Tips to stay cyber safe

As the volume and sophistication of cyber-attacks in general grow, it's more important than ever to stay one step ahead of online criminals. The following tips can be paramount in protection your data, even in times of crisis:

1 – Be alert to phishing emails and bogus 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 the caller.

2 – Stay secure while being online.

- Only visit trustworthy websites and bookmark them. A secure website starts with "https://" and the "s" stands for secure. The data exchanged with the website cannot be intercepted or modified.
- Use multifactor authentication where possible. Otherwise use unique, smart passwords and manage them in a password manager.
- Only consult known, reputable sources for updates on world events and donate through official channels.

3 – Be wary of public Wifi and downloads.

- 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.
- Only download software from trusted app stores and keep them up to date.

4 – Be careful what you share.

- Be mindful what you share and like on social media.

- 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.

5 – Stop. Think. Act.

- Stop, if something doesn't seem right.
- Think about the risks.
- Act securely in all your digital interactions.

Remember: UBS never contacts its clients by phone, email or SMS to ask them to log in or reveal their access, account details. We don't send emails with links to login pages such as e-banking contract number or PIN.