LIFE AFTER COVID-19

مؤسسة دبي للمستقبل
DUBAI FUTURE FOUNDATION

FUTURE TRENDS

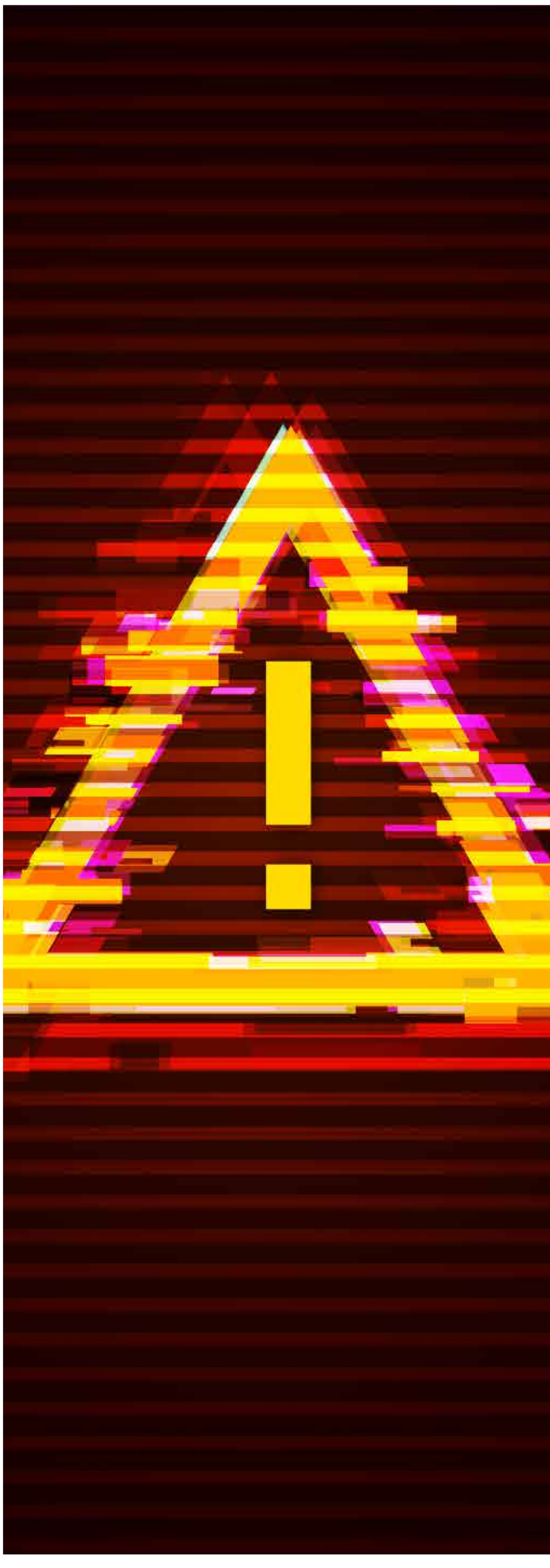
CYBER-SECURITY

INSIGHTS IN BRIEF

A rise in cyber-attacks has been reported by countries worldwide as the COVID-19 virus continues to spread.

The growth in cyber-crime has been driven by increased vulnerability in digital infrastructures now that IT and IT security staff are working remotely and opportunistic hackers are looking to exploit increased reliance on digital systems.

COVID-19 is causing countries to rethink their stringent data privacy policies to allow for the tracking and tracing of the virus. However, the loosening of these laws has provided hackers with further opportunities to target individuals.



