Version 3 April 2020

Dealing with digital security risk during the coronavirus (COVID-19) crisis

Key messages

- Digital security risk is increasing as malicious actors take advantage of the coronavirus (COVID-19) epidemic. Coronavirus-related scams and phishing campaigns are on the rise. There are also cases of ransomware and distributed denial of service (DDoS) attacks targeting hospitals.
- Individuals and businesses should exercise caution when they receive coronavirus-related communications, and use appropriate digital security "hygiene" measures (e.g. patching, use of strong and different passwords, regular backups, etc.).
- It is essential that governments raise awareness, monitor the threat landscape and publish easily accessible guidelines for digital security hygiene, in particular to vulnerable groups such as the elderly and small- and medium-sized enterprises (SMEs). Governments should also co-operate with all relevant stakeholders, including to provide assistance to operators of critical activities such as hospitals, as appropriate.

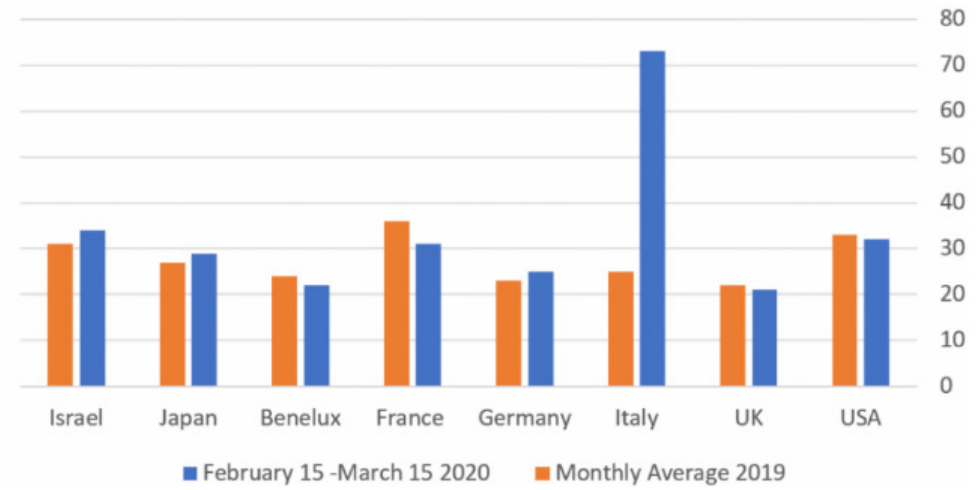
Digital security risk is increasing as the coronavirus (COVID-19) crisis unfolds

Malicious actors are leveraging the epidemic to make their attacks more successful. Since February 2020, there has been a surge in phishing[1] campaigns using COVID-19 content, including:

- emails with a coronavirus theme in the subject field or as an attachment filename
- emails or SMS impersonating the government in Australia and in the United Kingdom
- emails impersonating leaders or institutions, such as the World Health Organization
- emails, links or web applications mimicking legitimate initiatives.

A security firm found that Italian companies saw a rise in phishing attacks in March 2020. In Italy, one COVID-19 themed phishing campaign hit over 10% of all organisations in the country with an email luring recipients into opening a malicious attachment.

Figure 1. Spike of phishing attacks in Italy



Source: Cynet.

The Johns Hopkins University's interactive dashboard tracking coronavirus infections was mimicked by cybercriminals to spread password-stealing malware. The malware kit is for sale on underground dark web forums for USD 200.

An email campaign targeting healthcare and manufacturing industries in the United States in early March 2020 abused a legitimate distributed computing project for disease research. The email asked recipients to install an attachment in order to help find a coronavirus cure. The attachment contained malware stealing credentials and cryptocurrency cold wallets (cryptocurrency wallets that are stored offline).

Cybercriminals are also leveraging the popularity of tools used for teleworking such as Zoom for videoconferencing. Experts detected phishing campaigns with malicious attachments containing zoom in the filename, and over 1 700 new Zoom domain names have been registered since the onset of the pandemic, likely for malicious use. Other examples include new domains masquerading as the legitimate Google Classroom site.

[1] Phishing is the fraudulent practice of sending emails purporting to be from reputable organisations to lure individuals into revealing personal data, providing credentials, opening malicious attachments, etc.

There have also been cases of ransomware[2] and DDoS[3] attacks targeting essential activities such as hospitals, including in France, Spain and the Czech Republic.

