

# CYBER THREATS AWARENESS BOOKLET



**LEBANESE INTERNAL  
SECURITY FORCES**

PUBLIC RELATIONS DEPARTMENT

SERVICE - TRUST - PARTNERSHIP



# Table of Content

## Page

1- Introduction	4		
2- Objective	6		
3- Types of cybercrime	7		
3.1- Cyber Extortion	7		
3.2- Phishing	8		
3.3- Identity theft	9		
3.4- Cyber-bullying	10		
3.5- Hacking	11		
3.6- Ransomware	11		
3.7- Business Email Compromise Fraud	12		
4- Protection from cybercrime and cyberthreats	13		
4.1- Protecting Accounts and Applications from Internet Risks	13		
4.1.1- Creating a strong password	14		
4.1.2- Protection of Social Media Accounts (Instagram, Twitter, Facebook, LinkedIn, Snapchat ...)	16		
4.1.3- Protection of Email Accounts (Yahoo, Hotmail, Gmail ...)	18		
4.1.4- Protection of messaging applications (WhatsApp, Skype, signal, Telegram ...)	22		
4.2- Protection of children online	24		
4.3- Electronic devices protection measures	29		
4.3.1- Desktops and laptops protection measures	29		
4.3.2- Smartphones and Tablets protection measures	32		
4.4- Protection Measures of Wi-Fi Networks and the Devices connected to it	35		
4.4.1- Public Wi-Fi	35		
4.4.2- Private Wi-Fi	37		
4.5- Protection Procedures for Electronic and Financial Transactions	38		
4.5.1- Protection Procedures for electronic banking transactions	39		
4.5.2- Protection Procedures for online shopping	42		
4.5.3- Protection Measures against Financial Fraud via Business E-mail "Business Email Compromise"	44		
5- How to deal with cybercrime	46		
5.1- How to act when smartphones and portable devices are lost or stolen.	46		
5.2- How to Act When you are a Victim to Cyber extortion	48		
5.3- How to Deal with Cyber bullying	50		
5.4- How to deal with stolen accounts of various social media sites, text messaging applications or service providers	51		
5.5- How to Act When Devices Are Infected with malware	54		
5.6- How to Act When Devices Are Infected with Ransomware	56		
5.7- How to act when a credit card is lost or stolen.	60		
5.8- How to act when you are victim to online bank fraud	61		
6- Contacting the Internal Security Forces and requesting help	62		

# 1- Introduction

The ongoing technical development, especially in the Information Technology and Telecommunications field, has turned the world into a global village through the internet. It allowed the development of many computer programs including chat applications, social media platforms, and many other applications that brought people closer to each other and allowed them to communicate instantly by exchanging messages, pictures and data, as well as providing various online services that help to accomplish all kinds of electronic transactions.

On the other hand, new types of crimes have appeared, that take advantage of Information Technology to accomplish new form of crimes or traditional crimes but with new methods and techniques. In addition, cyber threats have become a huge issue by increasing the crimes related to hacking and stealing of the personal data of individuals and entities, and threatening the information infrastructure of vital systems and networks at the state level. Therefore, it become vital to raise awareness about threats and risks related to the internet, including identities theft, stealing accounts' credentials, data hacking, cyber extortion, etc. along with adopting the best practices regarding safety and protection, and enhancing the necessary security measures when facing such situations.

Due to this fact, it's imperative that the Internal Security Forces, as part of its national duties and responsibilities, provides protection to society members against all kinds of risks particularly from cybercrimes and cyberattacks. ISF is fully committed to fulfill this duty and take this responsibility by working to provide the protection needed on the internet, securing the Lebanese cyberspace and raising public awareness while carrying out all the necessary investigations to identify cyber criminals, arrest them, and bring them in front of the respective judicial authorities while keeping these investigations confidential, and respecting personal privacy and human rights standards.





## 2- Objective

This guide aims at raising awareness of all society members about the most significant cyber threats and cybercrimes, and at enhancing protection and personal privacy when connecting to the internet and benefiting from digital services.

Furthermore, this guide highlights the preventive measures and the best practices that should be followed to protect the information and personal data against theft, to prevent hacking of electronic devices, to avoid being victim to cyber extortion, and finally to help children and other family members staying safe on the internet.



## 3- Cybercrimes Types

With the increased reliance on electronic devices, specifically smart phones and mobile devices, to connect to the internet and using the online applications and services provided by various governmental and private institutions, these devices became the target of many cyber-attacks such as information theft, extortion, sabotage, profiting, or defamation. Below, we highlight the main cybercrimes that have recently emerged:

### 3.1- Cyber Extortion

Cyber extortion is the act of threatening and intimidating a victim by posting photos or videos, or leaking confidential information that belongs to him or to one of his/her family members, in order to make him/her pay amounts of money or exploit him/her for sexual, unethical, or illegal purposes for the benefit of the extortionist. Cyber extortion affects the psychosocial status of the victims to an extent that makes most of them hesitant to report such crimes fearing that their videos or any other material gets posted. They are also worried about the perception of the society towards them not to get damaged or affected. Therefore, they tend to succumb to the extortionist demands and transfer money or hurt themselves, and sometimes commit suicide!



### Following are some examples of extortion cases:

- a. Saving copies of videos, recordings, or personal or sexual photos captured during an online conversation and threatening to post them in exchange of money or sexual demands or others.
- b. Stealing personal or family photos and data from a mobile phone undergoing maintenance and blackmailing the owner.
- c. Deluding the victims by pretending to know the websites that they surf and blackmailing them by threatening to post them.

## 3.2- Phishing

Phishing is one of the manipulation techniques often used to steal users personal data like their sign-in information , passwords, phone numbers, credit cards numbers, and others. For example, cyber criminals create a fake website that looks like an original website (e.g. a website called **faceb00k.com** instead of **facebook.com**) and then they send the fake website link to the victims through emails or social media platforms, pretending that it is coming from a trusted source (e.g. from the company or the website that the victims deal with) and, relying on different techniques, drive them to click on that link. In this case, victims get directed to enter important personal information about themselves, which can be used later by hackers to commit fraud or illegal access to the victims' accounts, or install malware on their devices to steal information or just for sabotage.