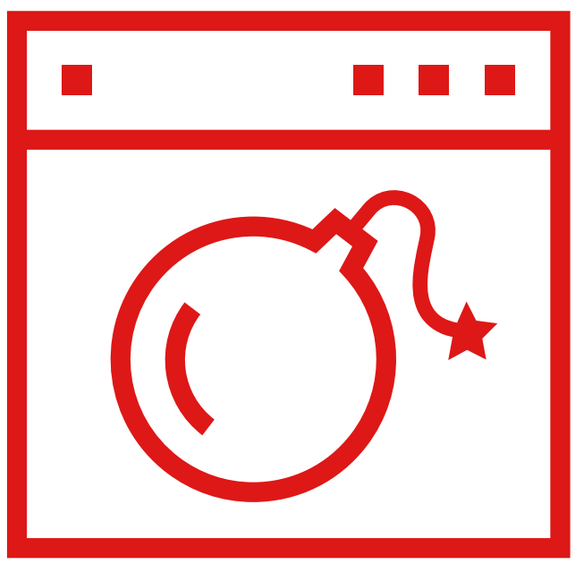
CURRENT SITUATION

A rise in cyber-attacks has been reported by countries worldwide as the COVID-19 virus continues to spread. Phishing emails alone have increased by over 600% since February, with attackers targeting individuals and institutions through email hacking and suspicious links, seeking to acquire log-in details and financial information.[1] During the first week of April alone, Google blocked 18 million phishing emails on its platforms.[2] Although phishing is one of the cheaper and easier forms of cyber-crime, there have been other types of cyber-attacks. For example, cyber-criminals have also created more than 100,000 new COVID-19 web domains in an effort to trick individuals into giving out their personal data.[3]

During the first week of April alone, Google blocked

18 million phishing emails

on its platforms



Cyber-criminals have created more than

100,000 new COVID-19 domains

[1] Muncaster, P., "#COVID19 Drives Phishing Emails Up 667% in Under a Month", InfoSecurity, 2020.
[2] "Protecting businesses against cyber threats during COVID-19 and beyond", Google, 2020.
[3] Miles, R., "How to protect against cyberattacks when working from home during COVID-19", Intelligent CIO, 2020.

This increase in cyber-attacks has several drivers. There is more vulnerability within digital infrastructures now that IT and IT security staff are working remotely and unable to detect the attacks as quickly, partly due to the fact that multiple servers are being used. Anxiety about COVID-19 is leading people to click on dangerous links in content that appears to be helpful information. Also, opportunistic hackers are looking to exploit the increased reliance on digital systems, such as those being used by hospitals and public service organizations.

The healthcare sector is one of the most vulnerable currently to cyber-attacks. Hospitals, medical centers and public institutions worldwide are being targeted, primarily through ransomware attacks. Healthcare professionals require digital infrastructure to tackle COVID-19 and cyber-criminals have been exploiting this necessity, believing the organizations will have no choice but to pay to re-enter their systems.[4] The World Health Organization has also experienced attempted attacks designed to target the personal information of their staff.[5]

[4] "COVID-19 cyberthreats", Interpol, 2020.
[5] Warrell, H. & Manson, K., "State-backed hackers using virus to increase spying, UK and US warn", Financial Times, 2020.

£1.6m

in losses due to COVID-19 related fraud in the UK.

Cyber-criminals are also using the healthcare crisis to sell fake medical supplies. There have been several scams, including individuals or entities impersonating government officials, claiming COVID-19 medical breakthroughs and promoting sales of bogus or non-existent medical products.[6] The UK's National Fraud Intelligence Bureau (NFIB) has reported £1.6 million in losses due to COVID-19 related fraud.[7] One victim paid £15,000 for masks that never arrived.[8]

[6] "Jackson Jr., J., "COVID-19 Raises Financial Crime Risks, Report Says", Law 360, 2020.
[7] Townsend, M., "Fraudsters exploiting Covid-19 fears have scammed £1.6m." The Guardian, 2020
[8] Sattler, J., "Latest Covid-19-related cyber security news: Hospitals under attack", F-Secure, 2020.

The financial and oil sectors are also being hit hard. In the UAE, the Central Bank has warned customers against fraudsters looking to hack bank accounts. With countries worldwide looking to potentially digitize currency and all financial transactions, cybersecurity is even more vital. The intergovernmental Financial Action Task Force has published a report outlining various risks that businesses are facing as a result of COVID-19, including the threat of increased fraud, such as by criminals impersonating officials and or using virtual assets to move illegal funds.[9]

The oil sector is no less vulnerable and is one of the hardest hit sectors in the MENA region.

