CYBER-CRIME DURING THE COVID-19 PANDEMIC

The pandemic of COVID-19 and the imposed lockdown, has led to more people to be confined at home with many more hours to spend online each day and increasingly relying on the Internet to access services, they normally obtain offline.

The dangers of cyber-crime have been there for many years, but the increase in the percentage of the population connected to the Internet and the time spent online, combined with the sense of confinement and the anxiety and fear generated from the lockdown, have provided more opportunities for cybercriminals to take advantage of the situation and make more money or create disruption. It is important to note that some more vulnerable segments of the population, such as children need to spend more time online for services such as schooling. This seismic change in how we live our lives and use the Internet has prompted a proliferation of e-crimes.

Common cybercrime techniques, such as phishing, have seen a spike. Phishing is the fraudulent practice of inducing individuals to reveal personal information, such as passwords and credit card numbers through fake websites or emails. New data gathered by Google and analyzed by Atlas VPN, a virtual private network (VPN) service provider, is shedding more light on the scope of this. According to the report, in January, Google registered 149k active phishing websites. In February, that number nearly doubled to 293k. In March, though, that number had increased to 522k - a 350% increase since January.[1]

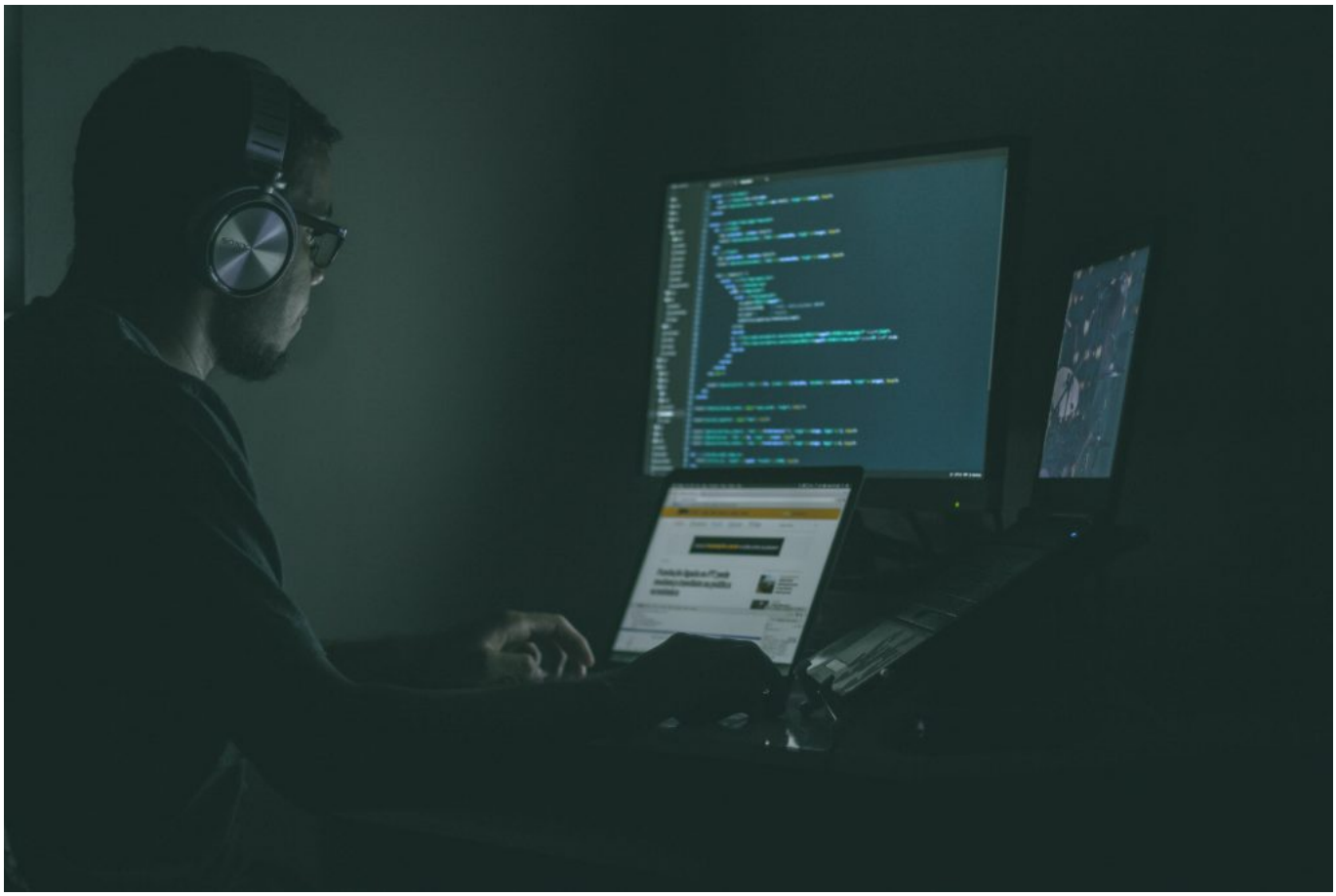
Countries all across the globe are reporting an increase in cybercrime during the pandemic.[2]
For instance, in Italy, the Polizia Postale, which is the law enforcement branch in charge of the cybercrimes, reported several kinds of scams and frauds[3] that came in the form of ads, emails, fake websites, but also through phone calls and messages. Cybercriminals are capitalizing on the anxieties and fears triggered by the pandemic, using malware, such as viruses, worms, trojan horses, ransomware and spyware, to invade, damage, steal or cancel personal data on personal computers. Stolen data can then be used for different malicious purposes, including accessing bank accounts and blackmailing the victims in exchange of ransoms.[4]
A "Corona anti-virus" software has also been flagged to the Italian law enforcement authorities. The application, BlackNet Rat, promises to protect the

user's device from coronavirus, but instead, it breaches the computer's security and takes control of the computer, effectively enabling the criminal to remotely control it.[5]

A sharp surge of fake or inappropriate drugs and medical equipment sold at a very high price to allegedly cure the Coronavirus was recorded on an increasing number of websites well-designed by criminals[6]. In connection to this, an increase in the trafficking of counterfeited products sponsored through emails and website, including hygiene items and facial masks, was recorded. Also, the Italian Police reported that in some cases legitimate crowd-funding campaigns to collect money in support of health institutions, under huge pressure during the past weeks, were deviated to alternative criminal pockets through fake websites.

