CREDIT SUISSE

Fraud Awareness Notification

The types of scams are evolving and becoming more sophisticated with technological advancements. Please remain vigilant and exercise good practice to avoid becoming a victim of fraud.

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

This notification is to raise awareness and to provide practical tips/guidance on how to protect yourself against fraudsters.

Social engineering – phishing, bogus calls

Emails and text messages let us share information with anyone in the world in seconds. But this comes at a price, cyber criminals can reach you just as easily. They try to steal your information via phishing emails, smishing (SMS, text messages) or via vishing (phone calls).

- Watch out for unusual or urgent requests you receive by email, phone or SMS (text message)
- Check the authenticity of a request before sharing any information with people you don't know. Never click on links or download attachments if you have any doubts
- Stay alert to bogus or spoofed calls. Never give information over the phone if you have any doubts about the authenticity of caller
- Be aware of spelling mistakes including check of email address to ensure it comes from a known source

Online browsing

The internet is all about connectivity. But how do you know the website you're visiting is legitimate, secure and free of malicious software.

- Only visit trustworthy websites and bookmark them. A secure website will start with https:// in front of the address
- Use multifactor authentication wherever possible. If not available use strong and unique passwords and manage them in a password manager
- Be wary of public WiFi hotspots. Avoid using them for online banking, emailing or updating social media, as hackers may be able to access your information
- Download software only from trusted app stores and keep them up to date

Social media – Sharing aspects of your personal and professional lives

Social media is all about sharing aspects of our personal and professional lives. So it can be a rich source of sensitive data for cyber criminals.

- Be mindful what you share and like
- Avoid posting (or including in your public profiles) personal information such as your date of birth, home address, contact details, holiday absences, and other details that may exploited by criminals
- Only add people to your network that you know and use privacy controls to limit who can see what

Investment fraud

- Do not entrust money to anyone who is not demonstrably acting on behalf or a trusted institution
- Discuss major investments with an expert
- Never allow yourself to be hurried when investing
- If something sounds too good to be true, it usually is not true
- Be alert when it comes to your finances
- Be vigilant and cautious when considering cryptocurrency investments
- Be careful about who you give access to your PC or your smartphone

If you suspect that you are victim of fraud or notice any unusual banking transactions in your account, please contact your Credit Suisse Relationship Manager or also email any security concerns to security@credit-suisse.com.