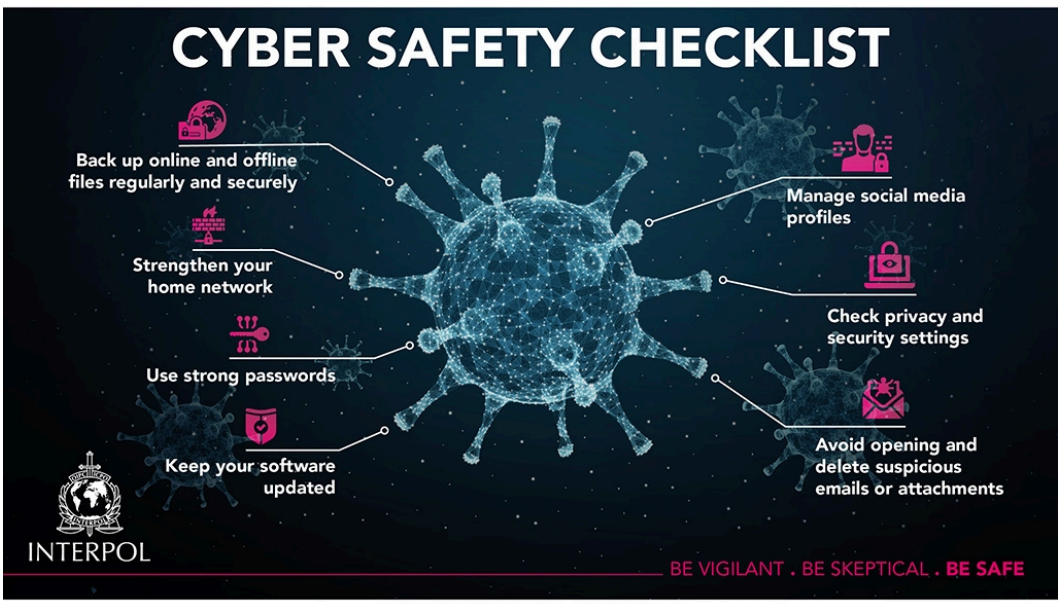
COVID-19 cyberthreats

Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception.

Cybercriminals are attacking the computer networks and systems of individuals, businesses and even global organizations at a time when cyber defences might be lowered due to the shift of focus to the health crisis.



PDF **Global landscape on COVID-19 cyberthreat** 704.24KB EN FR ES AR

Types of cyberattacks

Malicious domains

There are a considerable number of registered domains on the Internet that contain the terms: "coronavirus", "corona-virus", "covid19" and "covid-19".

While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware.

Malware

Cybercriminals are taking advantage of the widespread global communications on the coronavirus to mask their activities. Malware, spyware and Trojans have been found embedded in interactive coronavirus maps and websites. Spam emails are also tricking users into clicking on links which download malware to their computers or mobile devices.

Ransomware

Hospitals, medical centres and public institutions are being targeted by cybercriminals for ransomware attacks – since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom.

The ransomware can enter their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting a vulnerability in the system.

Recommendations and prevention tips

With an increasing number of countries encouraging citizens to stay, learn or work from home, now is the moment to focus on cybersecurity, whether it's for yourself or your workplace.

Keep your information safe

- Back up all your important files, and store them independently from your system (e.g. in the cloud, on an external drive);
- Always verify you are on a company's legitimate website before entering login details or sensitive information.

Check your software and systems

- Ensure you have the latest anti-virus software installed on your computer and mobile devices;
- Secure email gateways to thwart threats via spam;
- Strengthen your home network;
- Secure system administrations vulnerabilities that attackers could abuse;
- Disable third-party or outdated components that could be used as entry points;
- Download mobile applications or any other software from trusted platforms only;
- Perform regular health scans on your computers or mobile devices.

Be vigilant

- Talk to your family –including children – about how to stay safe online ;
- Regularly check and update the privacy settings on your social media accounts;
- Update your passwords and ensure they strong (a mix of uppercase, lowercase, numbers and special characters);
- Do not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender.

As always, if you believe you are the victim of a crime, alert your local police.

RELATED DOCUMENTS

PDF	**Global landscape on COVID-19 cyberthreat**	704.24KB	EN	FR	ES	AR