Rise In Cybercrime Due to COVID-19 Pandemic, Increased Device Connectivity

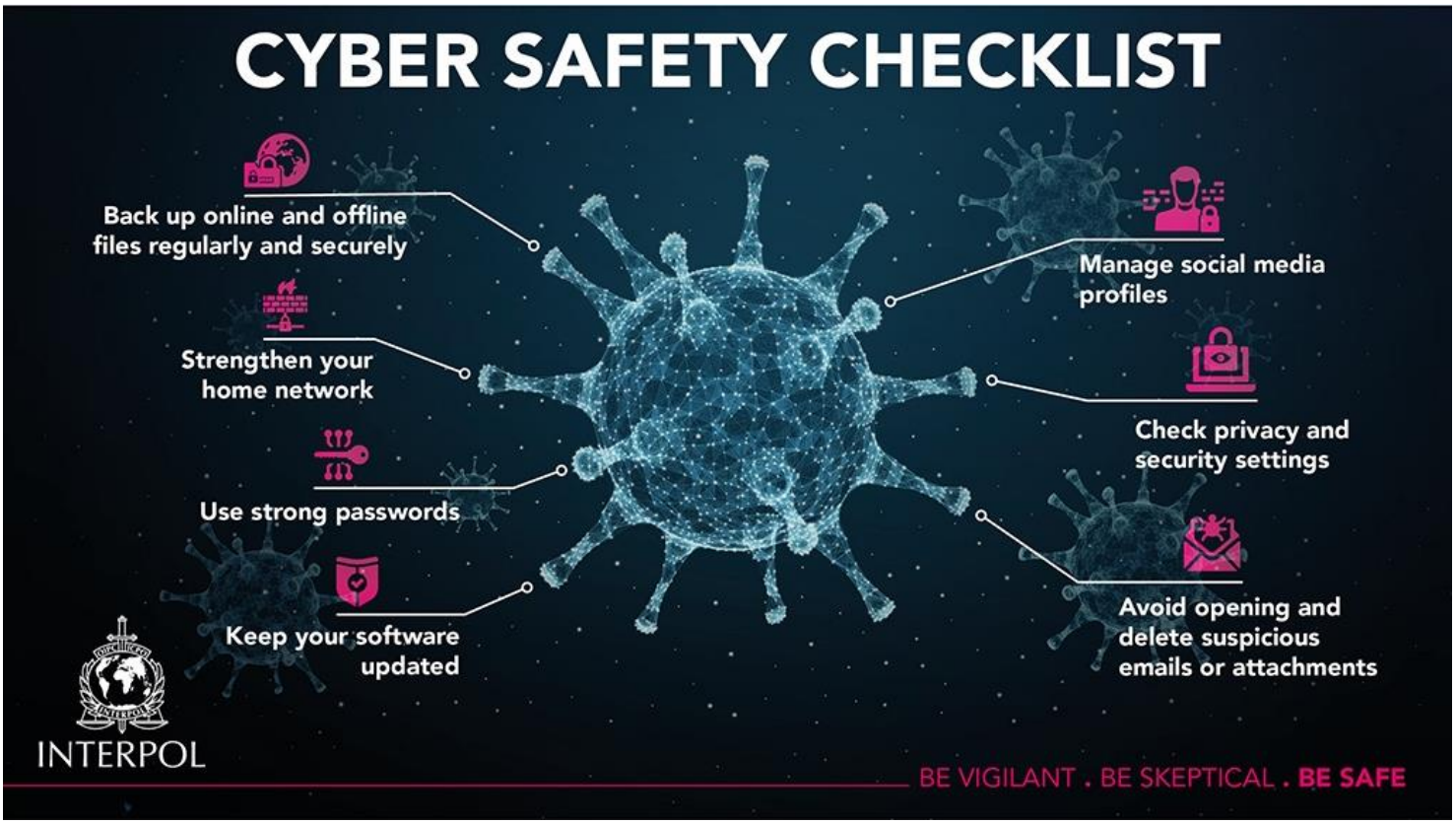
Alongside the rise in cybersecurity positions has been a rise in cybercrimes, with the largest cyber crimes ever being the LinkedIn breach causing the loss of 700M records in 2021, and the 2022 Shanghai police data breach of one billion records that we expand on more in this newsletter. What is responsible for the worldwide rise in cybercrimes? It appears that crime levels have risen due to remote work because of the COVID pandemic and increased IOT device connectivity, increasing the number of attack vectors by which hackers can gain entry into company systems.

According to ThoughtLab, the average number of cyberattacks and data breaches increased by 15.1% from the previous year. Half of US businesses still have not developed a cybersecurity plan, and cybercriminals can penetrate companies with a 93% success rate according to pentesting projects by Positive Technologies. Compromised credentials is the primary attack node (71% of attacks) that cybercriminals use to gain access to company datacenters, often due to the use of simple passwords, highlighting the importance of two-factor identification and zero trust architectures. Complex supply chains and a multitude of interaction points with vendors and third parties underscore the importance of cybersecurity solutions that include vendor and third party risk management.

Varonis provides comprehensive information regarding a variety of cybersecurity topics, offers a free security webinar, and provides the following comprehensive statistics:

- 95 percent of cybersecurity breaches are caused by human error. (World Economic Forum)
- The worldwide information security market is forecast to reach $366.1 billion in 2028. (Fortune Business Insights)
- The U.S. was the target of 46 percent of cyberattacks in 2020, more than double any other country. (Microsoft)
- 68 percent of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only five percent of companies' folders are properly protected. (Varonis)
- 54 percent of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks. (Sophos)

- Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 percent of companies. (Cisco)
- 43 percent of all breaches are insider threats, either intentional or unintentional. (Check Point)
- Data breaches exposed 22 billion records in 2021. (RiskBased Security)
- Approximately 70 percent of breaches in 2021 were financially motivated, while less than five percent were motivated by espionage. (Verizon)
- In 2021, nearly 40 percent of breaches featured phishing, around 11 percent involved malware, and about 22 percent involved hacking. (Verizon)
- There were 1,862 recorded data breaches in 2021, surpassing the 2017 record of 1,506 breaches. (CNET)
- The top malicious email attachment types are .doc and .dot which make up 37 percent; the next highest is .exe at 19.5 percent. (Symantec)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)
- Around 40 percent of the world's population is offline, making them vulnerable targets for cyberattacks if and when they do connect. (Data Reportal)



G2M Communications, a re-grate-it brand.