Isle of Man Government
Reiltys Ellan Vannin

10 Online Safety Tips

Protecting your personal data

Most of us use the Internet to interact with friends, family and businesses but we should consider what information we are sharing and who we are interacting with to make ourselves safer online.

1. Keep your personal information private, such as your telephone number, date of birth and your address. Turn off your GPS location services and your device's camera when not using them.

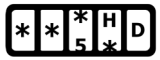
2. Avoid sharing your whereabouts online to avoid cyberstalking. Wait to post those concert or trip pictures until you get home so criminals are not aware when you aren't home.

3. Think twice before you post or say anything online; once it is in cyberspace, it is out there forever. Remember that what you post may impact you negatively in future.

4. Only do and say things online that you would do or say in real life. Think about how your decisions on what you post or say online can have positive or negative consequences later.

5. Speak up. If you see something inappropriate, let the website know by using reporting features where available and tell somebody you trust for advice.

6. Use strong passwords that also use a combination of numbers, letters, and symbols. Don't share your passwords with anyone.



We recommend using three random, but memorable, words with a mixture of upper and lower case letters, numbers and special characters (e.g. B1cycleSh0ePark!). Create a unique password for each of your important accounts such as your email, social media and online banking.

7. Be careful who you meet online. Simply because someone with mutual friends wants to add you on a website or app does not mean they are trustworthy.

8. Use privacy settings on social networking websites such as Twitter, Instagram, SnapChat, and Facebook. Think about who you want to see your posts before posting them. Here are some links privacy settings pages or instructions for popular social media platforms:

Twitter - https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public

Instagram - https://help.instagram.com/448523408565555

SnapChat - https://support.snapchat.com/a/privacy-settings

Facebook - https://www.facebook.com/help/1297502253597210

9. Be cautious when downloading applications on your smartphone — they may contain malware that could infect your device. Only download apps from trusted official app stores (e.g. Google Play, Apple App Store). Third party app stores can have a lot of fake apps that contain malicious code.

10. Be sure to review and understand the details of an app before installing it, and be wary of the information it requests. Some apps will allow you to use the app even if you say 'no' to certain requests for information or access to your device.

Website links correct as of July 2020

For more cyber security guidance and resources, please take a look at our OCSIA Knowledge Base

If you have any concerns, or have been affected by a cyber-related issue, report it to OCSIA by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia

Aware - Secure - Resilient


www.gov.im/ocsia


@cyberiom


IOM Government Office of Cyber-Security & Information Assurance