Information Security
Learn how to protect yourself by following the tips below.

Computer security

Ensure that the latest software and security updates are installed on your PC and mobile devices on a regular basis, or even automatically if supported by the software. Keep your antivirus software active and up-to-date by scheduling regular scans of your computer in addition to real-time scans. However, keep in mind that antivirus software is no substitute for common sense. Install a firewall on your computer to add an extra layer of security when your device is connected to the internet. Set your device to require a passcode for each user's access, and choose to turn off your computer instead of using sleep or idle functions. Prevent strangers from gaining remote access to your computer

Email security

Be careful when receiving suspicious emails, especially if they contain attachments or links. They may redirect you to a site other than the one listed in their tags. Ignore emails that ask for sensitive information such as account numbers, passwords, credit card details, etc. If you receive an email asking you to register or verify your personal information about KOPES BANK, do not reply as this is a scam. Please forward any suspicious messages to: support@kopesbank.com If you believe that there is a possibility that you have provided your personal information in any way, please call us immediately at +41 22 886 02 29 Password security Keep your internet/mobile banking passwords private. Never leave them open in places where someone else can easily access and use them. Try using a different password for each site you access instead of using the same password on multiple sites. Disable autofill and save passwords provided by browsers. Change passwords frequently.

Account Security

Check your transaction history regularly so that they can be identified. Do not leave your account inactive for a long time. Turn on email or SMS notifications for specific activities on your accounts so you can immediately identify any suspicious activity. Make sure that the mobile phone number registered with KOPES BANK is the one you are using. Internet security Make sure you only provide sensitive information about your online banking activities to sites that use encryption. (https instead of http - the "s" stands for "secure".) Avoid using shared computers/Wi-Fi in public areas for online banking. When banking information is obtained through such computers/networks, this information may be stored in the computer's memory. Log out of the online banking application you use when you terminate your business. It may not be enough to simply close the browser window. Be careful when the website ID (block) button displays warnings or errors. However, the confidentiality and integrity of the information provided is not guaranteed. Ignore any pop-ups that ask for your passwords, warn you about viruses, or that your antivirus software has expired. Be careful about sharing your personal information on social media. They can be used to misuse or obtain your passwords online. Set up Wi-Fi in your home to require a password for users. Follow the manufacturer's instructions. Make sure you have access to online/mobile banking applications through the KOPES BANK official website/app

Mobile Security

Set your mobile device to automatically lock if it has not been used for some time. Be careful not to leave your device unattended in public places. Keep it in a safe place. Be sure to uninstall the mobile banking app before replacing the device with a new one. Use the exit button every time you end your online banking business. Increase your security by using multi-factor authentication products provided by the Bank. Disable Bluetooth when using internet banking. Avoid rooting/jailbreaking your device to prevent any deviation from the security controls implemented by the operating system.