The oil sector is no less vulnerable and is one of the hardest hit sectors in the MENA region. Several companies in many countries, including the United States, Malaysia, Iran, Oman, the UAE, and Saudi Arabia, have been targeted with phishing emails supposedly sent on behalf of a real oil and gas company in Egypt, the state firm Engineering for Petroleum and Process Industries (Enppi). The hackers were looking to acquire sensitive details on individuals and oil production, information they could then sell on the dark web.[10]

[9] Jackson Jr., J., "COVID-19 Raises Financial Crime Risks, Report Says", Law 360, 2020.
[10] Paraskova, T., "Hackers Have Ailing Oil Industry In Their Crosshair", Oil Price.Com, 2020.

These break-ins, however, are not limited to governments or organizations. Video conferencing platforms are also at risk. With so many people congregating on these platforms for meetings, classes, appointments, family conversations and commercial purposes, such tools have recently experienced a number of security breaches. Participants have reported an influx of so-called 'zoom bombers', people who would randomly join a meeting and begin disrupting it with illegal content. There were also reports that recordings of videos on the Zoom platform were not being saved to a secure cloud storage space and were then disseminated online. These included private business meetings and personal conversations with family and friends.[11] Although Zoom has now put in place multiple verification layers, including adding mandatory meeting passwords and admission options for meetings, there is still considerable concern around conferencing apps.

Other platforms such as online gaming have also been hit by cyber-attacks. With an increase in the number of Nintendo accounts, due to the popularity of communal games such as Animal Crossing where real people can connect virtually,[12] there have been attempts to hack the network to acquire personal financial information. In response, Nintendo has disabled the ability to log into a Nintendo Account through a Nintendo Network ID (NNID).[13]

[11] O'Flaherty, K., "Zoom Security: Here's What Zoom Is Doing To Make Its Service Safer", Forbes, 2020.
[12] Basu, T., "Why games like Animal Crossing are the new social media of the coronavirus era", MIT Technology Review, 2020.
[13] Warren, T., "Nintendo confirms 160,000 Nintendo Accounts accessed in hacking attempts", The Verge, 2020.

OPPORTUNITY

During and after COVID-19, our lives will become even more dependent on digital infrastructure. However, this dependence also means an increase in cyber-threats. Countries have developed cybersecurity strategies and web security policies to counter these increasing risks. In the UAE, these have been led by entities such as the Telecommunications and Regulatory Authority (TRA) and the Dubai Electronic Security Center (DESC). Globally, measures such as the European Union General Data Protection Regulation and the 2018 California Consumer Privacy Act have been designed to protect privacy on the internet. However, COVID-19 is now causing countries to rethink policies on stringent data privacy to allow for the tracking and tracing of the virus. Countries such as South Africa have implemented exemptions to their data privacy procedures to allow for the aggregation of data during a crisis.[14] However, there are fears that the loosening of data privacy laws could provide hackers with further opportunities to target individuals by using contact-tracing apps to trace a person's location and hack into their phones.

[14] Daniel Visser, Research Call, C4IR South Africa, 2020.

COVID-19 is now causing countries to rethink policies on stringent data privacy to allow for the tracking and tracing of the virus.

Some companies are dealing with this issue by strengthening their systems. Google and Apple released a statement assuring users that their contact-tracing system will be encrypted and that the Bluetooth connection used for location tracking will be strong enough not to be hacked for location and device details.[15]

A group of Republican senators in the US Senate, on the other hand, is looking to introduce a privacy bill that would regulate data collected by COVID-19 contact-tracing apps. Entitled the COVID-19 Consumer Data Protection Act, the bill would provide Americans with more transparency on where and how their data is being used.[16] Although the details surrounding the bill are still unclear, the potential regulation poses a question about responsibility for cybersecurity. Is it the role of the system provider or that of the regulator? From Google and Apple's perspective, cybersecurity is the company's responsibility - ensuring the system is impenetrable. Governments, however, have viewed the role of tracing and security as their responsibility. This has led to a wider discussion around whether there needs to be greater government centralization, as countries with centralized digital infrastructures, such as China and South Korea, seem to be handling the crisis better than those with more diversified infrastructures such as the USA and UK.[17]

[15] McGee, P. & Murphy, H., "Apple and Google boost privacy and accuracy of contact tracing system", Financial Times, 2020.
[16] Lyons, K., "Senators' plan for reining in contact tracing apps doesn't make a lot of sense", The Verge, 2020.
[17] Goldsmith, J., "Internet Speech Will Never Go Back To Normal", The Atlantic, 2020.

