Cyber Safety and Security Tips and Best Practices

These security tips and best practices have been written to alert youngsters about the dangers of Internet on the occasion of the **Safer Internet Day 2022**. A section on the new cybersecurity and cybercrime law has also been included for the understanding of youths.

1. Back up your data

What you can do:

- Back up your data regularly, e.g., every week.
- Use an external hard drive to back up your data.
- Sign up to a cloud based service like Dropbox and do a cloud backup.

2. Choose unique passwords

What you can do:

- Use a different password for every online account you create.
- Try using a password manager, which will store and manage your passwords for you.
- Use a passphrase, rather than a password. Passphrases are usually stronger and easier to remember than passwords.
- You can add a mix of letters, numbers and symbols to make your passphrase more complex, for example “H@ppy Hol1d@ys 2 U @ll”.

3. Keep your devices and your apps up-to-date

What you can do:

- Keep the software for your devices and apps up-to-date.
- Set your system preferences to update them automatically.
- Remove any apps you do not use any more from your devices.

4. Turn on two-factor authentication

What you can do:

- Turn on two-factor authentication for your important accounts, such as your email and social media accounts.
- If several types are available, choose the option that is not SMS, as SMS is less secure. Still, using SMS as your second factor is still much safer than not using 2FA.

5. Avoid sensitive transactions on free Wi-Fi

What you can do:

- Avoid doing online shopping or internet banking on free Wi-Fi or an unsecure network.
- If you need to check your email, make sure you have two-factor authentication set up first.
- Use your own device where possible, not someone else's.

6. Install an antivirus and scan for viruses regularly

What you can do:

- Install an antivirus program on your computer.
- Run it regularly and clean up any viruses it identifies.

7. Be smart about social media

What you can do:

- Check the privacy controls on your social media accounts. Set them so only your friends and family can see your full details.
- Do not put too much personal information on your social media accounts.
- Remember our tip about passwords. If you share pictures of your pet on Facebook, make sure you are not also using your pet's name as your password.

8. Limit the personal information you give out online

What you can do:

- Stop and check before you give out any personal information.
- Make sure you know how the companies you deal with will contact you, and know what kind of information they will ask you for. For example, a bank will never email you with links to online banking and ask you to login.
- If you are not sure why you are being asked for information, call the company directly to check what they want it for.

What the youth should know about the new law?

The Cybersecurity and Cybercrime Act 2021

The Cybersecurity and Cybercrime Act 2021 caters for cybercrime targeting youngsters such as misuse of fake profiles, cyberbullying, cyber extortion, revenge pornography, amongst others. You being a youngster should be aware of the implications of doing wrong acts:

1. Misuse of fake profiles

Example: If you use a fake profile on Facebook, TikTok, Instagram or other social media to post derogative comments in the name of your friends or share their pictures to humiliate them, you could be liable to prosecution under **Section 16 of the Act.**

2. Cyberbullying

Example: If you use social media such as Facebook, TikTok, Telegram or Instagram to repeatedly instigate others to comment negatively on your friends' photos in order to shame them, both you and your friends could be liable to prosecution under **Section 17 of the Act**.

3. Cyber extortion

Example: If you use social media such as Facebook, TikTok, WhatApp, Telegram or Instagram to trick others into sending you nude photos of themselves and then blackmail them for money, you could be liable to prosecution under **Section 18 of the Act.**

4. Revenge Pornography

Example: If you use social media such as Facebook, TikTok, WhatsApp, Telegram or Instagram to post intimate images of your ex-girlfriend or boyfriend in order to take revenge from them, you could be liable to prosecution under **Section 19 of the Act.**

5. Failure to moderate undesirable content

Example: If you are the administrator of a Facebook page where people view and post content on a daily basis and it happens that someone posts content that promotes racism, you could be asked by the Police to remove that content. If you fail to do so, you could be liable to prosecution under **Section 23 of the Act.**

Contact Us

Computer Emergency Response Team of Mauritius (CERT-MU)

Tel: 210 55 20 | Hotline: 800 2378

General Enquiry: contact@cert.ncb.mu

Subscribe to Mail List: subscribe@cert.ncb.mu

Incident Reporting: incident@cert.ncb.mu

Vulnerability Reporting: vulnerability@cert.ncb.mu

Cybersecurity Portal: http://cybersecurity.ncb.mu

Website: www.cert-mu.org.mu