## 3.3- Identity Theft

It is a type of fraud that occurs when a person uses the personal identification information of another person without his/her consent, such as the name, passport number, identity card, driving license, credit card, electronic account details or even a personal photo, with the aim of committing fraudulent acts, stealing money and credit cards, or just causing damage and discrediting the reputation.

### Some of the most prominent examples of identity theft include:

- a. Theft of private accounts on social media services (LinkedIn, Snapchat, Instagram, Twitter, Facebook...) with the aim of impersonating victims and causing damage to their reputation by defaming them and spreading offensive information about them, or harassing their friends by using their accounts to bully them.
- b. Account theft on email and instant messaging services.
- c. Theft of accounts on electronic games websites.
- d. Opening bank accounts, obtaining loans, and carrying out illegal acts, by completely impersonating victims.
- e. Illegal use of victims' credit card accounts to make purchases or withdraw cash.



### 3.4- Cyber-bullying:

Cyber-bullying is when someone or a group of people harass, mistreat, or taunt a victim over and over through emails, websites, blogs, videos, or any other means of communication intending to harm him/her.

#### Examples of Cyber-bullying:

- a. Posting slanderous messages on social networks.
- b. Spread rumors on the internet.
- c. Incitement on the internet to exclude someone from a certain group or even socially.



### 3.5- Hacking:

This includes hacking or attempting to hack online data that belong to individuals, government agencies, or private entities in order to steal or sabotage it.

Such data may contain sensitive information about citizens, agents, staff or other equally important things related to intellectual property.

### 3.6- Ransomware:

This type of malware encrypts critical data or the whole device (a computer or a smart phone) so that the user can't access his/her data. The hacker then asks the victim to pay an amount of money (called a ransom) in the form of crypto-currency such as Bitcoin since it is difficult to be traced, in return of sending the key to decrypt the data and making things normal again (this is not guaranteed, thus it's never recommended to pay the ransom).



### 3.7- Business Email Compromise Fraud:

It is a type of fraud that targets companies involved in financial transfers or have suppliers abroad. It depends mainly on accessing emails that belong to CEOs or those responsible for financial transfers in the company. It works by creating similar emails or hacking the original addresses through Phishing or Social Engineering techniques. Then, deceiving the company's employees by pretending to be the CEO or any other executive entitled to authorize financial transfers abroad, in order to perform urgent financial transfers which would cause huge financial losses.

In other words, once the cyber-criminal gets familiar with the procedure, he/she uses the fake e-mail account of the manager to organize a request for money transfer and asks the employee not to follow the procedures that are usually adopted to ratify such transfer requests and quickly transfers funds to an account administered by the cyber-criminal in a bank, often located outside the state where the company is located. In this case, the real manager will be unaware of the content of the request and of any responses received by the employees.



## 4- Protection from Cybercrimes and Cyberthreats

This guide aims at raising awareness of all society members about the most significant cyber threats and cybercrimes, and at enhancing protection and personal privacy when connecting to the internet and benefiting from digital services.



### 4.1- Protecting Accounts and Applications from Internet Risks

The protection of emails, passwords, social media accounts, text messaging applications and electronic devices is an essential part of the society's protection against Internet risks. In addition, it is necessary to follow the following below mentioned procedures and guidelines and make sure they are fully implemented.

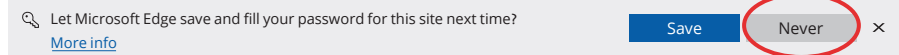


### 4.1.1- Creating a Strong Password:



- Use strong, complex passwords not less than 12 characters that include a combination of uppercase letters (A - Z) and lowercase letters (a - z), in addition to numbers, symbols and signs (#,\$,%,@,&!).
- Use complete sentences as passwords if possible (For example: TH1515@5TR0NGP@55) and replace some characters with special symbols.
- Avoid using personal information in passwords such as name, phone number, housing address, date of birth, etc.

- Passwords must not contain any words in the dictionary so that they cannot be easily guessed.
- Avoid using sequential characters (ABCD12345) and keyboard sequences such as (QWERTY) and (ASDZXC).
- Avoid using the same password for different accounts and applications.
- Use special and trusted Password Manager applications if possible, to help creating and managing passwords.
- Avoid saving passwords along with detailed account information in unsafe locations such as mobile phones, computers, or written papers.
- Do not share your passwords or enter them in a visible way in front of other people.
- Change your passwords immediately if you suspect that any of your accounts has been hacked.
- Change the passwords of your accounts regularly and be sure to create a new password that is different from the old ones.
- Be careful when choosing the password recovery questions, which are used by some sites to help remember the password in case you forget it, so that they are not easily guessed (For example, choosing the father's name as an answer to the recovery question).
- Avoid saving passwords on any of the applications that provide the "Save Password" feature.







## 4.1.2- Protection of Social Media Accounts (Instagram, Twitter, Facebook) LinkedIn, Snapchat ...)

- Adhere to the aforementioned password selection criteria.
- Provide the least required information that is necessary to open a new account on social media.
- Review and activate Advanced Security Settings to increase account protection, such as activating the 2 FA - two Factor Authentication feature, limit access to the account details, enhance the privacy options, and activate appropriate alerting method when suspicious attempts are made to access the account.
- Be careful to the detailed personal information you post about yourself and your family because it is difficult to control any information after it has been published.
- Avoid participating in any harmful and illegal cyber activities such as extortion, defamation, insulting or offending religious or sectarian beliefs, threatening others and harming them.
- Make sure you communicate only with trusted people and beware of strangers and those who request to add you as a friend.

- Do not respond to any conversations from an unknown source, especially as some, intentionally or unintentionally, change or hide their real identity (age, name, gender, and image) on social media.
- Avoid posting or reposting (share, retweet, ...) incorrect and unreliable information.
- Avoid accepting friend requests from unknown people and check their photos posted on their page and their friends list before adding them.
- Avoid exchanging your social media accounts data or allow anyone to use your accounts under any circumstances.
- Sign out of your social media accounts after you finish using them.
- Make sure that the social media accounts are linked to your mobile-phone number in order to verify your account data when accessing it, and to make it easier to recover if it is lost.
- Do not click on any unsafe links from unsafe sources within the social media is because it may contain malware.