In the MENA region, COVID-19 has pushed companies to re-assess their cybersecurity systems. Trend Micro, a multinational company with a base in the region, cited 8,434 threats to their software company over the past few months. The GCC is already one of the most vulnerable regions in terms of malware attacks, with almost 5.5 million incidents recorded over the past year. Saudi Arabia alone reported 2.4 million attacks during 2019.[18] In response to such vulnerabilities, companies are looking to implement multiple layers of cybersecurity, including further system firewalls and authenticated virtual private networks (VPNs). (This is discussed further in the Dubai Future Foundation Telecommunications report).[19]

The GCC is one of the most vulnerable regions with almost

5.5 million malware attacks

recorded over 2019

2.4 million attacks in KSA

during 2019

[18] Binali, M., "Remote working calls for regional organisations to overhaul their cybersecurity postures", Arabian Business, 2020.
[19] Telecommunications, Dubai Future Foundation, April 15 2020.

Within e-commerce, which is estimated to reach a market size of US$28.5 billion in MENA by 2022,[20] companies are attempting to deal with increased cyber-attacks and fraud. For example, Amazon, which had previously implemented an in-person verification process for sellers, is now piloting video calls to verify third-party vendors by ensuring that identification documents match the applicant.[21]

New technologies are also being used to update current cybersecurity platforms. Several intelligence agencies worldwide are looking into the use of AI to counter cyber-threats. Machine learning can be used to analyze data sets and to identify patterns and connections in attacks at far greater speed than intelligence officers can do by conventional means.[22]

Within the industrial sector, cyber-attacks have also increased with the growing reliance on the internet of things (IoT) for tracking and monitoring of supplies. Given that the sector makes up around 8% of the MENA region's GDP, it is detrimental to the economy for this sector to be disrupted further. COVID-19 has demonstrated to many companies that their supply chains are not transparent, even with new technologies in place. Such companies will therefore need to reassess their use of technology, and ways to deploy it responsibly.

[20] "Ecommerce in MENA expected to reach $28.5 billion by 2022: report", MENA Bytes, 2019.
[21] ANI, "Amazon pilots using video call to verify third-party sellers", Gulf News, 2020.
[22] Warrell, H., "UK intelligence urged to step up AI use to counter cyber threats", Financial Times, 2020.

LOOKING AHEAD

Short term insights
(during the COVID-19 outbreak)

1

With IT security staff working remotely, and unable to detect cyber-attacks as efficiently, given that employees are no longer using unified servers when working at home, there may be new measures put in place such as screen sharing and desktop monitoring to ensure that employees are safe. This will likely raise questions around data privacy while working remotely.

Short to long term insights
(post COVID-19)

1

Automation will become increasingly common in the sphere of cybersecurity. Government entities may begin to look into implementing AI-based cybersecurity systems to provide ongoing analysis of cyber-threats and potential attacks. Automation will also mean virtual audits of IT systems using self-authenticating tools such as blockchain.

2

Telemedicine will continue to grow as a form of healthcare, worldwide, during and post COVID-19. Standardized guidelines for how medical devices should be created and operated, including the security components of the device, will need to be put in place swiftly to ensure their safety and authenticity.

THE LONG VIEW

As technology advances, cyber-criminals and their attacks will become smarter and more difficult to combat. Quantum computing will become an important factor in cybersecurity, analyzing and repelling attacks within seconds.

On the other hand, autonomous vehicles may become vulnerable to cyber-espionage and terrorist attacks and will need to utilize AI systems to identify potential threats and patterns.

While cybersecurity, as a market, is growing, individuals working in the field may lose their initial jobs. With so much more automation in the future, individuals will become the coders and developers of the products that monitor systems and resist attacks, but not the monitors themselves. This will lead to a global AI-driven cybersecurity sector and this could potentially breach data privacy laws if machine learning overcomes restrictions on the use of personal information. There will need to be continuous adaptations to the systems put in place to ensure security and privacy for the individual.