How to protect yourself against
Remote Access Trojans* and other malware.

Keep your computer's (or mobile phone's) operating system and all software up to date (activate when possible automatic download of security updates)

In particular, take care in keeping your browsing software, e-mail client and extensions (including Java, Flash, PDF viewing software, etc) and office software suites (word processor, spreadsheet etc) up to date

Install and keep updated antivirus and firewall software on your systems

Do not click on links or download and visualise attachments from unwanted or otherwise unusual looking messages received through email, social networks or instant messaging tools.

If malware is detected by your anti-virus software before being installed, you may consider checking that all your updates have been done and recheck for the presence of other malware.

If any malware is detected as installed on your computer, don't forget that other malware can be installed at the same time, so proceed with a thorough examination of your computer. In particular with RATs, your personal information could have been compromised, thus you should check and if possible change all passwords recently used or that could be stored on your system. In addition, your banking information (credit card number, account number and credentials for online banking or online payment systems) could have been copied, so you should check your banking activity and if needed report the incident to your bank.

* Remote access trojans are malware that are used to spy on victims' computers (to access personal information, record on-screen activity, record webcam and microphone activity, collect passwords or credit card information). Remote access trojans are different from legitimate 'remote administration tools' that are often used in corporate networks to assist computer users or install software remotely, with the consent and knowledge of the users.