Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 6, July 2021: 6199- 6208

Research Article

Rapid Raise on Cyber Attacks due to Covid'19 over the Globe: A Survey

Vinoth Kumar C N S[a], Baranidharan B[b], Vasim Babu M[c], Ramasamy R[d]

[a,b] College of Engineering and Technology,
SRM Institute of Science and Technology, Chennai
[c] KKR & KSR Institute of Technology and Science, Guntur
[d] Veltech Rangarajan Dr. Sagunthala R&D Institute of Science of Technology, Chennai
[a] vinothks1@srmist.edu.in, [b] baranidb@srmist.edu.in, [c] vasimm.e@gmail.com,
[d]ramasamyr@veltech.edu.in}

Abstract

Cyber Attackers have rushed to misuse the current circumstance and are focusing on the service sector and the medical sector, for example, clinics, businesses like production and manufacturing, pharmaceutical and public ventures. Tragically, Covid-19 has prompted a sharp increment in digital assaults around the world. Additionally, assault keeps going to the PC systems and network frameworks of people, organizations and even worldwide associations when digital resistances may be brought due down to the move of a centre to the wellbeing emergency. There has been a quick increment since experts were approached to telecommute in the wake of the Covid-19 episode in the nation. The reason for this paper is to make mindfulness on the utilization of the pandemic as a digital assault instrument and to introduce remediation procedures to the individuals. Thus the brief research carried out using the social media, online websites and reports taken from the live updates at present. As per the investigation, half of the business pioneers don't think there is an expansion in assaults due to Covid-19. Additionally, this disposition is overflowing into security trainers for remote workers. As indicated by the report, albeit 56% said WFH expanded because of the infection, and 60% are utilizing their gadgets for work, about a portion of the respondents said they aren't offering security instruction that centres on remote work and there are no assurances that those individual gadgets have satisfactory security to meet corporate rules. Switching to remote working as a result of the COVID-19 can make digital security issues for both clients and service providers. At long last, because of the emergency, more work is led from home, and as a rule on close to home gadgets, organizations must remain careful, guaranteeing that their representatives are prepared on potential dangers and playing it safe to keep up the security of their systems, gadgets and information.

Keywords Cyber-attacks, Covid 19, WFH, emergency, gadgets, and service providers

1. Introduction

There has been an expansion of domains enlisted with the watchwords 'COVID' or 'Corona', to exploit the developing number of individuals looking for data about COVID-19. Huge numbers of these are viewed as evolved with the malignant goal – In the March-end, 2,022 vindictive and 40,261 high-hazards recently enrolled domains were found [1]. In mid-April, Google announced that in the only multi-week, it saw over 18 million everyday malware and phishing messages identified with Covid-19 tricks were sent employing Gmail al-one and that is notwithstanding the 240 million day by day Covid-19 related spam messages recorded. While we as a whole attempt to become acclimated to the Covid-19 pandemic's forced principle is making the individual changed in our work and home lives, this year has been a period of an uncommon open door for digital attacks and threats. The worldwide reaction to the pandemic, and our longing for the most recent data about it, has supercharged crooks and programmers using the same old thing models of phishing messages and phoney sites.

Verizon's 2019 Data Breach Investigations Report indicated that 32% of corporate information penetrates began with a phishing email. Likewise, phishing was available in 78% of digital secret activities occurrences [2]. So it's nothing unexpected that attackers will continue attempting to fool clients into surrendering delicate data by exploiting the enthusiasm around the pandemic, and taking off notable associations and organizations, for example, the World Health Organization (WHO), Zoom, Microsoft or Google.

Cybercriminals are making counterfeit sites identified with COVID-19 to lure casualties into opening pernicious connections or clicking phishing links, bringing about character pantomime or illicit access to individual records. Likewise, Trend Micro detailed that about one million spam messages have connected to COVID-19 since January 2020. Business Email Compromise (BEC) has become the plan of decision, including the service spoofing and customer email addresses – or utilization of indistinguishable email addresses – to direct the assaults. The tremendous requirement for key supplies gives a perfect situation to cyber attackers to gather subtleties or to occupy a huge number of dollars to get hold of assets into criminal records. Likewise web security organization that we have been seeing an expanded measure of site abuse endeavours [3]. Negatively, numerous dangers on-screen characters have begun to mishandle the frenzy and inconvenience of the COVID-19 pandemic to lead extraordinary made malware and phishing assaults around the world.

