UNDSS Cybersecurity Advisory

The de-facto authorities in Myanmar are planning to impose a stricter "cybercrime" law, with ambiguous definitions for what may constitute a crime. The draft law — which has not yet passed the parliament - includes a ban of Virtual Private Network (VPN) connections.

Despite the law not having been passed yet, there have been recent multiple reports of spot-checks carried out by security forces on owners of smartphones. Some owners who have VPNs and social media apps installed on their phones have been harassed, extorted or arrested, with some having their phones confiscated. The contacts saved on these phones may become subjects of investigations, too.

In the light of these events, we recommend you read and share these tips with co-workers and with your dependents, who might have internet access:

1 . Phone calls (=calling phone number over the local telephone network) are unsafe and likely monitored by software that is programmed to recognize keywords you might use (such as "protest" or "PDF" etc.). Do not discuss sensitive issues over the phone! Choose encrypted Voice over IP services instead, such as on WhatsApp, Signal, Telegram etc., when available. Once the planned VPN ban is enforced, such communication may be restricted to UN-Wi-Fi networks.

2. Switch off your "Location services" on your tablet and smartphone for all applications where you do not absolutely need it (such as UN tracking or messaging apps like eTA or SCAAN). Your location may be monitored.

3. Switch off Bluetooth, when you don't need it. Remove Bluetooth-paired devices when you no longer use them.

4. Use official VPN service when connecting your official UN computer/ tablet/ smartphone only. A VPN protects us from people outside our VPN connections to monitor our internet traffic. If you connect to your local internet provider without VPN, your data and all your activities on the computer MUST be monitored by the provider and your usage kept on record for the authorities. Consult with your IT officer what official VPN connections are possible from your office networks, if you don't have it already working. The private use of a commercial VPN (connecting through a VPN with your private device and/or for other than UN official communication) may make it impossible for the UN to invoke "functional immunity" if you are apprehended.

5. Restrict applications on the smartphone/tablet when out of your office! Smartphones allow to temporarily disable applications on your smartphone, if you have admin rights. This feature is mainly used to for parental control and the restrictions can be reversed anytime with your password. Disabled applications do not appear on your smartphone's screen.

6. Do not give away any user credentials for any page or service to another person. That also applies to TRIP. Your credentials are not necessary. If you want your TRIP requests done by your assistant, let the person do that with her/his personal TRIP account and without your password. You are the only person responsible for your complete and correct data in your TRIP profile and travel requests.

7. Switch your computer on "sleep" or "standby" when you step out of your office. Your Password should be needed to "wake-up" your computer after that.

8. Do not post any content publicly on social media and check your privacy settings when you post on social media, such as Facebook, Twitter, Instagram, TikTok etc. and limit all your postings to your "friends"! If you have "friends" on social media whom you do not know personally, stop posting or exclude them. The Cybersecurity unit of the police is not only 24/7 screening social media profiles for critical postings, but they also rely on a wide network of informants for investigating and arresting specific profile owners.

9. Stay out of messaging groups if you don't know ALL participants! Group messaging lets multiple people carry on a group conversation. All replies from recipients are delivered to all recipients, in a group conversation thread. Such messaging groups may be created under a fake identity to gather information about participants invited into the group. Never accept messaging invitations from unknown individuals! If you do not personally know every single participant of that group, you should not join! If you need to join for essential formation, refrain from sending any messages and delete messages received.

10. Regularly delete your text messages. Check your messaging services for an automatically deletion of your messages after a certain time.

11. Regularly change your passwords! All your online passwords you use should be changed on a regular basis. There are a number of excellent password-vaults available for cross platform use, that can help you with reminders, password suggestions and encrypted password storage.

12. Report immediately any incident with security forces or telecommunications authorities related to your use of telecommunications devices to your Agency and to UNDSS.

13. Talk to your Organization’s IT Officer for more specific advice on internet security.

Best regards,

UNDSS Myanmar

17 June 2024