## How to Protect Yourself on the Internet?



**Don't click on links and attachments in e-mails received from unknown senders**



**Think well before posting any photos or videos of you and your family**




**Preserve the privacy of your personal information, your house and work location, as well as your accounts, phone number and passwords**



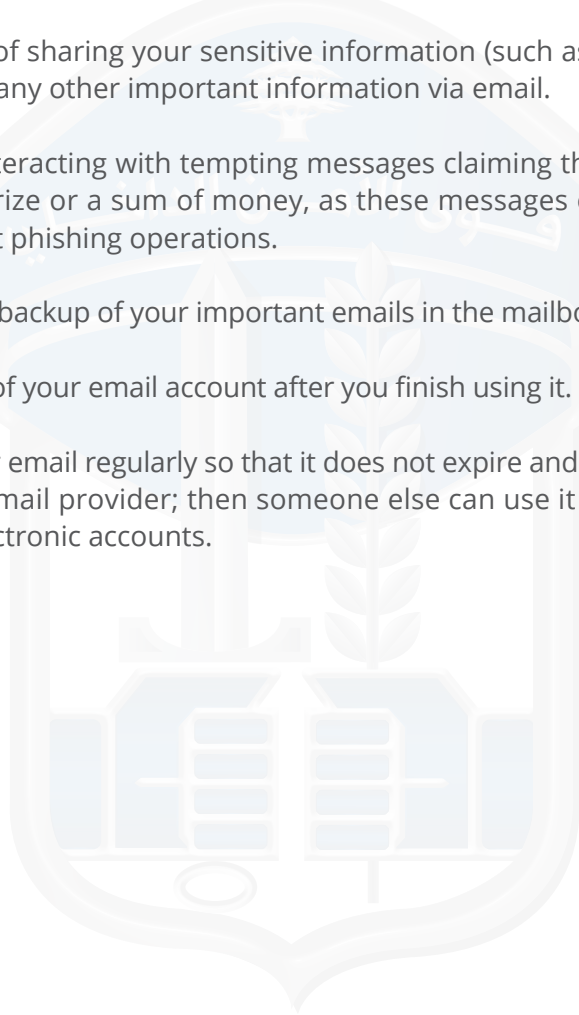
**Don't communicate with strangers, but only with trustworthy persons that you know well**



### 4.1.3- Protection of Email Accounts (Yahoo, Hotmail, Gmail ...)

- Adhere to the aforementioned password selection criteria.
  - Create new e-mail accounts by yourself, and be careful when someone is helping you since he/she would be able to recover your password later even if you change it.
  - Review the Advanced Security Settings of your accounts and make sure to activate them so to increase the protection level of the Email addresses. Examples include activating 2FA - Two Factor Authentication and spam protection and using Email filters, etc.
  - Share your email address with trusted people only.
  - Check the CC, BCC, and TO fields before sending an email to make sure not to add unwanted people.
  - Create an additional email address to be used for restoring your primary e-mail account if it gets hacked or stolen.
  - Avoid using your email address to take part in competitions or suspicious games.
- Be careful of peepers when having to sign in to your account in front of others or in a public place.
  - Ignore emails coming from unknown sources that may request your personal data such as usernames or passwords, etc.
  - Be careful not to open links within your e-mail inbox or to open any attachments before verifying the source in order to avoid downloading malicious software aiming to hack the account and the device for spying or sabotage purposes.
  - Delete spam messages immediately and avoid interaction or responding to them because it could expose you to further intrusive messages.
  - Never leave your email address visible to everyone on social media platforms and other sites and only give it to people you know.
  - Beware of messages that aren't addressing you personally , and uses general greeting phrases such as "Dear User" and "Dear Email User" because it might be attempts to commit phishing.
  - Make sure to connect to the Internet through secure HTTPS if possible, which is usually preceded by a lock symbol , to make sure that information is safe while connecting to the email Service providers.

- Beware of emails that suggest an emergency related to you (For example, you have exceeded your share of emails, you have been a victim of phishing, or your email account is about to be closed...) as this can be an attempt to violate your privacy or hack your account.
- Beware of sharing your sensitive information (such as your credit card) or any other important information via email.
- Avoid interacting with tempting messages claiming that you have won a prize or a sum of money, as these messages often aim to carry out phishing operations.
- Retain a backup of your important emails in the mailbox regularly.
- Log out of your email account after you finish using it.
- Use your email regularly so that it does not expire and be retrieved by the email provider; then someone else can use it to hack into your electronic accounts.





#### 4.1.4- Protection of Text Chat Apps (WhatsApp, Skype, Signal, Telegram ...)

- Adhere to the aforementioned password selection criteria.
- Review the Advanced Security Settings of the text chatting applications and make sure to activate them to increase the protection level of the text chat apps. Examples of this include activating 2FA - Two Factor Authentication, encrypting messages, retaining a backup of important messages, ...
- Beware of anonymous messages that request private or personal information, and avoid opening the included links or attachments, because they can download malicious software to steal personal information and data and hack the device.
- Report spam messages as soon as you receive them to the application management (Report as spam)
- Block unwanted numbers to prevent them from communicating directly with you.
- Never be attracted to links that come through chat applications regardless how tempting they may be, because they may contain malware.
- Avoid joining chat groups that promote information that may be aggressive or threatening to you.
- Do not reply and respond to any chat from unknown senders.

- Do not communicate or exchange your private photos while video chatting with anyone to avoid being a victim of extortion in any of its forms.
- Deactivate your various chat application accounts and delete all related data from your device before giving it up for whatever reason.
- Enhance security settings by using a PIN number to lock chat applications.
- Download all applications from official stores (e.g. Apple Store or Google Play Store).
- Do not send confidential data or bank accounts details or passwords or any other sensitive documents through these applications.