2. Literature Review

Cyber attackers influence enthusiasm during public health threats and other prominent occasions to carry out fraudulent activities and disperse malware. This pattern will proceed with the development of new and reused tricks including financial fraud and malware identified with the corona outburst [4]. Pernicious attackers are probably presenting links on counterfeit causes and fraud sites that request gifts or charity donations for relief aid or convey malware. Almost certainly, more tricks and malware will follow through the span of the reaction time frame. Web clients should practice alert before opening related messages, link joins, visiting sites, or putting forth charity donor to corona infection alleviation attempts.

Remote work has been the standard for many officials and a huge number of organizations before COVID-19 showed up, and considerably more have been utilizing BYOD and shadow IT for quite a long time. In any case, presently work from home (WFH) has been officially insisted in major associations that may have not expected over time, though it conceivable or had no enthusiasm for permitting remote work. Also, these organizations are presently confronting another reality and new security challenges, which, as per a Crowd Strike, that includes: i) Use of individual gadgets and email for business or dealing with insightful data. ii) Provisioning corporate resources to help remote working provisions. iii) Proper organizing and setup of remote administrations, corporate VPNs and related two-factor verification strategies [5]. All things considered: Many organizations that have had longstanding remote work and BYOD strategies have attempted to implement security approaches encompassing these issues. It is sensible to believe that associations that had WFH dropped on them unexpectedly and expected to modify on the fly would be uncertain of how well their cyber-security endeavours would be.

U.S. Lawyer Andrew Murray and the FBI gave a caution, asking the general population to stay cautious against COVID-19 tricks. Phishing messages or messages from elements acting like the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC). Malware embedded in versatile applications intended to follow the spread of COVID-19 that can take data put away on gadgets. Malevolent COVID-19 sites and applications that can pick up and lock access to gadgets until a payment (ransom) installment are made [6].

Many existing composed cyber-criminal bunches have changed their strategies to utilize corona virus-related materials on medical care updates, counterfeit fixes, financial bundles, emergency crisis advantages and flexibly deficiencies. Since mid-February, KPMG part firms have seen the quick form out of framework by cyber attackers used to dispatch coronavirus themed skewer phishing assaults and to draw individuals to counterfeit sites trying to gather Office 365 user details. Numerous phishing messages tricking clients to counterfeit duplicates of the Center for Disease Control (CDC) site which request client’s details and passwords. Phishing messages are indicating to originate from the World Health Organization, government specialists, and real organizations coordinating prudent steps, again implanting malware to the individuals [7].

The Cyber Threat Index is a month to month estimation and investigation of the worldwide attack scenario across the records and applications and depends on information accumulated from Imperva sensors everywhere throughout the world—including more than 25 Petabytes of system traffic going through the Imperva CDN every month. With more than one trillion all out solicitations dissected and 21 billion application cyber spoofing blocked, it offers an unmatched and wide-ranging appearance at application security and gives a straightforward score to reliably follow cyber-attack levels and detect inclines after some time [8].

3. COVID 19 CYBER ATTACKS AND ITS TOOLS

COVID-19 pandemic is transforming us. Individuals are concerned, and with that worry comes a craving for data, wellbeing and backing. Sorted out wrongdoing bunches are abusing the dread, vulnerability, and uncertainty which COVID-19 brings to target people and organizations in an assortment of ways. The new pattern of digital assaults through malware and ransomware with regards to COVID-19 is 'Fear ware'. The digital aggressors are misusing the dread of coronavirus to make the casualty fall prey to digital attacks [9]. The programmers are discharging new processing infections and versatile applications identifying with COVID-19 updates and other data. They are additionally structuring phishing sites, messages and phishing UPI accounts in name of COVID-19, which are prompting Cyber cheats. Cybercriminals are exploiting the coronavirus emergency to spread malware, upset tasks, sow uncertainty, and make a brisk buck [10].

