

An Garda Síochána Crime Prevention Information Sheet



Laptop & Tablet Safety Information



Laptop and Tablet Devices

Laptop and tablet device owners should take great care of their property. It only takes a moment of distraction for a thief to take your laptop or tablet device. Along with cash, laptops and tablets are the most common items taken in burglaries. The cost of replacing the data contained on the device can sometimes cost more than replacing the hardware itself.

Laptops



Do:

- Treat your laptop like cash. - You wouldn't leave a large amount of cash unattended in a public place or in the back of the car. Keep a watchful eye on your laptop.
- Lock your laptop with a security cable. - Use a strong cable & lock and attach it to something immovable.
- Be on guard in airports and hotels. - Be extra vigilant when passing through security screenings. Keep an eye on your laptop when it passes through the security detectors. Store your laptop in the hotel safe.
- Consider carrying your laptop in something less obvious than a laptop case. - Consider using a suitcase, a padded briefcase, or a backpack instead.

- Consider an alarm for your laptop - Some alarms are motion sensitive or deploy when the computer is taken out of a specified range. Alarm applications which show the location of the device when it is connected to the internet may also be useful.
- Use security markings on your laptop. - Overt and covert markings make it easier to return recovered property to their owners. Record the laptop's serial number and take a pictorial record of your security markings for proof of ownership.

Don't:

- Leave your laptop unattended - Even for just a moment. If you have to, lock it or leave it with a trusted friend or colleague.
- Put your laptop on the floor. - When in public never leave your laptop on the floor. You cannot see it and it could be swiped without your knowledge.
- Leave your laptop in the car - Never leave valuables on display in unattended cars. Avoid leaving laptops in the car boot; you never know who is watching you!
- Keep passwords with your laptop or in its case. - Just like you wouldn't leave your pin number beside your ATM card! Why make it easy for the thief to access all your private details.
- Store sensitive material on your laptop - Consider Using 'cloud' applications for storing or accessing sensitive material and backing up of important or sentimental documents or images.

**FOR FURTHER INFORMATION ON THIS OR OTHER CRIME PREVENTION ISSUES,
PLEASE CONTACT
your local GARDÁ CRIME PREVENTION OFFICER
or
visit the Garda website at www.garda.ie**

Tablet Devices



It seems the tablet device will soon replace the laptop, just as the laptop took the place of the desk top computer. The practical uses and mobility of the devices have seen a huge increase in the numbers of people using them. Many of the security tips outlined above for laptops can be applied to tablet devices.

Consider the following security actions in addition:

- Always maintain physical control of your tablet. If it falls into the wrong hands much of the information stored within could be accessed and exploited. The security systems on the device can be overridden by those with sufficient know-how. If you do lose your device consider the fact that all data contained on it may be compromised and you should take appropriate action to remedy this.
- Maintain, update and use the security software offered by the manufactures of the device. The manufacturers spend vast sums of money improving their security applications in order to avoid attacks, so make sure you install the latest edition of their software.
- Use the Auto Lock functions on your device. This function will lock your device automatically after a period of non use. Most manufacturers would recommend three minutes of inactivity before the Auto Lock engages. This should be used in conjunction with a password, which should not be kept in the vicinity of the device. Ensure you are the administrator password holder. Many devices have a function to erase data after ten failed password attempts. You should also consider disabling the password and user name recall function on your device.
- "Jail breaking" is the term that refers to the process of modifying the tablet device's operating system in violation of the end-user license agreement.

Jail breaking significantly damages the device's ability to resist attacks because it disables the enforcement of code signatures, which is an important security feature. Jail breaking makes the attacker's job substantially easier. Consider the fact that the applications used for Jail breaking may in fact be corrupt and could destroy your data.



- Connectivity – Turn off your Bluetooth function and avoid using untrustworthy Wifi. You have little or no protection for data sent or received by your device as it could be intercepted. Some devices automatically connect to and remember Wifi areas. Turn off these applications on your device and only connect to Wifi you know and trust. When sending emails ensure you use encryption software otherwise they may be easily intercepted.

The advice contained in this information sheet is not intended to be exhaustive or absolute. Nothing contained in this publication should be interpreted as mandatory, obligatory or designed to conflict with any statutory regulations.

Always report stolen laptops or tablet devices to your local Garda Station.

Remember to supply serial numbers and details of security markings.

Never buy devices from untrustworthy sources.

Useful Contacts and Links

*The Garda National Crime Prevention Unit,
Garda H.Q., Harcourt Square, Dublin 2.*

Tel: (01) 6663362, Fax: (01) 6663314

Email: crime_prevention@garda.ie

An Garda Síochána

www.garda.ie

**Issued by the National Crime Prevention Unit,
Garda Community Relations and Community Policing Division,
Harcourt Square, Dublin 2.
www.garda.ie**