Dmitriy Yeremin

CYSE 201S

4/17/2026

Case Study: Covid 19 and the Cybercrime That Followed

Introduction

COVID-19 has been a draping curtain of pain, distress, uncertainty, and a feeling of no going back. Outside of all the societal division and medical conspiracies, it ushered in a sweeping swarm of cyber attacks that preyed on the vulnerable. COVID-19 became mainstream news in January 2020. Alawida et al. (2022) noted that the World Health Organization (WHO) declared COVID-19 as a pandemic on March 11, 2020. After this day, American society came to a screeching halt. Businesses closed their doors, people were told to stay at home, and there was no clear message from the media on the progress of the pandemic.

Analysis

Although society was becoming stagnant, the cybercrime world was working overtime. Compared to the previous year, there was an 8% increase in data breaches from September 2020 to September 2021, totaling 1,291 breaches and affecting over 155.8 million people (Alawida et al., 2022). From a psychological standpoint, fear and anxiety impaired people's critical thinking, making them more susceptible to deception. The urgency surrounding pandemic news also caused people to react emotionally rather than rationally, making phishing emails such as fake vaccine updates or government alerts particularly effective. Beyond data breaches, attacks including phishing, malware, DDoS, BEC, and APT became increasingly common. With people confined to their homes for extended periods, the likelihood of clicking on

malicious links increased significantly. Additionally, those working from home for the first time were likely unfamiliar with the security risks of using an unsecured home network.

Solutions

There are no groundbreaking solutions here, but there are some strong starting points. On the technical side, organizations should have required cybersecurity training for employees before allowing them to work from home, as the likelihood of incidents increases when working outside of a secured, layered network. A barrier to this solution is that many companies cut their cybersecurity budgets during the pandemic to save money. From a social science perspective, public health and cybersecurity messaging should have been better coordinated, as clear and trusted communication from authorities reduces the panic that attackers exploit. A barrier to this approach is that people were already overwhelmed with information during the pandemic, making it less likely they would retain or even consider cybersecurity guidance relevant to their situation.

Reflections

In society cybersecurity is viewed as a purely technological problem. COVID-19 proved that human behavior is just as much of a vulnerability as any software flaw. Understanding the psychological and sociological factors that make people susceptible to attacks is just as important as building a better firewall. A multidisciplinary approach gives us a more complete picture of how to protect people, not just systems.

Conclusion

The COVID-19 pandemic exposed how quickly cybercriminals can pivot their attack methods to tailor social events and exploit human vulnerabilities at scale. This event proves to us again that we need more than just technical solutions. Computers are predictable, but humans are not which makes them very difficult to manage in a security perspective. By

combining cybersecurity with social sciences, we can build more resilient defenses for the next time the world is caught off guard.

References

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University – Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003