Cybercriminals are progressively utilizing the Covid-19 pandemic period to target individuals with malware which can bargain pivotal individual information just as those of associations. A favourable looking email, encouraging the most recent update on Covid-19 insights or projections during the week ahead will effortlessly pull in the consideration of web clients. Indeed, even the sender's letters ID will show up very certified. In any case, it could be malware for phishing information from the PC or giving remote access to cybercriminals or ransom-ware which requests cash for re-establishing access. Normal cybercrime procedures, for example, phishing, have seen a spike. Phishing is the deceitful act of inciting people to uncover individual data, for example, passwords and Visa numbers through phoney sites or messages. New information assembled by Google and broke down by Atlas VPN, a virtual private system (VPN) specialist co-op, is revealing more insight into the extent of this. As indicated by the report, in January, Google enlisted 149k dynamic phishing sites. In February, that number almost multiplied to 293k. In March, however, that number had expanded to 522k - a 350% expansion since January [11]. The COVID 19 related threats in Quarter 2020 are shown in Figure 1

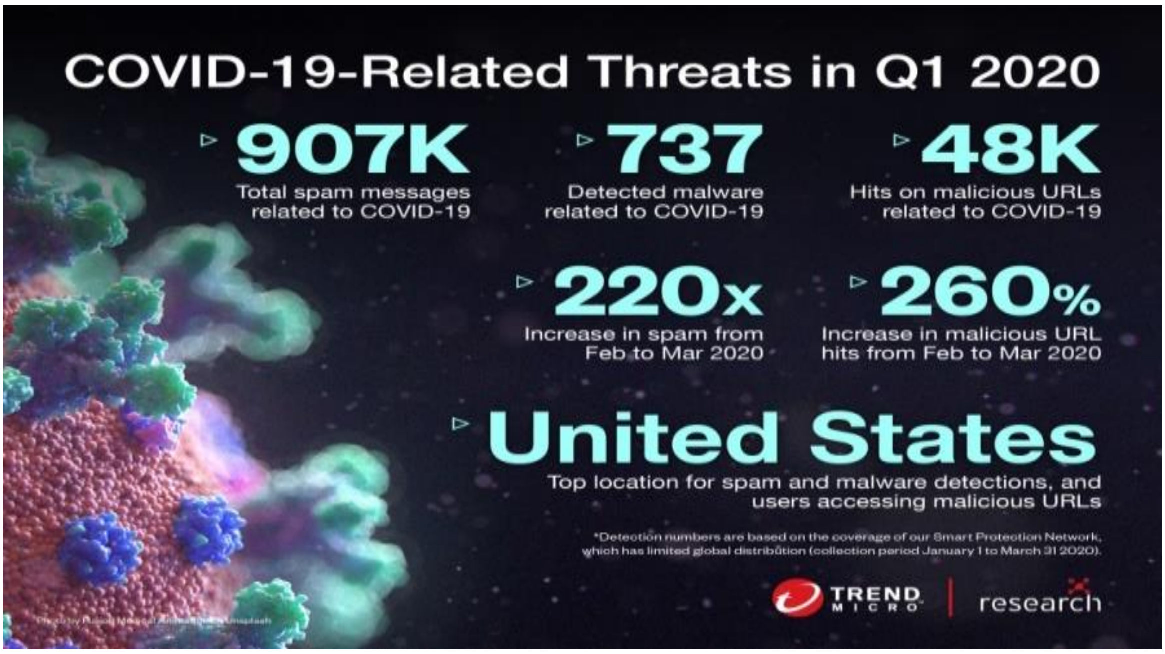


Figure 1 - Covid 19 related threats in Quarter 2020 [12]

Coming up next are a portion of the episodes announced in India and different nations. A few models / Case Studies allude to patterns of Cyber Security Risks as a major aspect of COVID-19 interruption.

3.1 Malware Attacks

The awful spread of COVID-19 is turning into an open door for cybercriminals to spread malware or dispatch digital assaults. One such sort of malware assault is with use 'Corona-virus Maps' – It's a malware tainting PCs to take passwords. One of the absolute first cyber-attacks identified with COVID-19 was in regards to the phony COVID-19 maps.