Another common scam taking place on the web in this time of lockdown are promises[7] of fake investment opportunities. This phenomenon has gone global and both INTERPOL and the United Nations[8] have warned of specific online frauds such as this linked to the COVID-19.[9] In the United Kingdom, an increase in scams and attacks targeting businesses has also been witnessed. For instance, emails pretending to relate to the government's new grant scheme have stolen money or downloaded ransomware[10].

Financially motivated hackers have in fact been profiting from such feelings of uncertainty to target businesses and specifically retool existing malicious programs, such as ransomware -which is a type of malicious program used by hackers to take control of files in an infected system - and then demand large payments to recover them[11]. For example, companies such as Cognizant, an information technology service provider, reported that it was hit by a "Maze" ransomware cyberattack, which is a specific attack involving hackers threating to release information on the internet if the target company fails to pay[12].



On a similar note, with regard to attacks against other key organizations and infrastructure actively dealing with the virus response, INTERPOL's Cybercrime Threat Response Team has also warned of cybercriminals using ransomware to hold hospitals and medical services digitally hostage, preventing them from accessing vital files and systems until a ransom is paid[13].
Several countries have registered cyber-attacks from unknown hackers at the expense of national health institutions, extremely critical infrastructures during the time of a pandemic. In Italy, on 1st April, a cyber-attack was conducted against the Spallanzani Hospital,[14] a center of excellence in the research on the coronavirus. A week earlier, also the Spanish Police has issued a warning that the entire computer system of Spain's hospitals was being targeted in a cyber-attack by a ransomware that targets enterprise and government agencies.[15]
During the same week, also the World Health Organization (WHO) has been attacked.[16]

At the same time, the lockdown has also significantly increased concerns about vulnerable persons online. While children, for instance, are greatly benefiting from e-schooling, they are equally more exposed to threats coming from the internet:[17] file-sharing abuse, inappropriate content, and the grooming of children for sexual purposes are some of the dangers their parents should be aware of in these challenging times. The elderly, who usually rely on

offline shopping and have now to purchase what they need from the internet, equally find themselves more exposed to cybercrime.

Another side-effect of the protracted lockdown has been a growing demand for pornography. The industry has seen an increase in the number of users, but also concerns are being raised about vulnerable categories being pushed into exploitation, including drug addicts and children trafficked by families in need.[18]

Although the risk of being attacked will remain, some mitigation measures may help users and employers. For the users, it is recommended to be very vigilant about phishing emails and websites, practice good cyber hygiene, use only trusted wi-fi networks and consider adopting a password manager to help to avoid using the same password for multiple websites. It is also important to use double channels of communications with counterparts before transferring sensitive data or downloading a file from an email that may contain malware. Sending an SMS, a WhatsApp message or making a quick call to make sure that the sender is a colleague or friend can prevent a cyber-attack. Rather than immediately clicking links in emails, it is advisable to look for information from trusted websites. Regarding the collective conference calls, which are being used more frequently, it is important to be mindful of sharing screens or sending screenshots that may contain sensitive information. Employers can, among other things, make sure a secure remote access to the organization's files is set up, provide the right security capabilities[19] and ask employees to avoid working with their personal computers.[20] Finally, it is recommendable that they provide employees with appropriate courses to enhance their cyber-security knowledge.

---

[1] https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine/

[2] https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

[3] https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-rischi-e-minacce/index.html

[4] https://www.ilmessaggero.it/italia/coronavirus_reati_truffe_online_ultime_notizie-5111692.html

[5] https://www.techradar.com/news/corona-antivirus-infects-victims-with-malware and https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html?fbclid=IwAR13sai7vB5-_eBSRopHb0wqBqOX24i8hvhz3YOR06toRUMYVj6k3iV0Cpc and https://www.dqindia.com/cyber-crimes-surge-coronavirus-era/

[6] https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation

[7] https://www.scamwatch.gov.au/news/warning-on-covid-19-scams

[8] UN health agency warns against coronavirus COVID-19 criminal scams: https://www.uneca.org/stories/un-health-agency-warns-against-coronavirus-covid-19-criminal-scams

[9] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19

[10] https://www.aljazeera.com/news/2020/04/uk-coronavirus-scams-online-doorstep-200414220652029.html

[11] https://www.reuters.com/article/us-health-coronavirus-cyber-corporations/hacking-against-corporations-surges-as-workers-take-computers-home-idUSKBN21Z0Y6

[12] https://www.reuters.com/article/us-cognizant-tech-cyber/cognizant-hit-by-maze-ransomware-attack-idUSKBN2200YA

[13] https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[14] https://www.poliziadistato.it/articolo/155e84aa96b6ae8096181274

[15] https://murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html

[16] https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-

who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

[17] https://globalinitiative.net/crime-contagion-impact-covid-crime/

[18] Men's Health, 23 March 2020, https://www.menshealth.com.au/coronavirus-pornhub-spike-in-traffic-free-premium-membership.

[19] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[20] https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks