



States of Jersey Police



States of Jersey Police



# CYBER CRIME

PROTECT YOURSELF ONLINE



How you can help protect yourself from online crime

Over the past decade the way criminals work has changed dramatically. They are increasingly using the Internet to target hard-working islanders.

By following the simple steps in this leaflet you can help reduce your risk of attack.

# CYBER CRIME

PROTECT YOURSELF ONLINE

Find out more about protecting yourself online at:

[www.getsafeonline.org](http://www.getsafeonline.org)

[www.cyberstreetwise.com](http://www.cyberstreetwise.com)

[www.jersey.police.uk](http://www.jersey.police.uk)



**CRIMESTOPPERS**  
0800 555 111  
Call anonymously with information about crime



**CRIMESTOPPERS**  
0800 555 111  
Call anonymously with information about crime

# Here are a few simple steps you can take to help protect yourself online

## 1. Use Strong Passwords

Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining upper case letters, lower case letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

<http://bit.ly/use-strong-passwords>

## 2. Secure your computer

### Activate your firewall

Firewalls are the first line of cyber defence; they help reduce connections to unknown websites and will keep out some types of viruses and hackers.

<http://bit.ly/activate-firewalls>

### Use anti-virus software

Help prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

<http://bit.ly/use-anti-virus>

### Block malware attacks

Help prevent malware from infiltrating your computer by installing and updating anti-malware software.

<http://bit.ly/use-malware>

## 3. Be Social-Media Savvy

Make sure your social networking profiles (e.g. Facebook, Twitter, YouTube, Instagram, etc.) are set to private. Check your security settings regularly as the companies often adjust their settings and policies. Be careful what information you post online. Once it is on the Internet, it is there forever!

<http://bit.ly/be-social-media-savvy>

## 4. Secure your Mobile Devices

Be aware that your mobile devices are vulnerable to viruses and hackers. Get an anti-virus/anti-malware app installed. Only download apps from trusted sources.

<http://bit.ly/mobile-device-apps>

## 5. Install the latest operating system updates

Keep your applications and operating system (e.g. Windows, Mac, Linux, Android and iOS) up-to-date with the latest system updates. Turn on automatic updates to keep your Operating System up-to-date and help prevent potential attacks on older software.

## 6. Protect your Data

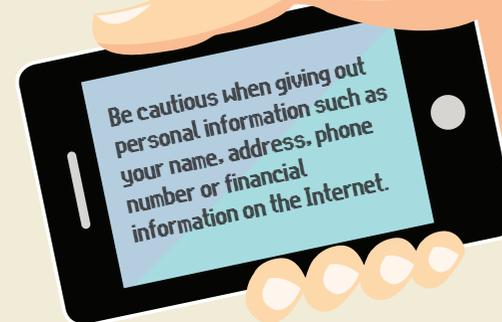
Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location or on a separate storage device.

<http://bit.ly/protect-data>

## 7. Secure your wireless network

Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review / modify your routers default settings, ensuring your Wi-Fi connection is password protected. Public Wi-Fi connections, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

<http://bit.ly/secure-wireless>



## 8. Protect your e-identity

Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure when making online purchases by looking for https:// or the padlock symbol in address bar. Also make sure that you've enabled your privacy settings when accessing/using social networking sites.

<http://bit.ly/protect-e-identity>

## 9. Avoid being scammed

Always think before you click on a link or file of unknown origin in an email. Don't feel pressured by any email comments or titles. Check and verify the source of the message if you are unsure. Never reply to emails that ask you to verify your information or confirm your user ID or password.

<http://bit.ly/spam-and-scam>

## 10. Call the right person for help

Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to the States of Jersey Police. If you need help with maintenance or software installation on your computer, consult with your devices manufacturer, service provider or a certified computer technician.