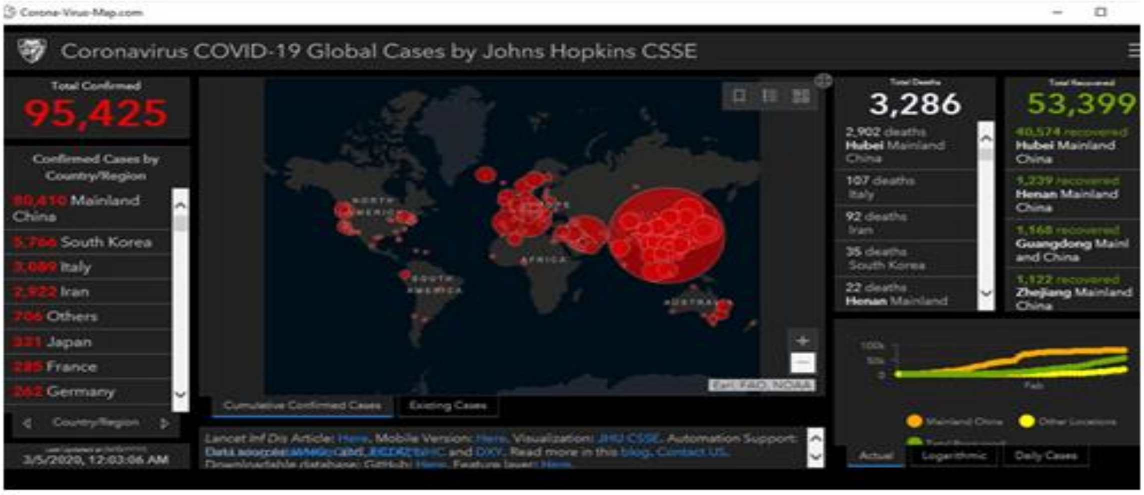

Corona-Virus-Map.com
Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE
Total Confirmed
95,425
Confirmed Cases by Country/Region
80,410 Mainland China
5,766 South Korea
3,089 Italy
2,922 Iran
706 Others
331 Japan
285 France
262 Germany
Country/Region
3/5/2020, 12:03:06 AM
NORTH AMERICA
EUROPE
AFRICA
SOUTH AMERICA
AUSTRALIA
Esri, FAO, NOAA
Cumulative Confirmed Cases
Existing Cases
Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support:
Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.
Total Deaths
3,286
2,902 deaths Hubei Mainland China
107 deaths Italy
92 deaths Iran
35 deaths South Korea
22 deaths Henan Mainland
Total Recovered
53,399
40,574 recovered Hubei Mainland China
1,239 recovered Henan Mainland China
1,168 recovered Guangdong Mainland China
1,122 recovered Zhejiang Mainland China
100k
50k
0
Feb
Mainland China
Other Locations
Total Recovered
Actual
Logarithmic
Daily Cases

Figure 2 - Covid 19 global cases

The Johns Hopkins University gave one of the absolute first maps which included measurements to the world. This has been an incredible asset to society and has demonstrated to be hugely useful. Nonetheless, since it was so famous, digital assailants made their own 'phony' renditions of the site that necessary you to download a module, and Figure 2 demonstrating exactly how persuading the phony pages can show up. Cybercriminals are exploiting the across the board worldwide correspondences on the corona-virus to cover their exercises. Malware, spyware, and Trojans have been discovered inserted in intelligent corona-virus maps and sites. Figure 3 shows the phishing sites detected by Google in the month of January-march, 2020.

