**The Impact of Corona Virus on Cyber Security**

The Covid-19 (Coronavirus) pandemic is spreading globally at an alarming rate, and along with disruption in global health, it is also causing damages to social, economic and political systems all over the world. Nearly the entire world workforce is now working remotely from homes, causing them to heavily rely on digital tools and remote means of communication. This has allowed cyber criminals to capitalize the situation and actively exploit the Covid-19 crisis. According to the [Global Cyber Security Market Analysis](https://www.researchandmarkets.com/reports/5021764/global-cyber-security-market-analysis?utm_source=dynamic&utm_medium=GNOM&utm_code=b4lhdg&utm_campaign=1387344+-+Economic+Impact+of+COVID-19+on+Global+Cyber+Security+Market&utm_exec=cari18gnomd) report released in April 2020, the global cyber security market is forecasted to grow at a very slow average rate of 6.2% per annum up to the year 2023 – as a consequence of economic downfall due to the 2020 coronavirus pandemic.

In a broad perspective, coronavirus crisis has already resulted in a massive overload on internet traffic. This is evident from the increased workload on technical support teams, weaker online security controls, workplaces with lesser secure devices and more exposure to risk. People are using online channels as a default medium for shopping as well as basic means of communication. Consequently, hackers are now more tempted to insert malicious code and generate more vulnerabilities with high-risk threats.

**The Risk Factors**

Let us consider some major changes resulting from the coronavirus crisis under this scenario.

Firstly, with covid-19, organizations are now more dependent on outsourced tools to keep running their business operations and to ensure their survival. This is highly likely to result in sensitive data being exposed, thus increasing the potential for supply chain attacks.

Furthermore, since most online operations that have end-customers are using web-based services, and with most of these end users being unwary of risks, there are clearly more opportunities for cyber criminals. This explains why online businesses are now more exposed to cyber threats and that the trend will keep growing during the coronavirus crisis.

Another trend on the rise is increased phishing attempts emphasizing on false information of Covid-19. Such attempts take advantage of a panicked masses using social engineering methods, and eventually may lead online users or an organization to take wrong decisions – all to the disadvantage of their cyber security.

**Threats to Look Out For**

The National Cyber Security Center (NCSC) has removed approximately 2000 corona-related online scams in March 2020 which included 471 online shops selling fake coronavirus relief items, 832 advance-fee fraudulent websites promising a reward in return for registration payments and another 555 malware sites intended to harm their visitors.

Malicious websites have been set up in times of coronavirus with their domains registered with names including the word ‘corona’ or ‘coronavirus’. Spam emails are being made to grab a user’s attention by offering high-demand Covid19 products such as masks, sanitizers and vitamins. If not this, then they intend to create panic and build a discourse of trust by presenting conspiracies about the pandemic. Moreover, phishing emails are supposedly being received from organizations like World Health Organization where the scammers carefully craft emails appearing to be coming from these organizations and asking users to open phishing links or malicious attachments. In some instances, there has also been an increase in fake HR office emails where you are requested to participate in a fake coronavirus survey by impersonating as your IT or HR department and trying to steal username and password of users.

In other instances, charities have also been contacted by fraudsters that claim to be from a legal organization and proposing to provide information of elderly or poor people at risk and in need of charity support. They are then asked to click on a fraudulent link to get their information which leads them to a fake website or are requested to pay money for the virus victims.

Similarly, the move towards online medium and the same need as before for receiving instant response even in this crisis era means that client-side frameworks and third-party applications have to be involved directly on the websites. They are expected to launch effective marketing campaigns with efficient services and improved technical functionality. In the midst of this crisis, third-party code is being attacked by malicious campaigns and it is only a matter of time that the next breach takes place.

In the wake of this crisis, for online businesses, some factors to be considered are attacks carried through third-party vendors, website attacks and those on storage hosting providers. In few cases, the hackers may compromise a software update eventually impacting your website visitors. In many other direct cases, they exploit third party vendors which can directly access your website code. Once inside they abuse the code and steal your data maliciously.

**Managing the Threat Landscape**

For remote workforce, organizations can take some important step to ensure security as employees work from home. They need to ensure that the remote access systems have been configured securely and are fully patched. Moreover, they should also have the capability to endure DDoS attacks and move their users towards approved and better solutions. Ecommerce websites also need to adopt online security best practices and propagate [safe buying](http://www.cardzgroup.com/ContactSmartCard.html) to their customers to ensure long term customer satisfaction.

**Final Thoughts…**

The coronavirus pandemic outbreak has resulted in an increase in the likelihood and impact of cyber fraud as organizations face massive financial and operational challenges. The nature of threats is also changing as cyber criminals exploit uncertainty, fear and panic arising out of the covid-19 crisis.