Theft or loss of the *smartphone*

Prepare and don't panic

RISCCO | January 24, 2023 | 8 minutes | 981 words

Content

- Risks of theft or loss of the *smartphone*
- Prepare and adopt good prevention practices
- Tips on what to do if your *smartphone* is lost or stolen

1. Risks of theft or loss of the *smartphone*

For many, the smartphone is almost an essential item. The theft or loss of a smartphone generates stress or anxiety. It is not just losing photos-videos of family gatherings, but also disconnecting from the digital world and becoming a fraud victim.

On the next page, we list some risks of theft or loss of the smartphone:

Some risks about the theft or loss of the *smartphone*

1. Criminals can access data, photos, videos, audio, personal conversations, and credentials to online services. Being the victim of identity theft and/or being extorted for your smartphone's content.

2. They can impersonate your identity to your family, friends, work collaborators, and/or customers.

3. Criminals will be able to access the online services on the Internet that you usually use, if the services can be accessed automatically from your *smartphone*, allowing them to make unauthorized purchases. They could also access your login credentials if you have saved them in notes or photos on your phone.

4. Impossibility of timely access to online services (shopping, online banking, etc.) if you only have the smartphone enabled as the only second-factor authentication option (2FA).

5. Inability to access your email account. This is critical because most online services use your email account to confirm a password change, authorize a transaction, etc.

Having the "auto-lock screen" enabled is not a guarantee that the criminal will not have access to the smartphone. The criminal will try to steal your phone while you are using it, allowing criminals to disable the "auto-lock screen" option and gain access to the smartphone.

2. Prepare and adopt good prevention practices

1. Enable a password to access the smartphone, either a PIN or biometric mechanism. If you use Android smartphones, preferably not define a predictable pattern like the letter “M”, “L”, “C”, “S”, and “O” (see image to the right).

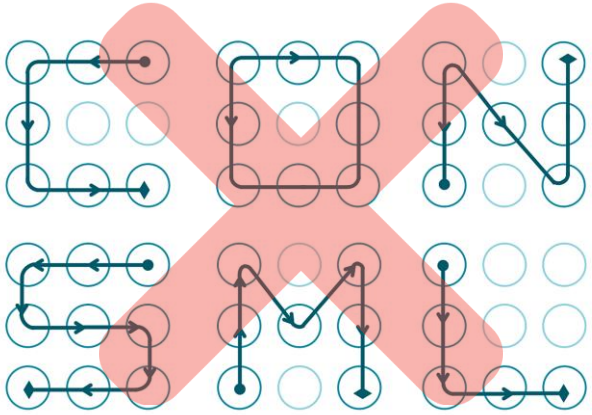
2. Enable the “auto-lock screen” option to activate in a minute or less.

3. Enable the “Find My iPhone” (iPhone) or “Find My Device” (Android) option and memorize the login credentials.

4. Have the customer service phone number accessible (not on your smartphone) to cancel/suspend: a) your phone line; b) your credit cards; c) online banking.

   In addition, memorize the iCloud (iPhone) log in credentials and their Android equivalent.

5. It makes sense that someone close to you has the information of point #4. Memorize that person's phone number so you can call them.



Make regular backups of the contents of your smartphone.


Facing the theft or loss of a smartphone, every minute counts. Being prepared and acting fast can be the difference between having a hard time or being a victim of financial fraud or extortion.

3. Tips on what to do if your smartphone is lost or stolen

a) Access the “Find My iPhone” (iPhone) or “Find My Device” service from the phone or computer of a trusted person and:

   1. Check if your smartphone is still close to where you are.
   2. Activate the “play sound” option. Even when the phone is silent, the sound will be heard for at least for two minutes.
   3. Lock your *smartphone.*

b) Change the password of the email accounts set up on the smartphone.

c) Call from another phone to your smartphone. It may be that it is nearby or that someone has found it.

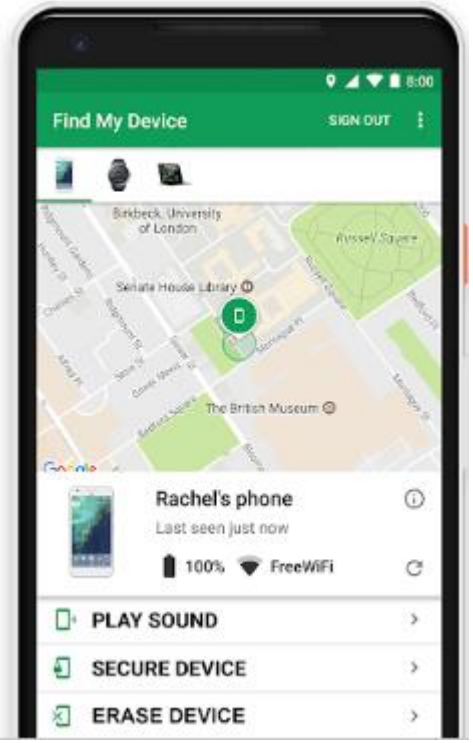
d) Contact the customer service of your telephone operator; Credit cards; online bank; and suspend/cancel the service.

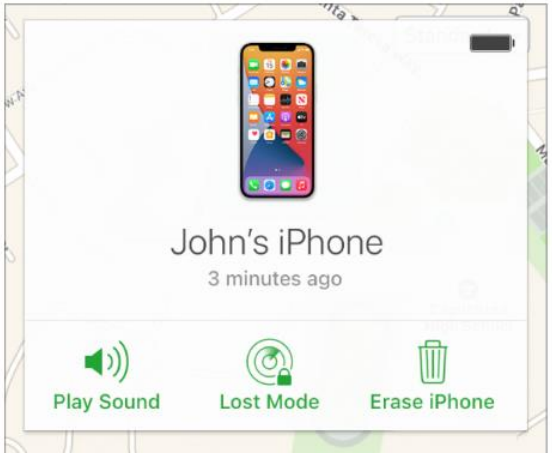
3. Tips on what to do if your smartphone is lost or stolen

e) Change the iCloud login passwords (iPhone) or its Android equivalent.

f) Access the “Find My iPhone” (iPhone) or “Find My Device” service and try to remotely wipe the contents of your smartphone.

g) If you find the smartphone some time later, it is recommended that you wipe the data and reset the smartphone to factory settings. There is a possibility that some malicious program has been installed on the phone.





CONTACTS

Panama and CARICOM

Antonio Ayala I.
aayala@riscco.com

Rubén Fernández
rfernandez@riscco.com

Dominican Republic and Puerto Rico

Rubén Fernández
rfernandez@riscco.com

Costa Rica and El Salvador

Roberto Delgado
rdelgado@riscco.com

Guatemala, Honduras and Nicaragua

Roberto Delgado
rdelgado@riscco.com

riscco.com

RISCCO It is an independent regional company dedicated exclusively to helping organizations face their challenges in GRC (Governance, Risk & Compliance) and ESG (Environmental, Social & Governance); composed of professionals with the necessary knowledge and credibility to translate highly technical aspects into simple language with business sense. With fourteen (14) years of having started operations, RISCCO has in its client portfolio private companies and Government Institutions in the region, leaders in their field.