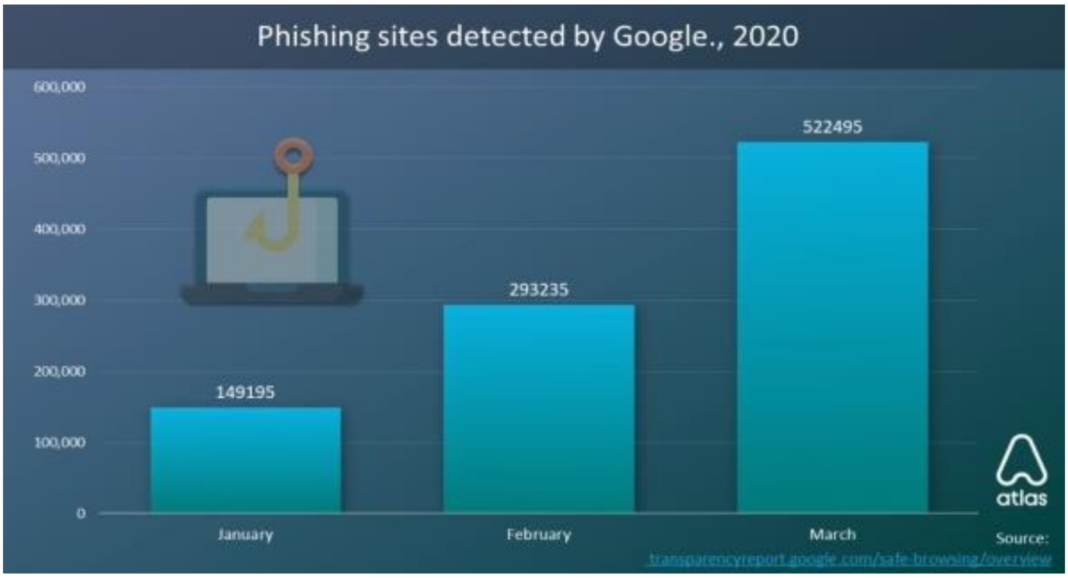


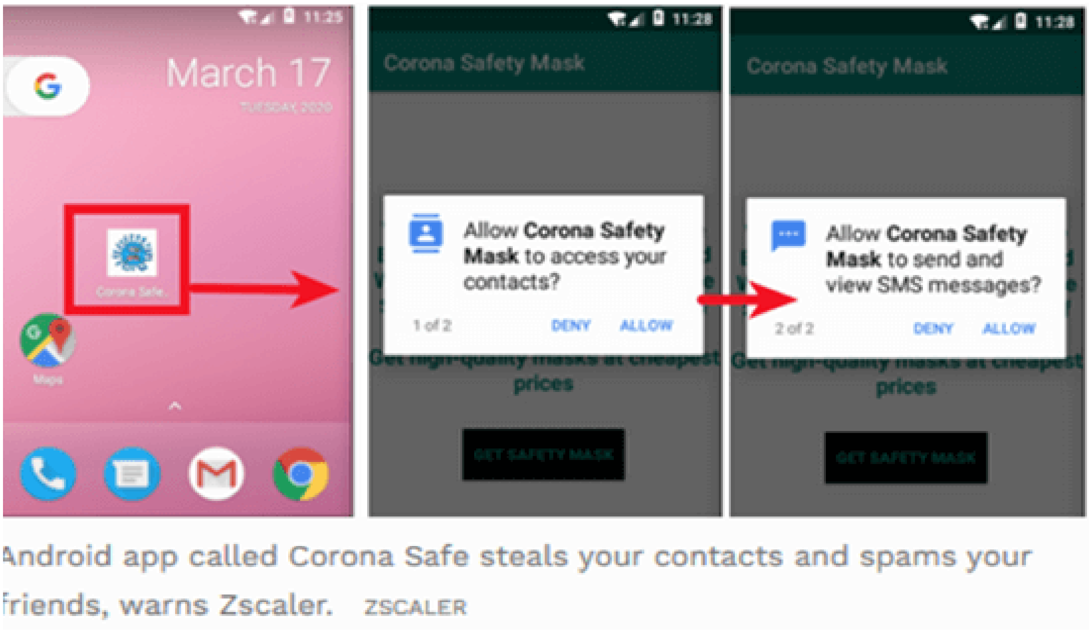
Figure 3 - Covid 19 related threats in Quarter 2020

3.2 Email based attacks

Utilizing World Health Organization mail for the sake of COVID-19 as a genuine application by the fraudsters and spreading malware to control your end gadgets [13]. The email appears as though it's from the WHO, sent by a Tim Hardley, head social insurance official from WHO's the provincial office for the Americas. A Google scan hurls no outcomes for such a WHO official. The connection has noxious and conveyed a modern, multi-layer payload dependent on the Lokibottrojemailan (Trojan: Win32/Lokibot.GJ!MTB).

3.3 Fake Mobile Applications

Cybercriminals have begun making a colossal number of phony versatile applications for the sake of COVID - 19 as genuine applications from an association, for example, WHO for spreading phishing sends/destinations and phony news and taking important data. Malware being conveyed by employing Android applications that take casualties offering Corona-virus wellbeing cover upon establishment [14]. Figure 4 shows the fake mobile app called Corona safe steals your contact from your mobile device.



Allow **Corona Safety Mask** to access your contacts?

1 of 2 DENY ALLOW

Allow **Corona Safety Mask** to send and view SMS messages?