## 4.2- Protection of Children Online



Raise their awareness on the use of security and privacy setting



Discuss with them the potential risks of internet usage



Set and regulate the time of internet usage



Keep electronic devices in a place easily seen in the house



Raise awareness on the potential risks of webcam and video conversations



Don't communicate with strangers and don't share any photos, videos or personal information



Report any problem, threat or strange request



Raise awareness of the importance of making strong passwords



- You should always discuss with your family members cyber threats that may happen on social media and text chatting applications, especially cyber-bullying and sexual extortion “Sextortion”.
- Children that use the internet should be monitored, and it is recommended that the various electronic devices should be kept and used in a visible non isolated place at home, such as the living room instead of the bedrooms.
- You should spend some time with your children on the internet to teach them how to surf safely and be aware of their internet usage techniques.
- Make sure to discuss frankly and clearly with your children about personal information and explain why it has to remain private, as it is possible to abuse such information to identify their identity, their address, the places they go to, or even the activities they take part in.

- Advise your children to be very cautious when posting pictures or videos of themselves on the Internet and social media, because once published, everyone can access them and abuse them.
- Warn your children to refrain from communicating with strangers, and never to share with them any pictures, data, videos or personal information (home address, phone number, and E-mail address). Also, they should never video chat with strangers nor approve to meet them under any circumstances.
- Teach your children that it's necessary to notify you about any problem, threat, or extortion they might face on the Internet, no matter how bad it may seem.
- Explore with your children their favorite sites and help them subscribe or register in them by choosing a proper pseudonym and without disclosing any information about their personal identity.
- Implement a set of rules for children and make sure they know what can be shared with others; also identify the types of websites that can be visited and the online games that are appropriate for their age groups.
- Specify the total time allowed for children to be online, as they need to achieve a balance in online and offline activities to enjoy a healthy childhood and take appropriate measures to enforce that timing, such as turning off the “wireless router” during bedtime or others.
- Encourage your children to use the Security and Privacy Settings in programs and applications in order to ensure their protection.

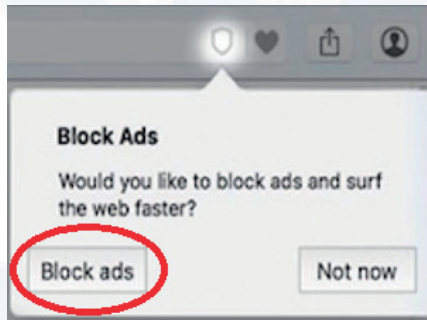
- Create a family electronic account for entertainment activities that can be used to participate in competitions and other activities.
- Advise your children not to post offensive information, videos, or pictures of other people on the Internet, as this is wrong and it exposes them to legal prosecution.
- Encourage your children not to respond to negative posts that they don't like and not to communicate with anyone who posts abusive messages to them.
- Advise your children not to download illegal or unauthorized copies of programs, applications, music clips, or films, and let them commit to a quality of games that suit their age groups.
- Advise your children not to click on buttons or links that promote advertisements, competitions, or prizes, as most of them contain malware or help spreading bad content.
- Anonymous emails that contain attachments or links should not be opened because they may be a form of phishing attacks or they may contain harmful viruses.



- Advise your children to use search engines appropriate for their age groups like Kiddle.co, kidrex.org, and other engines.
- You should periodically check your children accounts on social media and ask yourself "Can any stranger exploit these information?"
- You should periodically check the browser's history to see the sites and e-mail addresses that your children are browsing.
- Never give children a credit card in order to ensure that they don't make unusual purchases and payments without your prior knowledge.



- Use monitoring programs such as “filtering and parental control” that help in watching and blocking unwanted programs and websites and allow parents to control the children activities on the internet and prevent them from accessing inappropriate sites.
- Advise children not to delete offensive messages and keep them to be used as evidence when needed.
- Activate the browser security settings, such as ad blocking and Web filtering.



## 4.3- Electronic Devices Protection Measures

In order to enhance safety and protection measures, users can follow procedures that help them protect their electronic devices from being hacked as follows:

### 4.3.1- Procedures to Protect Desktops and Laptops:

- Adhere to the aforementioned password selection criteria.
- Make sure to activate the updated firewall that is integrated in Windows and MAC operating systems opening only the required Internet ports.
- Activate automatic screen/device lock after a short period of inactivity.
- Ensure that automatic updates are enabled for all software, applications, and the operating system in order to stay protected from threats and vulnerabilities even the newly discovered ones.

- Disable remote access settings on the computer and activate it only when needed.
- Make sure to use original copies of reliable Antivirus & Anti-malware programs to protect against viruses and malware and keep them constantly updated.
- Always make sure to keep the laptop camera covered when not used.
- Turn off all the device's network communications (Bluetooth, NFC, WiFi) when not used.
- Always download programs or games from their original sites and never from other unreliable ones.
- Ignore Ads & Popup messages that encourage you to download certain programs claiming to clean your computer from viruses and malware.
- Ignore requests to upload/download any program or application that provide specific services when they are received from unreliable sources.
- Beware of free offers to download music and games because these are popular ways to spread malware.
- Check carefully the permissions required by applications and programs and the extent of their actual need before downloading them.

- Uninstall all applications and software that you don't need.
- Avoid working on portable devices, in crowded places that have little privacy (such as coffee shops, hotels, etc.), to avoid shoulder surfing or peeping at your device, especially when working on private or sensitive data and information.
- Do not use any USB flash drive or other external storage devices before checking it and making sure it is free of malware.
- It is necessary to log out of all your accounts and clear all browsing history & cookies, when you connect to the internet in public places (for example in an Internet cafe, library, or hotel).
- Always make sure to keep backup copies of important content of your device and your data on a CD, DVD, an external hard disk, or on the Cloud, in order to reduce the damages that may result from infection with any kind of virus or malware (ransomware) or from having your Laptop stolen, broken, or lost, and make sure that the backup can be recovered.
- Wipe sensitive and personal data from your computer before getting rid of it for any reason.
- Never use an account with Admin Rights and privileges for daily activities.





