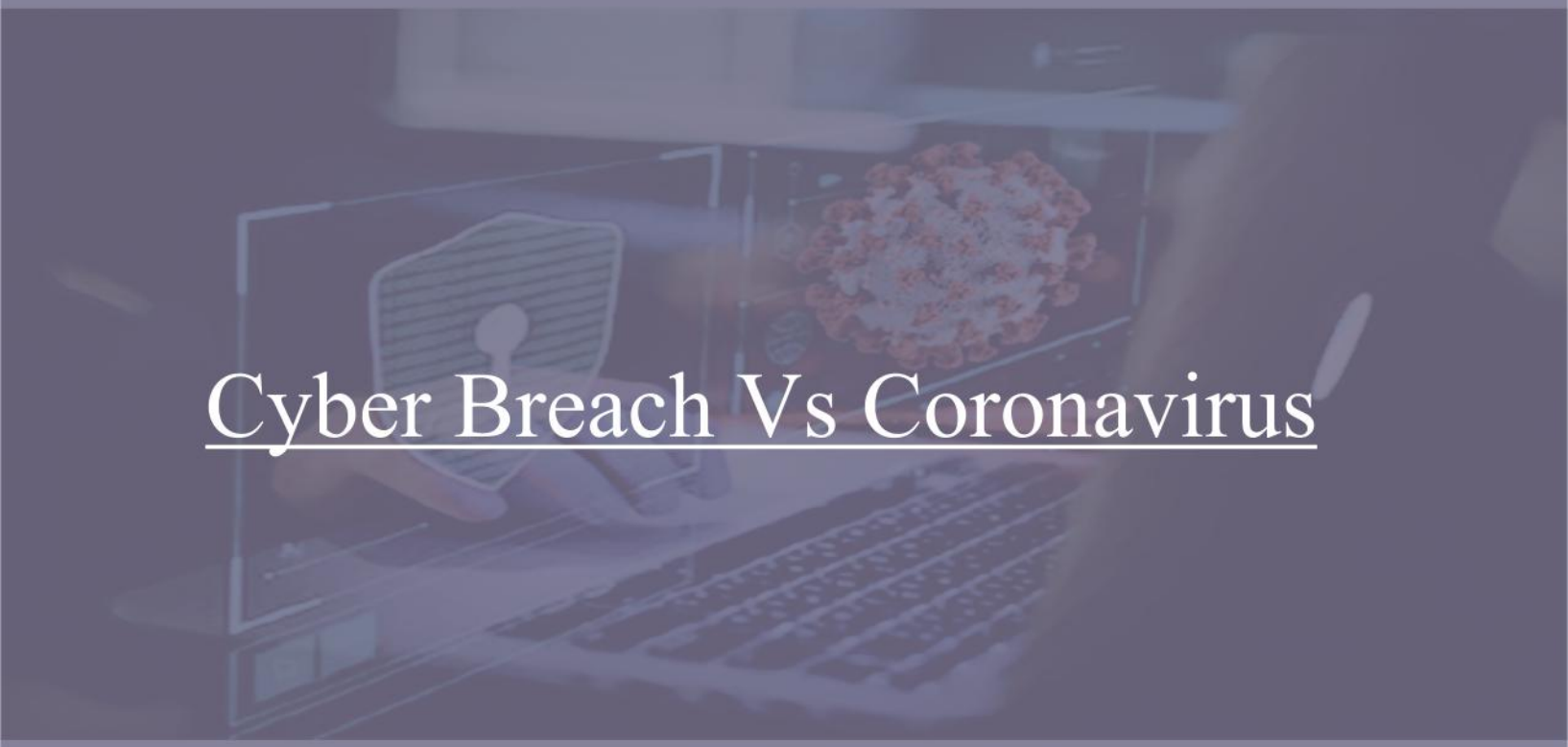
KAY LEGAL & ASSOCIATES LLP



# Cyber Breach Vs Coronavirus

# Cyber Breach Vs Coronavirus

Everyday escalation of the Pandemic Coronavirus (Covid - 19) is creating massive fear among the human orbit. People are concerned about their health and welfare. But this is not the only concern rising out of this Pandemic; some hidden elements are emerging fast on the backend which is creating a bridgehead to cyber breach.

**Coronavirus and Cyber Breach-** In addition to so many fake apps, fake domain, fake websites in the world of internet and their search of latest updates on Coronavirus, and the second most upcoming culture " Work from Home" via remotely.

## Rising the Fear of Coronavirus

Everybody is stuck at home due to Lockdown. Everyone is tracking the latest on the Coronavirus outbreak and the global response.

The cyber attackers are taking advantage through these fake apps, domains websites clamming live tracking of updates about the rise , and steps to fight the Novel Coronavirus.

These attackers range from credential phishing, malicious attachments and links, business email compromise, fake landing pages, spam and malware and ransomware strains.

Various app stores have already started making the shield for all these apps, and remove them instantly.

The attackers aim towards knitting a trap on the Internet infrastructure, a variety of phishing attacks and financial crimes.

## Remote User Credentials Breach/Theft

The impact of Coronavirus has led to "Lockdown "and Quarantine Policy which has compelled majority of Organizations to allow their team, their Workforce to "Work from Home" in order to maintain and sustain the business world.

Consequently, the shifting of significant portion of "workload remotely "renders an exploitable opportunity to the attackers.

Increase of remote login to the organizational resources, which never done before the attacker could easily conceal a malicious login without being detected by the target user. The attackers are hunting in full force for user credentials.

On the other hand, Employees that work from home often would do so from their personal computers which are significantly less secure than the organizational ones, making them more vulnerable for the attackers.

# Cyber Breach Vs Coronavirus

The attackers possess in different ways:

- Weaponized Emails
- Weaponized Documents
- Emails with link to malicious websites
- Email containing malicious executable

In current time, leading to a spurt of cyber breach due to the coronavirus outbreaks worldwide.

## #STAYSAFE

With the help of proper Vigilance and Diligence, you can keep yourself safe from these attackers.

- Verify the details of the apps before installing them via details of the developer, reviews and rating given by the others.
- Install apps from the verified apps stores, like Apple Store for IOS Users and Google Play store for Android Users.
- Do not open the emails from the unverified sender.
- Do not open the emails coming from WHO regarding any health and precautionary updates regarding coronavirus. It's better to check the update from their official website.
- Check HTTP and HTTPS status of the website. HTTP= Bad, HTTPS= Good. The HTTPS websites stands that the website is encrypted and protect you from the attack.
- Use Password Manager. (Try to use complexity password)
- Do not defer critical updates to software.
- Stress the IMPORTANCE of not to share password (Remote working leads to more password sharing)
- Do not leave the machine UNLOCKED.

## CONCLUSION

In the light of mass increase of "Work from Home", (Work Remotely), many Organizations are not yet equipped with proper shield from the attackers.

So, with Vigilance and Diligence we can protect our data & privacy.

**The coming decade will be a game-changing one for the cyber security industry, the world over.**

# KAY LEGAL & ASSOCIATES LLP

INFO@KAYLEGAL.IN

WWW.KAYLEGAL.COM