- The Czech Republic's second largest hospital, the Brno University Hospital, was attacked on 12 and 13 March, causing an immediate computer shutdown in the midst of the coronavirus outbreak. The hospital, home to one of the largest COVID-19 testing facilities in the country, was forced to cancel operations and relocate acute patients to other hospitals.
- The university hospital trust operating in Paris and its surroundings (AP-HP) faced a one-hour DDoS attack on Sunday 22 March, paralysing two Internet facing addresses. The attack did not affect the health infrastructures.
- In Spain, a ransomware attack was launched against healthcare institutions on 23 March 2020.
- The United States Health and Human Services (HHS) Department faced a DDoS attack on 15 March 2020.
- In France, the information system of Marseille's local government faced a ransomware attack on 14 March 2020, the eve of local elections. All public-facing applications, as well as several internal systems, went offline.

Cybercriminals are counting on the likelihood that individuals and organisations will more easily fall for scams or pay ransoms in periods of stress and crisis, in particular those who lack good digital security practices or face organisational disruptions. **However, as their attack techniques and malicious code are not new, the application of basic digital security "hygiene" is an effective way to mitigate these attacks.**

Countries are already taking steps to counter heightened digital security risks

Across OECD countries, government agencies in charge of digital security are responding to the crisis by raising awareness, monitoring the threat landscape, providing assistance where appropriate, and co-operating with all relevant stakeholders, including at the international level.

- The United States' Cyber and Infrastructure Security Agency (CISA) set up on its website a new section entirely dedicated to security risks related to the COVID-19 crisis (www.cisa.gov/coronavirus). It includes alerts and recommendations regarding COVID-19-related scam and phishing campaigns, guidance on teleworking and a note on Risk Management for novel coronavirus.
- The European Commission, ENISA, CERT-EU and Europol released a statement on 20 March highlighting their cooperation to track COVID-19 related malicious activities, alert their respective communities and help protect confined citizens.
- The Canadian Centre for Cybersecurity published an alert assessing that the COVID-19 pandemic presents an increased level of risk to the digital security of Canadian health organisations involved in the national response to the pandemic. The Centre recommends that these organisations remain vigilant and take the time to ensure that they are engaged in cyber defence best practices. It also raises awareness to all organisations in Canada.
- In light of the evidence found during the resolution of the Brno Hospital incident, the Czech National Office for Cyber and Information Security (NÚKIB) ordered selected healthcare entities to carry out measures to enhance the security of key ICT systems. NÚKIB offered consultations and support to these entities.

In addition, many businesses, as well as industry and professional groups, are communicating to the public about digital security risks related to the COVID-19 crisis. They have created one-stop shops and resource libraries, and provide advice on specific topics such as secure telework.

[2] Ransomware is a type of malware that most often encrypts users' data and threatens to block access to data unless a ransom is paid.

[3] A DDoS attack floods a target's service (e.g. a website) with requests from a large number of IP addresses, resulting in the unavailability of the service for legitimate users, lasting from a few minutes to entire days.

Key recommendations

The general public is encouraged to adopt personal security measures to protect themselves and others:

- Treat with caution all communication related to the coronavirus crisis, even indirectly (e.g. teleworking tools) including emails, messages on social media, links, attachments and SMS.
- Keep computers, smartphones and other devices up to date with recent security patches.
- Regularly back up content, especially important data.

Governments and other stakeholders are encouraged to:

- Raise awareness on the increasing digital security risk related to COVID-19, in particular regarding phishing campaigns, ransomware and DDoS attacks. Offer practical guidance practical and tools (posters, diagrams, case studies) that can be picked up easily by other stakeholders.
- Publish information and guidelines for public sector organisations, businesses and individuals, including on emerging threats and good practices for digital security hygiene and teleworking.
- Support vulnerable groups, particularly the elderly and SMEs, as they will likely be spending more time online and may be less familiar with threats.
- Monitor the threat landscape (e.g. phishing, ransomware) and alert targeted communities.
- Encourage operators of critical activities, in particular in the health sector, to raise the level of digital security and provide them with specific assistance, as appropriate, in line with the OECD 2019 *Recommendation of the Council on Digital Security of Critical Activities* (OECD, 2019).
- Facilitate cooperation and information exchange on digital security risk between key stakeholders, both nationally and internationally, and at the sectoral level (e.g. health care).

Further reading

OECD (2019), Recommendation of the Council on Digital Security of Critical Activities, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456.

OECD (2015), Recommendation of the Council on Digital Security Risk Management for *Economic and Social Prosperity*, OECD, Paris, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

The OECD is compiling data, information, analysis and recommendations regarding the health, economic, financial and societal challenges posed by the impact of coronavirus (COVID-19). Please visit our dedicated page for a full suite of coronavirus-related information.