### 4.3.2- Smartphones and Tablets Protection Procedures

- Enable advanced security settings on smartphones and tablets, such as complex and strong passwords, biometric verification (such as face recognition, fingerprints, and eye print), as well as the use of complex patterns for an advanced protection of the devices.
  - Activate the Find my Phone and Auto lock features to secure the device's protection and make it easier to find it in case of loss or theft.
  - Activate the automatic update feature for all programs/applications and OS operating systems, in order to stay protected from software vulnerabilities that may be exploited to penetrate your device.
  - Avoid tampering with your phone's factory settings (Ex: Jail breaking or Rooting).
  - Turn off all wireless communications (such as NFC, Bluetooth, Wi-Fi) if not used.
  - Do not grant permissions to applications or software on the Portable device or the smart phone if it seems exaggerated or illogical.
- Download only the actually needed applications from the official stores (such as the Apple Store or Google Play Store) to avoid infecting the device with malware.
  - Make sure to review users' rating & reviews about performance, effectiveness and reliability of the app you intend to use before downloading it.
  - Download an original and reliable Antivirus & Anti-malware program on the mobile phone and update it regularly.
  - Use a reliable network to connect to the Internet and avoid free and public Wi-Fi networks unless necessary.
  - Avoid saving passwords or sensitive information on a smartphone or a portable device.

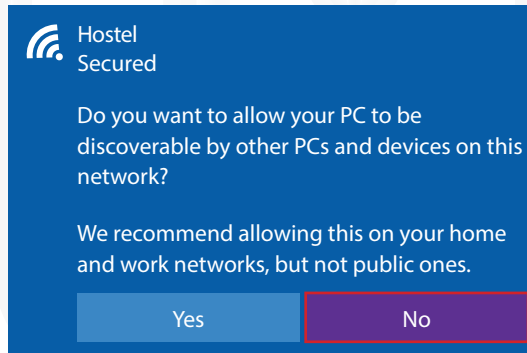


- Always make sure to keep backup copies of the content of your device and your important data (such as contacts, text messages, files, private photos, videos, chatting applications chats, etc.) on CD, DVD, external hard drives, or on the Cloud, to reduce the damage that may occur from being infected with any kind of viruses and malicious programs that demand ransom, or from losing your phone or portable device.
- Make sure to delete public Wi-Fi networks that you previously used in certain periods.
- Ensure that your device is always under your sight in public places, and that it is not left out of your reach, even for a short period of time.
- Make sure to save the IMEI number of your mobile device.
- Reset your smart phone or tablet device to the factory settings “Wipe Data/Factory Reset” before handing off or getting rid of it for any reason.

## 4.4- Protection Measures of Wi-Fi Networks and the Devices Connected to it

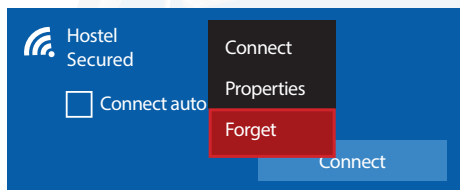
### 4.4.1- Public Wi-Fi

- Avoid connecting to public Wi-Fi networks: cafe, restaurants, hotels, etc. Using Internet through the mobile phone remains more secure.
- However, if it is necessary for you to connect to a public Wi-Fi network, be sure to follow these procedures:
  - Do not allow your computer device to be discoverable while connected.

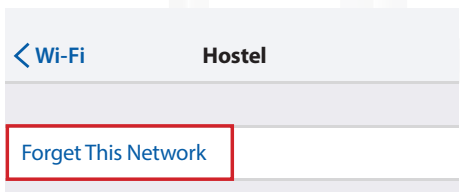


- Avoid automatic connection by removing (Forget) the Public Wi-Fi networks that you do not intend to connect to in the future.

- Example: Removing a Wi-Fi network on Windows:



- Example: Removing a Wi-Fi network on iPhone:



## 4.4.2- Private Wi-Fi:

- Adhere to the aforementioned criteria for selecting passwords and apply them to connect to your Wi-Fi network.
- Review the security settings of the Wi-Fi device or the router and change the default Wi-Fi SSID, the username, and the password set by the WiFi router manufacturer, and apply automatic updates to the Router Software.
- Activate encryption settings for the connection of the private Wi-Fi network through the latest types of encryption (currently WPA2/3) to protect the incoming and outgoing data from the wireless router.
- Apply two-factor authentication settings on electronic devices and accounts connected to the Internet, whenever possible.
- Turn off the Wi-Fi router when not used to prevent potential hacking attempts.



## 4.5- Protection Procedures for Electronic and Financial Transactions

Following are some instructions and procedures that assist users in keeping their funds and credit cards safe and protecting their financial and electronic transactions on the Internet.



## 4.5.1- Protection Procedures for Electronic Banking Transactions

- Accomplish electronic banking transactions through secure computers and mobile devices with the latest Antivirus software in order to detect and stay protected from most threats and vulnerabilities in applications and operating systems installed on them.
- Avoid conducting electronic banking transactions if you are connected to the Internet via a public Wi-Fi, or if the sites you are connected to do not use the https protocol 🔒 .
- Do not disclose the details of your accounts or bank cards except to trusted people (for example, representatives of banks, hotels, etc.) and be attentive to the information that you disclose to them.
- Be attentive to the information you share over the phone with any caller who asks for details about your accounts, bank cards, or financial transactions.
- Do not share PIN codes and OTP “One Time Password” given by the bank with anyone, even if he is an employee at the bank, keeping in mind that the bank employee will never ask you about the codes for your account or credit card.
- Ensure that the number pad is shielded from others when typing your PIN code at the ATM or points of sale, and avoid disclosing it to anyone.

