



INFORMATION SECURITY AWARENESS

GENERAL PUBLIC PAMPHLET

(PROTECT YOUR DEVICES)

v0.1 NOVEMBER 2019

PREPARED BY
HADI HOSN MSc, CISSP, CISM, ISO27001 LA / LE
SENIOR INFORMATION SECURITY CONSULTANT

Version Control

Version	Date	Comments
v0.1	28/11/19	<i>Initial Draft for discussion during workshop</i>

Document Approval


Name	Organisation/Position	Date
Peter Salloum	Crown Agents	
Lt. Col. Khaled Youssef	ISF (ID)	
Lt. Col. Nader Abdallah	ISF (IT)	
Beindy Dagher	EU Delegation	

These days, devices we use are a one-stop work, gaming, productivity, payment, texting, tweeting, Facebook-checking machine. The objective of this pamphlet is to raise awareness about the latest cyber security threats and the steps you can take to protect your devices.

Examples of cyber threats

- **Malware:** Software designed to penetrate or damage a computer system. Examples include viruses and ransomware.
- **Data Breach.** Release of private information from your device to an untrusted person.
- **Cyber spying.** Controlling the device without knowledge of owner to obtain sensitive information.


Protect Your Devices

- Review security settings of devices (e.g. **laptop, desktop, smartphone, tablet, WiFi router**). Enable more secure configurations, for example strong passphrase, encryption, application firewall, automatic updates, auto-lock screen saver, find my device activation, etc.
- Disable device features and connectivity (e.g. Bluetooth, NFC, and WiFi) when not in use.
- Download the applications that you really need only from **trusted sources**, such as Windows Store, Apple App Store or Google Play Store.
- Install **Antivirus** application on your device and **ad blocking** web browser add on. Prior to installing applications, read the user reviews on performance and security.
- Double check the permissions applications require before you download them. For example, access to your camera, microphone, location, contacts, administrator rights, etc.
- **Remove/Uninstall** applications and software that you do not use.
- Browse only secure websites (look for the padlock , or https) and be aware when clicking web links, pop-up windows, banners or advertisements online as some may contain malware.
- Avoid working on sensitive information when in crowded places (for example, airplane, coffee shop, airport lounge) and do not leave device out of reach in public even for short period of time.
- Enable **password protection** or **encryption** on external drives (e.g., USB memory stick).
- **Backup your most important data** regularly (for example contacts, notes, emails, instant messaging chats, files, pictures, etc.).
- **Delete sensitive data from device and factory reset it** before you donate, resell or recycle it.
- If you are using a public computer, log out of all your accounts, clear browser history and cookies, and lock the computer or shut down when not in use.

Dealing with common cyber problems

- If you realize **your phone or tablet is lost or stolen**, there are steps you can take. **1)** Call your phone. **2)** Use phone finder app. **3)** Check location of the device on the app and sound an alarm if device is nearby. **4)** Do not go to device location, instead contact police (more on that below). **5)** Lock your phone remotely. **6)** Perform remote erase on your phone. **7)** Call phone provider to stop phone number and suspend service. **8)** Change passwords for accounts associated with your phone.
- If you notice your PC is acting strange, you may have **malware**. There are steps you can take to clean up and restore your device. **1)** Back up all your documents and files. **2)** Enter your device in Safe Mode. **3)** Perform Disk Cleanup. **4)** Scan your device with your antivirus and follow its advice. **5)** If malware was not removed by Antivirus, format your device. **6)** Restore your backed-up data from the 'last known' good backup.

ISF is here to help

- If the guidance above is not enough and you need the ISF's expert help, you can call the 24/7 Hotline number: **01- 293 293** or send an email to cybercrime@isf.gov.lb
- If you would like to **report a cybercrime to the ISF**, go to the ISF website (<http://isf.gov.lb>), and complete  form or call phone number or send email.