Protect yourself. Protect the UN.

Protecting the United Nation's data, resources, and reputation is vitally important. As the Organization stores, processes, and shares more and more information electronically, preventing breaches is paramount. The Office of Information and Communications Technology (OICT) has been implementing a global plan to strengthen information security. Progress to date has significantly addressed critical shortcomings and most urgent needs.

While these measures are critical, **every** staff member plays an integral part in information security. A mandatory information security awareness programme gives all UN staff and authorized ICT users the fundamental tools and knowledge to help strengthen information security. Advanced courses and additional resources are also available, providing everyone with comprehensive information to stay cyber safe, even at home.

>150 COUNTRIES

>400K MACHINES

impacted by the global ransomware attack "WannaCry"

DOs

DO use hard-to-guess passwords or passphrases. A password should have a minimum of 12 characters (more is stronger) using uppercase letters, lowercase letters, numbers and special characters.

DO use different passwords for different accounts. If one password gets compromised, your other accounts are not at risk.

DO change your passwords regularly, and change a password immediately if you suspect that it has been compromised.

DO shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended. A login must be required to start or wake-up. Set a passcode on mobile devices.

DO keep all areas containing sensitive information physically secured, and allow access by authorized individuals only.

DO store your critical data on central systems: approved secured locations, such as Unite Docs or Unite Connections.

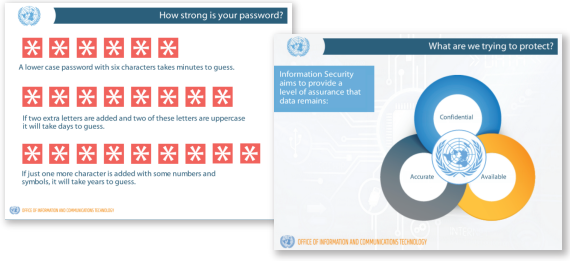
DO protect personally-owned home computers and other devices when working remotely. Regularly update security software including anti-virus protection.

DO use privacy settings on social media sites to restrict access to your personal information.

DO check social media sites for fraudulent accounts in your name.

DO enable encryption for your personal phones and other mobile devices.

Information Security Awareness Course



DON'Ts

DON'T share your password with anyone or allow others to use your username or password.

DON'T use email to transmit sensitive information or store it on mobile devices.

DON'T open e-mail, links or attachments in suspicious email messages (e.g. email address does not match name, unknown sender). If you receive anything suspicious, delete the message and report it immediately to abuse@un.org.

DON'T leave devices unattended. Keep all mobile devices, such as laptops, cell phones, and tablets physically secured. If a device is lost or stolen, report it immediately to the Unite Service Desk (call x3-3333, except in Asia which is x3333).

DON'T post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites, or share with anyone by email.

DON'T use public Wi-Fi hotspots. Wireless is inherently less secure.

DON'T use a public or shared computer (e.g. those at coffee shops and airport lounges).

DON'T select the "Remember My Password" option in websites, applications, or other systems.

DON'T install or download unknown or unsolicited software/apps.

DON'T connect USBs from unknown sources to your computer.

DON'T use personal email accounts (e.g. Gmail, Hotmail) or personal cloud storage services (e.g. Dropbox, Google docs) for work related communications and documents.

DON'T click on "cancel" or "exit" buttons in pop-up windows or unexpected warnings, instead close the windows by clicking on the "X" in the upper most right-hand corner of that window.

SOCIAL ENGINEERING

Be vigilant and exercise caution
NEVER give your passwords or login to another person or post private data to public sites or share by email

ACCESSING INFORMATION ON THE INTERNET

When sensitive information is communicated over the Internet, make sure the website address starts with "https://"

ELECTRONIC MESSSAGES AND PHISHING

Only click on URLs (website addresses and links) and open attachments when you are certain they come from a known and trusted source

PASSWORD SELECTION AND USAGE

NEVER use the same password for multiple accounts and NEVER share your password with anyone

1. TAKE THE MANDATORY INFOSEC AWARENESS COURSE
2. REVIEW GUIDES AND VIDEOS https://unite.un.org/infosec
3. REPORT INCIDENTS TO servicedesk@un.org
4. WHEN IN DOUBT, DON'T CLICK CONTACT: abuse@un.org

Recognizing suspicious emails. A few phrases and clues to look out for:

- "your account will be disabled in 24 hours"
- "email your username and password to IT Department"
- "copyright United Nations"
- a link to the UN email system that does not open https://webmail.un.org or https://unite.un.org/mail and instead opens a similar, but forged site with a different URL