- Beware of having your credit card snatched when you are in a crowded place.
- Destroy expired credit cards by cutting them into small pieces and ensure that the magnetic stripe and chip are totally destroyed.
- Review your bank accounts from time to time, especially those linked to your credit cards, to ensure the accuracy and correctness of executed financial transactions and inform your bank about any suspicious transactions or payments that you haven't carried out, or even continuous withdrawal of small amounts of money.
- Conduct additional audits and validations of transactions (for example, calling back the requesting party) regarding any payments exceeding the specified allowed limits.
- Avoid entering details related to your bank account after clicking on a link in an email message, or text message, as this could lead to theft of your personal and banking information.
- Never respond to any email messages claiming to be from the "bank" or any company requesting your account or confidential information such as passwords, credit card numbers, personal identification numbers or tax identification numbers.
- Logout from your account as soon as you finish using the online banking services.

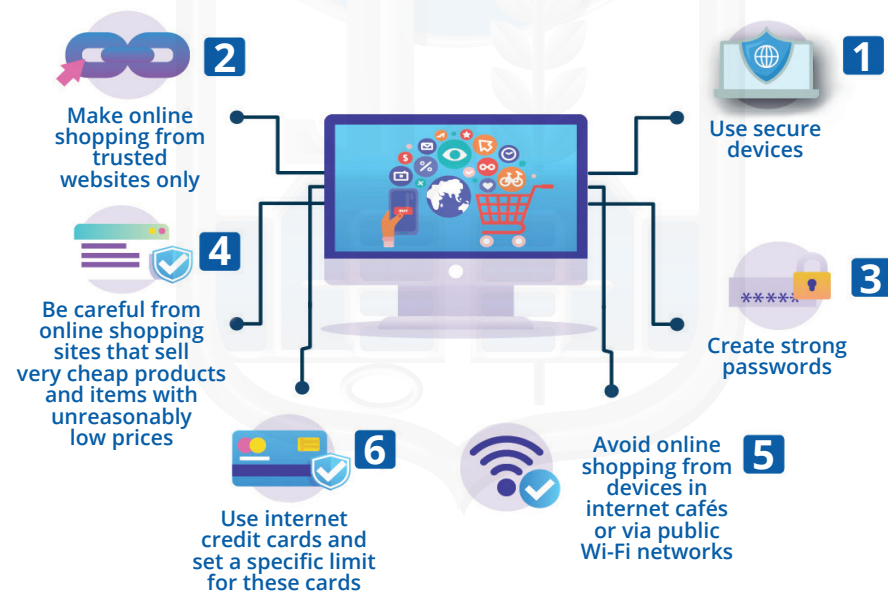
## Protection Procedures for Electronic Banking Transactions

- |   |  |
|---|--|
| ✓ Use secure devices to make your electronic and banking operations   | ✗ Don't undertake electronic banking operations if you were connected to the internet via a public Wi-Fi network                   |
| ✗ Don't share via your phone or through an electronic message or a sms or links any details about your accounts, bank cards or financial transactions | ✓ Make sure to use the official website of the bank (be careful from the suspicious links that claim to be affiliated to the bank) |
| ✓ Create strong passwords   | ✗ Don't reply to suspicious messages or calls  |
| ✗ Don't share any of your passwords, usernames or pin codes   | ✓ Make additional auditing and authentication of financial operations  |





## 4.5.2- Procedures for Secure Online Shopping



- Shop online through trusted sites that provide the ability to have a secure and encrypted connection to the Internet (HTTPS or the padlock symbol ).
- Beware of the suspicious customer service contact details in online shopping platforms (For example, the email address of customer service is “supportcompany@gmail.com” instead of “support@company.com.”).
- Beware of electronic shopping centers that promote products at very low and illogical prices as they are very likely to carry out fraudulent operations.
- Beware of suspicious online shopping addresses, such as Brands-at-awesome-price.com, that may be intended to carry out phishing operations.
- Avoid shopping online through certain links that come through emails (for example, an email intended for fraudulent phishing includes a fake display of a desired product with the “Buy Now” button).
- Avoid shopping online from devices connected to the internet in cyber cafes or through public Wi-Fi network.
- Be careful not to provide more information than necessary to complete the online purchase process.
- Carefully review previous consumers’ opinions when dealing with the same site, seller or product.
- It’s necessary to set a limit on your credit card to specify the maximum amount allowed to be withdrawn or purchased simultaneously. You can also use Internet credit cards or prepaid cards.
- Do not save credit card details on online shopping sites.



### 4.5.3- Protection Measures against Financial Fraud via Business E-mail “Business Email Compromise”

- It's necessary to conduct a thorough analysis of the various e-mails, especially those related to financial transfer requests and unfamiliar requests from executives.
- It's necessary to put in place strict mechanisms and measures for financial transfers received from e-mail requests before sending any data or transferring any amount of money, such as:
  - ◊ Check the invoice carefully
  - ◊ Check and verify the payment details related of the recipient
  - ◊ Check with the executive manager, the lawyer, or the insurance company... regarding any request related to financial transfers
- Verify emails that include misspellings or unusual requests, especially if the given deadline for the payment or transfer is short.
- Check carefully the sender's email address, as most of the time the email of a hacker contains a different or additional character.
- Verify the payment adjustment requests by calling the concerned party from a previously known phone number and not the one mentioned in the e-mail containing the current request.
- Ask the sender to send the adjustments related to the new payment method through a letter that contains the company logo, and verifying the authenticity of this logo.
- Verify any changes to the seller's payment details by using a second signature of one of the company's employees.





## 5. How to Deal with Cybercrime

The following describes how to act when exposed to a cyber-crime or cyber risk:

### 5.1- How to Act when Smartphones and Portable Devices are Lost or Stolen

In case your portable device or smartphone was stolen or lost, you can take a series of important steps . some of them are related to safety measures of mobile devices described previously in this guide.

#### In this case:

- First try to call the mobile phone from another number, to determine if you can hear it ring.
- If you have previously enabled “Find My Device” feature (through the links [android.com/find](https://android.com/find) for Android or [icloud.com/find](https://icloud.com/find) for the iPhone), follow these steps:
  - a. Check the location of the device using the application and run the alarm in case it was near.
  - b. Do not go to the device’s location if it is far away, but contact the internal security forces immediately.
  - c. Use the Lock Device or Secure Device feature, which enables you to lock your phone remotely so that no one can access your phone’s content. In addition, you can display a message of your choice on the lock screen indicating that the device is missing.