2 of 2 DENY ALLOW

Get high-quality masks at cheapest prices

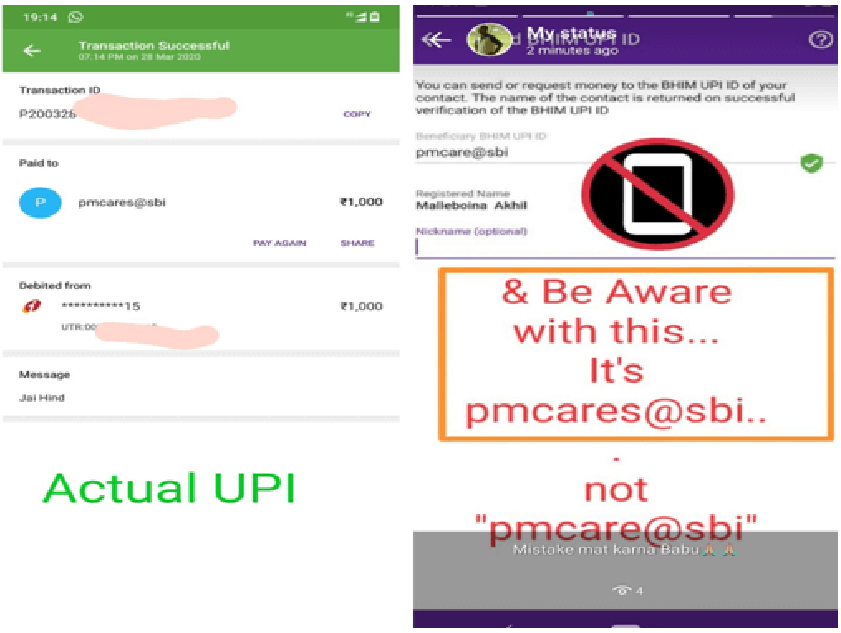
GET SAFETY MASK

Android app called Corona Safe steals your contacts and spams your friends, warns Zscaler. ZSCALER

Figure 4 - Fake mobile app called Corona safe steals the contact detail from mobile

3.4 UPI Frauds

UPI or Unified Payment Interface is a technique to make installments carefully and has just picked up prevalence. As the strategies for causing installments to have gotten innovatively propelled, fraudsters have additionally advanced various approaches to trick you out of your well-deserved cash [15]. It is so miserable to see that even amidst such a genuine compassionate emergency like COVID-19, these cybercriminals can just consider advantage and robbery. Cybercriminals are additionally exploiting rising corona-virus worry for gathering good cause. The Prime Minister's Citizen Assistance and Relief in Emergency Situations Fund' (PM CARES Fund)' set up were not saved and inside a couple of hours of its declaration, "about six" comparative sounding sites were made, for example, "PM-care" and so forth which is shown in Figure 5



Transaction Successful
07:14 PM on 28 Mar 2020

Transaction ID
P200328 [redacted] COPY

Paid to
P pmcares@sbi ₹1,000
PAY AGAIN SHARE

Debited from
***********15 ₹1,000
UTR:00 [redacted]

Message
Jai Hind

Actual UPI

My status
2 minutes ago
BHIM UPI ID

You can send or request money to the BHIM UPI ID of your contact. The name of the contact is returned on successful verification of the BHIM UPI ID

Beneficiary BHIM UPI ID
pmcare@sbi

Registered Name
Malleboina Akhil

Nickname (optional)

& Be Aware with this... It's pmcares@sbi.. not "pmcare@sbi"

Mistake mat karna Babu 🙏🙏

Figure 5 - Fake mobile app called Corona safe steals the contact detail from mobile

3.5 Disruptive malware (Ransom-ware and DDoS)

Cybercriminals are sending problematic malware like Ransom-ware against basic foundation and reaction organizations, for example, emergency clinics and clinical focuses, which are overpowered with the wellbeing emergency. Such Ransomware or DDoS assaults don't regularly intend to take data yet keep it from getting to basic information or disturb the framework, fueling an effectively desperate circumstance in the physical world [16].

During this period of vulnerability and expanded online movement, cybercriminals are effectively attempting to abuse the ebb and flow COVID-19 story with assaults planned for exploiting the circumstance. It is significant now like never before to know about online tricks and dangers as they are expanding in volume and complexity. Figure 6 shows the cyber safety checklist to avoid the cyber-attack.

