DATA PROTECTION OFFICE

This communiqué is issued by the Data Protection Office to sensitise citizens on the precautions, rights and avenues of remedy concerning those using social media and the Internet in Mauritius.

Precautions

1. Ensure you have adequate protection against viruses, spyware and malware on your device such as an updated antivirus and anti-malware software before browsing on the Internet.
2. Keep your device safe by applying updates on operating systems such as Windows, MAC IOS and Linux. Activate the firewall settings on your device.
3. Phishing is a fraudulent attempt mostly through emails to steal your personal information. These types of emails usually appear to come from a well-known organisation and ask for your personal information such as credit card number, national identity number, bank account number or password. Be careful when clicking links to another page or running an online application contained in phishing emails since attackers use these links to distribute their malware. You need to spam/block these types of emails in your email account.
4. When registering on websites, understand the terms and conditions associated to them.
5. Read carefully the website's or social platform's privacy policy before signing up a service. If you find the privacy policy not clear, do not sign up or limit the use of such service.
6. When creating an account, use a strong password that uses a combination of words, numbers, upper and lowercase letters, and special characters that is easy for you to remember, but tough for other people to guess. Skip common password elements like birthdates, anniversaries, and the names of your children or pets.
7. Keep separate email accounts for social networking and another one for shopping online to minimise the amount of personal information loss in case your email account is hacked.
8. Use different passwords on different systems or social networks.
9. Verify and configure the privacy settings of your social media account. The default settings for some social networks might make your information accessible to everyone and you need to control to whom you wish to give access. You have to verify the available options and choose the most appropriate privacy options according to your needs.

10. Social networks are accessed over the internet which is a global public resource. Cached copies of information may still exist on other computers on the network even after you have deleted them from your account. Therefore, make a selection of the type of information you post.
11. When accessing internet, you must delete internet history after each usage which will remove cookies of websites accessed. The cookies feature must also be disabled in order to prevent any unwanted tracking.
12. Control the amount of personal information you post and avoid posting data that could put you in a vulnerable situation such as your location data or posting information like being away from home as this may attract wrongdoers.
13. Install applications or third party applications from trusted sources and with great care as they may contain malicious settings which may retrieve your personal data.
14. Know the people you friend with, in real life if possible. Also, don't hesitate to use the "block" feature when the situation seems to call for it.
15. Encryption helps people to protect secrecy of personal information by encrypting documents, network space, portable devices and email messages.
16. Verify the padlock symbol or ''*https*'' tag on websites when performing online transactions. This indicates that personal information being sent is encrypted and the connection is secured.
17. You should take care when using public Wi-Fi as most of these hotspots transfer information in plain text. As a result, data transmitted is unencrypted and can be easily intercepted.
18. Teach children on internet safety and be aware of their online habits.
19. Always log out when you are done using an application or device.

You have the:-

1. Right to be informed about the purpose(s) of processing of your personal data, the consequences of such processing and your individual rights from controllers and processors.
2. Right to express your consent for the processing of your personal data for specified purpose(s).
3. Right of access to know whether data concerning you is being processed.
4. Right to rectification when your personal data are inaccurate or incomplete.
5. Right to withdraw consent to the processing of your personal data for specified purpose(s).
6. Right to erasure when your data is no longer necessary for specified purpose(s), consent is withdrawn or processing is unlawful.

7. Right to restrict the processing of your data by imposing a limit on its processing under specific conditions.
8. Right to object at any time to the processing of your personal data.
9. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or significantly affects you.

If you feel that a person or organisation is not meeting its data protection obligations, you have the right to lodge a complaint with the Data Protection Commissioner who has the power to investigate and advise prosecution whenever deemed appropriate.

Controllers and Processors have to abide by the following obligations:

- Collect necessary personal data for lawful purposes
- Bear the burden of proof for establishing an individual's consent concerning the processing of his personal data
- Notify any personal data breach to the Data Protection Office (DPO) and communicate the breach to the individuals concerned where necessary
- Ensure appropriate security and organisational measures are in place
- Destroy personal data as soon as the purpose of processing lapses
- Ensure the lawfulness of processing of personal data
- Comply with the requirements to process sensitive personal data
- Ensure appropriate consent for the processing of personal data of children is obtained
- Keep records of all processing operations under his or its responsibility
- Perform data protection impact assessments for high risks operations
- Ensure transfer of personal data outside Mauritius is lawful and is carried out with appropriate safeguards
- Comply with the requirements for prior authorisation or consultation from DPO in the required circumstances
- Designate an officer responsible for data protection compliance issues

DATA PROTECTION OFFICE
5th Floor, Sicom Tower, Wall Street,
Ebene
Phone: +230 460 0251
Email: dpo@govmu.org
Website: http://dataprotection.govmu.org