank websites

Before logging in, check whether you are really on the official website/official online banking platform. One way you can recognise this is by the 'lock' symbol in the browser and the URL starting with 'https'. If you are unsure, go directly via our website. You can find our online banking platform via the following link: https://www.warburg-bank.de/#/

Stay alert to cybercrime!

Banks never ask their customers to update sensitive data by email, text message or telephone. If a purported employee of a bank urges you to make transactions relating to your account, end the call immediately and contact your bank directly.

M.M.WARBURG & CO
BANK

www.mmwarburg.de/en