Fraud awareness

The fraud landscape is evolving rapidly, with new and more sophisticated tactics emerging quickly. It is crucial to remain vigilant and to take proactive steps to protect yourself and your business from becoming a victim of fraud.

The ongoing integration of UBS and Credit Suisse creates a unique opportunity for fraudsters to contact our clients claiming to be from our organization or selling fake investment schemes using the name of UBS entities. This could be a means to obtain information from you or to trick you into sending money to unrelated accounts. Please be vigilant if you are contacted by an unknown party. UBS, as part of our security measures, may require you to provide identifying information during the call-back verification procedure. However, we will not, under any other circumstances, ask for any sensitive information, in particular login credentials, e.g., username and password either by phone, email or SMS.

This note is designed to raise your awareness and offer practical guidance on staying secure against fraudsters.

Social Engineering – and AI-Powered Fraud

Fraudsters often use social engineering tactics to create a sense of urgency and emotional pressure to manipulate individuals into disclosing sensitive information or authorizing fraudulent transactions. By using Artificial Intelligence (AI), fraudsters can now generate realistic phishing emails, voice impersonations or chatbot interactions that mimic trusted sources.

- Watch out for unusual or urgent requests (e.g., to verify account details) received via email, phone, or SMS,
- Look out for poorly crafted emails or messages containing links or spelling mistakes.
- Check the authenticity of a request before sharing any information with people you do not know. If you have any doubts, don't click on links or download attachments until they have been verified.
- Always verify any new payment requests, and any requests you receive asking you to update existing contact details and/or bank details.
- Stay alert to fraudulent or unauthorized calls. Never share personal information like passwords, financials details, or authentication codes unless you have verified the request is legitimate.

Social Media and Synthetic Identity

Social media platforms are increasingly becoming a valuable resource for cybercriminals to gather personal information and create synthetic identities. By combining real data with fabricated information, criminals can establish fake identities that are difficult to detect.

- Limit the personal information you share publicly on social media, such as birthdates, home address, and travel plans.
- Be selective with your connections and only accept requests from people you know and trust.
- Regularly review your privacy settings to ensure you are sharing information only with trusted individuals.
- Monitor your online presence and perform regular searches to ensure no false profiles are being created using your information.

Digital Banking and Payment Fraud

The rise of digital banking and e-commerce has made online payment fraud more common. Cybercriminals are exploiting vulnerabilities in cardholder authentication processes, often using stolen or fraudulent card information.

- Ensure websites are secure before conducting transactions and the URL is correctly typed. A secure website will start with: https://
- Use multifactor authentication wherever possible. If not available, use strong and unique passwords and manage them in a password manager.
- Regularly monitor your accounts and set up alerts for any unusual or unauthorized transactions.
- Be wary of public Wi-Fi hotspots. Avoid using them for online banking, emailing, or updating social media, as hackers may be able to access your information.
- Only download software from trusted app stores and keep them up to date.
- Ensure your anti-virus and firewall software is current and is regularly updated from trusted providers.

Investment fraud

Fraudsters are increasingly targeting individuals and businesses through investment scams, especially in high-risk markets like cryptocurrency. They use promises of high returns or inside information to lure victims into fraudulent investments.

- Be cautious about unsolicited investment opportunities or "too good to be true" offers. Be suspicious of high-pressure sales. Treat any investment opportunities advertised online with skepticism. Do not entrust money to anyone who is not demonstrably acting on behalf of a trusted and regulated institution.
- Consult with a trusted and expert financial advisor before making significant financial decisions.
- Take time to research and verify any investment, never allow yourself to be hurried when investing.

By staying alert and following best practices, you can reduce your exposure to fraud and help protect your finances. If you suspect that you are victim of fraud or notice any unusual activity/transaction in your UBS account, please contact your UBS Client Advisor.