- If you keep your credit card information on the browser or in one of the applications on your phone, you must immediately contact the bank and inform them so they cancel these cards and issue new ones. However, if you are using Internet Phone banking services, you have to request the immediate change of passwords in case you are not able to do it yourself.
- All passwords belonging to the various accounts connected to your phone should be changed. Perhaps the most important thing is to change the password of the applications stores so that no one can make other purchases.
- Inform local law enforcement/Judicial authorities of the lost/stolen device and provide them with the device’s IMEI serial number if they requested it.
- Make sure to call the customer service center of the telephone company to cancel your phone number and suspend all services related to it.
- Log in to all services and accounts that you have previously used from your stolen phone, using a different device that you own and make sure to logout from all other devices “Logout from all other devices” in order to disable them on the stolen device.





## 5.2- How to Act When Falling Victim to Cyber Extortion

If you are a victim of Cyber extortion and you are not sure what to do, follow these steps:

- Stay cool and do not make any decisions alone. Talk to someone you trust, such as a friend or family member.
- Never harm yourself or others, because police forces are ready to help you and to prevent crime and punish the perpetrators.
- Save all evidence and content of the email messages related to the cyber-extortion so that you can show them as evidence to the police later.
- Do not communicate with the extortionist, even when under severe pressure.

- Do not comply with the extortionist's demands, such as transferring money, giving credit card number, or to any other request, as this may lead to increased pressure to achieve additional demands.
- Avoid arguments with the extortionist and report blackmailing or bullying attempts to the security agencies without giving any indications of your plan to the extortionist.
- Keep communicating with the extortionist in order to trace his/her location or to collect additional evidence, if the police asked you to do so.





### 5.3- How to Deal with Cyber Bullying

- Be careful not to respond or take revenge.
- Gather all evidence and keep mobile phone messages, emails or social media chats, and talk to someone you trust, such as a family member or a friend.
- Report the bullying incident and follow the police advice regarding:
  - Blocking the bully and change your privacy settings in order to limit the access of strangers to your data and your account posts.
  - Reporting the abuse through the dedicated service on the application.



### 5.4- How to Deal with Stolen Accounts of Various Social Media Sites, Text Messaging Applications or Service Providers

Sometimes the cyber criminals make some changes occasionally to the social media accounts (Facebook, YouTube, Instagram, Twitter, WhatsApp, Gmail, Snapchat ...) that are difficult to be noticed but suspicious. For example:

- Not being able to log in with your password.
- Add/Remove friends, follow requests, likes, or options that you did not make.
- Update the status or posts/tweets not done by you.
- Upload photos without your knowledge.
- Send private and annoying messages to your friends.
- Modify the main profile page (or profile photos) of your accounts without your knowledge.
- Receiving unanticipated emails or notifications from the social media sites administration, for example: Your email address has been changed.

In case any of the previous incidents happened, you can take the following actions to limit the damage done by hackers, and start working to recover your stolen account:

- Try to log in with another device to see if you have already lost access, and make sure to check the password that you enter many times.
- Check whether you received any warning e-mails from websites and internet service providers about suspicious activities in your account (such as someone trying to log into one of your accounts from an unfamiliar computer or from an unfamiliar place or someone changed your username or password).
- Go to the support page that provides assistance at the official website (Snapchat, Gmail, Instagram). You can also send a report of the problem you are facing and request to block the account (Twitter, Facebook).
- Follow the instructions provided by the official site or service provider to recover the account. In this case, you may be required to verify your phone number, backup email address, or answer personal questions to prove that you are the true owner of the account.
- If an account (WhatsApp, Telegram, Signal ...) was stolen, delete the application from your device, re-download it, and use text messages or calls for verification. Consequently, the account will be deactivated from the hacker device, and activated on your device again.

- After logging in to your account again, change your password immediately and check all your personal information and other settings, to ensure that there is no change in the phone number and the backup email address, personal questions...
- Ensure not to reuse any previously used passwords.
- Change the password of all other accounts that use the same old password for log in; Notice that using the same password for multiple accounts is not recommended at all.
- Log out from all other sessions except for the current session you are using (Logout from All Other Sessions).
- Check the additional security settings in your accounts and activate them, such as the two-factor authentication (Double Factor Authentication) feature (password + code sent to your cell phone) and other security features that are designed to prevent Cyber-attacks. For example: Facebook allows you to add a list of trusted friends who can confirm the authenticity of your identity in case your account was hacked again.
- If you are unable to recover your account, contact your friends and all the contacts on your account and inform them that your account has been hacked, or being used for Cyber extortion, and warn them not to accept any message or click on any links sent from it; Also, ask them to report the stolen account to the administration of the site, so the account gets banned.



## 5.5- How to Act When Infected with Malware

There is a series of problems that affect the computer performance and suggest that it has been infected with viruses and malicious programs, such as running extremely slow, quickly discharging, losing control of the device, deletion or shuffling the order of some files, disruption of some services and functions, automatic and unusual run of some applications.

In this case, the following actions should be taken to solve the problem:

- If there is no available backup copy, transfer your important data and files to a USB storage memory or external hard disk; which may become infected in case the transferred files were infected.
- Disconnect the device from the Internet.
- Change all passwords for your online accounts using another device.
- ◊ Put your device on safe mode and run Check Disk and Disk Cleanup through the operating system.
- ◊ Perform a full scan and clean your device using anti-virus program following the recommendations and instructions it provides.

In case the anti-virus program did not succeed in removing and erasing the Malware, you should do the following:

- Format the infected computer and re-download an original copy of the operating system such as Windows, Linux or MacOS, this way, you ensure that your device is free of malicious files.
- Download and install a reliable, robust and original anti-virus program from its source.
- Update the operating system and the antivirus program and make sure that the update was successful before scanning the data of the most recent backup, or the data that you transferred to an external disk or a USB flash memory as mentioned in the first step.
- Restore the data back to your device.
- Check your device and data using the updated antivirus regularly.



