Telecommunications Regulatory Commission

Cybersecurity Guidelines

Consumer Cybersecurity Gudelines, 2017

- Use Strong Passwords
- Use Secure Web Browsers
- Update your Operating Systems
- Avoid Unknown or Unexpected Emails
- Do NOT give out Private Information
- Do NOT accept Unknown Friend Requests
- Post Sensibly
- Check Your Privacy Settings
- Know When to Ask For HELP!

1. Overview

Cybersecurity is a body of technologies, programs and practices, which are designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

This is of critical importance to ensure that people and their information are safe while using the internet and mobile devices.

2. Purpose

The purpose of these guidelines is to provide consumers with some suggested best practices to achieve personal security.

The internet and mobile phones are prevailing and exciting ways to communicate and learn. Therefore, it is important to ensure that usage is responsible so that people can stay safe while enjoying their online experience.

3. Statement of Guidelines

When considering cyber security, you may wish to consider implementing the following safeguards:

Strong Passwords – this can be a combination of UPPER and lower case letters, numbers and symbols. Eg. P@$sW0rd#1

Secure Web Browsers – when sharing sensitive information, look for 'https' and a padlock at the start of a web link/URL or another indication that the link is secure.

Updated Operating Systems – ensure that the management software for all of your electronic devices, also known as operating systems (Microsoft Windows, Mac OS, Linux, etc.), are regularly updated.

Updated Anti-Virus Software – ensure that you have an anti-virus software (AVG, Norton, Intel, etc.) on all electronic devices, which is up to date. Failure to use the latest version of such may result in your information being unsecure.

Avoid Unknown or Unexpected Emails – opening or responding to emails from people that you do not know or are not expecting to hear from may put you at risk of viruses and malicious software. Be vigilant because sometimes emails look like they come from trusted providers – but do not.

P.O. Box 4401, 27 Fish Lock Road, 3rd Floor LM Business Center
Road Town, Tortola, British Virgin Islands

Conceal Private Information – when using electronic devices, do not give out private information (health, financial, etc.) about you, your family or friends as this can lead to identity theft, financial loss or other mishandling.

Avoid Unknown Friend Requests – accepting friend requests from people that you do not know may put you and your online security at risk. Similarly, beware of people that create false accounts of people that you do know and send you another friend request under the guise of a known person. If in doubt, contact your friend some other way to verify the authenticity of the request.

Sensible Posting – electronic devices and social media are great mediums for expressing yourself. However, you should think about who else might see the message that you send or comment, video, or photo that you post. Information sent to another person or posted online cannot be retrieved. It can be used for multiple purposes, which you do not intend for it.

Check Privacy Settings – without your knowledge, privacy settings can change. This can happen for a variety of reason including application updates. Checking your settings regularly ensures that your audience is as intend. It is recommended that your social media account is set to private or friends only. Similarly, you should tell your friends to ask your permission before uploading or tagging you in a photo and you should do likewise. This ensures that posts are not viewed by unintended audiences.

Seek Help – when something uncomfortable happens online, find a trustworthy adult to speak to about it. If you notice something unusual or inappropriate online, report it to the relevant authorities. If your observation includes images or videos of child sexually explicit conduct/sexual abuse, report it to the Internet Watch Foundation's BVI Reporting Portal (https://report.iwf.org.uk/bvi).

4. Disclaimer

The above information is non-exhaustive and general in nature. It is provided only for guidance and should not be taken as providing a legal interpretation on any of the matters explored.