UBS

Cybersecurity

Follow these steps to minimize your risk of becoming a victim of cyber-crime.

Cyber fraud has increased exponentially over the last few years and it is no longer a question of whether you'll be targeted by cybercriminals, but when. It is important that you are prepared and protect yourself as much as possible from this growing threat.

E-mail compromise	Your e-mail or an associate's e-mail is spoofed or hacked and used to trick you or your bank into making a payment.
Viruses	Malicious programs that attach themselves to authentic programs and run without permission on your computer or device.
Social engineering	Criminals convince you to provide your personal or financial information under false pretenses, often by posing as someone else.
Phishing	Cybercriminals use e-mail to try to lure you into revealing your personal or confidential information by clicking a link or an attachment.
Identity theft	The unauthorized acquisition and use of someone's personal information, usually for financial gain.
Ransomware	A malicious program that blocks access to your computer, device or data, and demands that you pay a ransom to regain access.
Deepfakes	AI generated images and video of co-workers that are indistinguishable from the real people.

Key action steps

– Make sure you always stop and consider each e-mail you receive and call back the sender on a known number if something seems unusual or pressured in the request.
– Avoid opening e-mails from unknown senders, downloading unexpected attachments or clicking on unfamiliar links.
– Use strong passwords and avoid sending personal or confidential information on unsecured networks.
– Secure your computer and devices by installing security patches and anti-virus protection.

Real World Examples:

Business E-mail Compromise (BEC)—E-mail requests for order placing of fund transfers

– A fraudster impersonates your business partner's e-mail (e.g., JoeVVright@gmail.com as supposed to JoeWright@gmail.com) and sends a last minute request for you to make a payment to another bank account.
– Rather than responding to the e-mail request, use an alternative channel or known contact number to verify the request.

Tech Support Scam (e.g. Acting as Microsoft Tech Support)

– A current live scam that is prevalent globally relates to fraudsters spoofing the incoming telephone to appear to be the official tech support team of a reputable tech company. The bad actor then uses social engineering skill to install malware and hijack your e-banking account to disburse payment(s).

Deepfake Video

– An emerging scam that uses AI generated video of senior managers in the target company that are so realistic they convince staff to perform false (and costly) transactions.

Browse the web and check e-mail securely

- ☐ Avoid using public computers or Wi-Fi hotspots when sending personal or confidential information
- ☐ Only shop with reputable online vendors, and use credit cards or PayPal (not debit cards)
- ☐ Be careful about what personal information you make publicly available and send it only on secure websites ("https")
- ☐ Learn to recognize phishing; never open unfamiliar attachments or click on unfamiliar links
- ☐ Ignore e-mails or text messages that ask you to confirm or provide personal information by replying to the e-mail or message
- ☐ Use the filtering settings on your internet browsers and search engines

Manage your social media activities

- ☐ In your profiles and posts, avoid publishing personal information that is typically used for security or verification purposes, such as your full birthdate or your mother's maiden name
- ☐ Use privacy settings to control who can access your information, and review your privacy settings regularly
- ☐ Accept friend requests only from people you know; only "follow" (not "friend") entities or public figures
- ☐ Be wary of sharing your current location or future travel plans; never announce when you won't be home
- ☐ Be careful about taking online polls or quizzes or downloading apps that allow the organizer to access your account or data on your devices

Strengthen your passwords

- ☐ Create passwords that are at least 6 to 15 characters long
- ☐ Use a combination of special characters, numbers and upper and lower case letters, passphrases or password managers
- ☐ Avoid including personal identifiers, such as names or birthdates, in your passwords
- ☐ Store your passwords securely and change them regularly, at least once every 3 – 6 months
- ☐ Do not use the same password for all of your accounts
- ☐ Use multi-step authentication procedures whenever possible
- ☐ Do not allow "auto-save" of your passwords

Be suspicious

☐ If something seems oddly urgent, strange, or unusual, do not trust and VERIFY the source

☐ If you are asked to join an impromptu or unexpected video call with a senior manager for a large, urgent, or secret transaction, follow all procedures to verify that they are who they say they are, especially if they try to convince you not to

Protect your computer and devices

- ☐ Use a strong password and biometrics when available to access your devices
- ☐ Set your computer and devices to auto-lock after a short period of inactivity
- ☐ Set all computers and devices for automatic software updates
- ☐ Install up-to-date security software with anti-virus, anti-malware and identity protections
- ☐ Avoid keeping financial and confidential information on your devices unless necessary
- ☐ Use file encryption for personal information that must be stored on your devices
- ☐ Keep a copy of critical data on a separate, secure medium (e.g., an encrypted external hard drive)
- ☐ Do not allow text messages or caller ID to appear on your locked screen
- ☐ Make sure you completely erase your hard drives prior to disposal
- ☐ Make sure that an owner's permission and password is required to access your home Wi-Fi network and that it is password protected and secure
- ☐ Create a security PIN to access your device
- ☐ Turn off location services and unnecessary apps on your devices
- ☐ Do not store or send personal or confidential information via e-mail or text
- ☐ Monitor your phone for unusual activity (texts you did not send, unusual pop ups or higher than normal battery usage)

Monitor financial statements and credit reports

- ☐ Request and review credit reports from each of the three national consumer reporting agencies regularly
- ☐ Review your bank and credit card statements regularly, and look out for suspicious activity or unfamiliar charges
- ☐ Review your Social Security Administration records annually
- ☐ Go through your health claims carefully to ensure you've received the care for which your insurer paid
- ☐ Remove your name from marketing lists, including for the three credit reporting bureaus (Experian, Transunion, Equifax), to prevent unsolicited credit offers
- ☐ Sign up for identify theft protection products or services, as appropriate for you
- ☐ Place a fraud alert on your credit files if you are concerned that your personal or financial information has been compromised or misused
- ☐ Freeze your credit to block new credit cards, loans or credit lines being opened without your consent