## 5.6- How to Act When Devices Are Infected with Ransomware

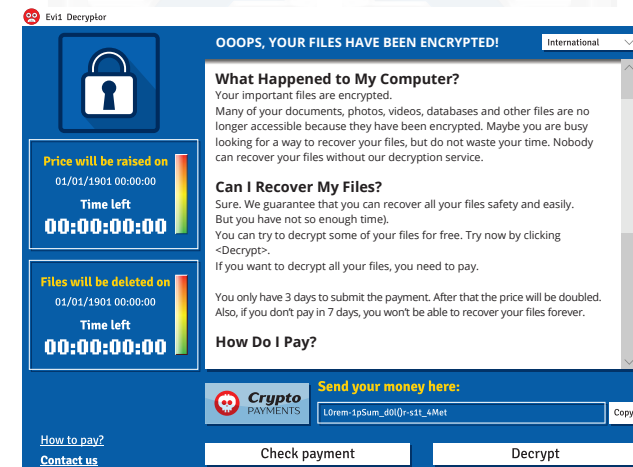
When a computer or a smartphone is infected with this type of malware, we recommend not to yield to the hacker's demands in paying the required amount of money or ransom for the following reasons:

- There is absolutely no guarantee that you will recover your data since ransomware operators aim only at collecting money.
- Your device will remain infected with viruses until you perform a full device scan and remove them.
- Hackers will continue to extort you to pay more money, or they will attempt to cyber-attack you again to get you to pay other ransoms in the future.
- You will be contributing in financing these criminal groups.
- You will be encouraging these criminals to develop these types of malware and maybe they will target you again.

Rather in this case, it is recommended to take some steps to clean the device and return it to its normal condition, as follows:

- Try to identify the type of ransomware, as it is either a Blocker/Locker virus or a file encryption virus "Cryptor".
- In case you are unable to skip the notification message on the screen that warns you of a virus, your device is probably infected with a 'Lock Screen' virus; however if you could skip it but can't access some or all of your files, your device is infected with a 'File encryption' virus.

- If you are able to browse the system and read most of the files without any problem, then this is just an attempt to delude you of being a victim, in order to force you to pay money by placing a picture on your desktop background.
- In case of infection with a 'File encryption' virus:
  - Disconnect your device from any other device and external drive.
  - Use a camera to take a picture of the virus notification that appears on the screen and inform the police of that.
  - Try to retrieve some encrypted files using free decryptor programs that can be useful with certain types of ransomware.
- Use an anti-virus program and scan the device to try to get rid of the ransomware. Following this solution, you may not be able to retrieve your encrypted files, but you will be sure that there are no more malware left on your device.



- Check whether you are able to recover files that were deleted. Some types of encrypting viruses copy your files, encrypt the copies, and then delete the original files. In this case, it is possible to recover deleted files using free applications such as ShadowExplorer.
- Try to use applications that help identifying the type and name of the encrypting virus that you are dealing with, such as Crypto Sheriff, ID Ransomware Tool, among others...
- Search for a decoder tool at “nomoreransom.org”.
- In case you did not succeed in disabling and unlocking the ransomware, reset your device to the last restore point; and if this failed too, reset your device to the factory settings “Restore Factory Settings”, re-download the operating system again and then restore your files from the backups you created earlier.
- As for the screen-locker viruses, restoring the system will be sufficient to access it again. In case this does not work, the solution would be to use a bootable disk before starting the device (rescue CD) and perform a scan.





## 5.7- How to Act when a Credit Card is Lost or Stolen.

When there is a suspicion that your credit card has been stolen, lost, or hacked and being used without your knowledge and consent, the following procedures should be followed:

- Contact the credit card issuer directly through reliable communication channels, such as calling customer service using the phone and report theft or loss of your card in order to take the necessary measures to cancel it and request a replacement.
- Review the account statement of the card to ensure that there are no illegal transactions and no additional fees or costs on the regular transactions.
- In case unusual costs have been noticed, file a dispute to the card issuer as soon as possible in order to take the necessary measures to recover the money.
- After receiving the new credit card from the issuer, follow the aforementioned safety and protection measures.
- Update your mobile wallet and all your accounts on the online shopping sites in case the lost card is used to make payments.



## 5.8- How to Act in Case of Falling Victim to Online Bank Fraud

When you suspect that you have been or about to become a victim of any bank or financial fraud, you should follow these steps:

- Immediately report this by contacting the relevant party that is concerned for frauds in your bank to take necessary actions.
- Change the password of your bank account on the website or on the mobile application.
- Document the date and time of the discovery/report of the fraud and any other relevant notes.
- Monitor your bank account and document any suspicious banking transactions that happen from your account for legal proof.
- Try to record what happened? Who did this? Is the fraud still ongoing? When did it happen? What is the value of the losses or the potential losses?
- Identify all the evidence related to the fraud as well as bills, contracts, purchase orders, checks, etc.



## 6- Contacting the Internal Security Forces and requesting help

The Internal Security Forces ensures the complete secrecy of cybercrimes investigations and it will spare no effort to help you solve the problem you are facing.

Report any cybercrime, or any cyber threat or danger that you may face to the Internal Security Forces through one of the following:

- Cybercrime Prevention and Protection of Intellectual Property Bureau:  **01/293293**
- “بلغ” or the Report Service available on the main Internal Security Forces website: [www.isf.gov.lb](http://www.isf.gov.lb)



### Report Service

\* Report Text

\* Report Type

Cyberbullying

\* Email

\* Phone (only numbers)

\* Would you like us to contact you ?

Yes

**Note:** If there are attachments, please send them via the email mentioned above to the address: [ballegh@isf.gov.lb](mailto:ballegh@isf.gov.lb)

- No, I will not send attachments.  
 Yes, I will send attachments via email.

Send





# **LEBANESE INTERNAL SECURITY FORCES**

**PUBLIC RELATIONS DEPARTMENT**

**SERVICE - TRUST - PARTNERSHIP**

**Prepared by:**  
Cyber Security Committee  
November 2020



Funded by the European Union