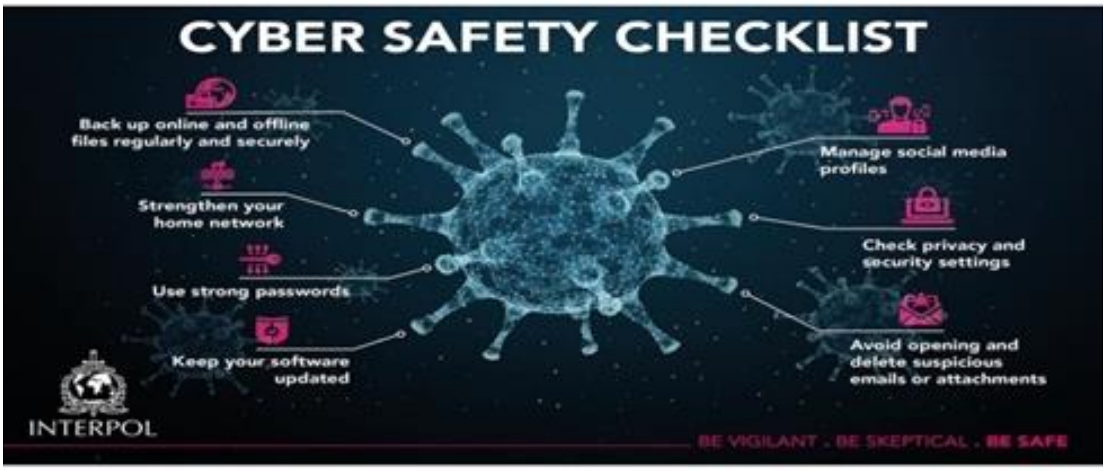

CYBER SAFETY CHECKLIST
Back up online and offline files regularly and securely
Strengthen your home network
Use strong passwords
Keep your software updated
Manage social media profiles
Check privacy and security settings
Avoid opening and delete suspicious emails or attachments
INTERPOL
BE VIGILANT . BE SKEPTICAL . BE SAFE

Figure 6 - cyber safety check-list [17]

4. Defensive Measures To Be Taken Out For Covid'19 Cyber Threats

In this Covid-19 pandemic situation, still there are no specialized remedy measures for countering cyber-attacks. But there are some well tested general measures to be applied to overcome these kinds of challenges. These general measures include both behavioral change from employee end and technical change from the organizational end [18].

4.1 Employee or Individual user measures

At first, threat aware employees should be educated well about the new situation and the measures to be taken by them.

i. All the organization employees need to be suspicious about the emails they are receiving from the unknown end or some from some unusual sources. Sometimes, the phishing emails may be coming from the superiors with whom these kinds of mails would be unusual.

ii. Abstain from clicking the link sent by an unknown source and forwarding it to their known circle. A single click may be the most vulnerable point in passing the critical data to hackers.

iii. Advise the employees to install corporate-sponsored Anti-Phishing and Anti-virus software in their devices since most of the company related transactions are happening from their own devices.

iv. Timely updates are mandatory in all the applications they are using in their day-to-day life. Either it may their corporate device or personal device; make updates as a mandatory step.

v. Update all your web accounts with a much more complex password and make it very hard to break it. Also, use a multi-level authentication mechanism.

vi. Use Virtual Private Network (VPN), since it enables trusted communication between employees and the organization. Also, VPNs offer the same level of protection and firewall services as like in their office premises.

4.2 Organizational measures

An organization is also having equal responsibility or more than that of an individual user in mitigating cyber-attacks. From the organization side, the following measures should be taken,

i. All the organizational heads along with their security team have to devise-clear strategies and implement their security measures according to their organization and business needs.

ii. Circulate what-to-do list to their employees in case of any security violations. The security team should be reaching the employee as soon as possible like in an emergency.

iii. Multi-factor authentication should be mandatorily implemented to increase security measures.

iv. Organizations should develop the ability to filter out malicious links and to do DNS sinkholes to mitigate the phishing attack.

v. The organizations should work more closely with their Internet Service providers (ISP) to enable more security services apart from the basic primitive measures [19]. ISPs are the right point to mitigate Distributed Denial of Service (DDoS) attacks and mobile device vulnerabilities.

vi. Companies should insist on their employees using only company devices since they will be having a range of software for data protection. It is observed that a lot of data leaks occurred when the employees used their devices over company devices.

It is observed that healthcare and finance tech industries are worst affected due to this Covid-19 pandemic. The organizations and ISPs are the best places to implement the rigorous security measures to counter the cyber-attack than an individual user [20]. An individual user also should be properly educated about the phishing attacks since it is the most vulnerable point.

Table 4.1 shows a hand-curated rundown of the digital assaults and its measures identified with the worldwide pandemic.

Threat description	**Type**	**Description**	**Remedies**
Businesses Underestimate COVID-19 Cybersecurity Risks	Misc	As per the examination, half of the business chiefs don't think there is an expansion in assaults due to COVID-19. Likewise, this demeanour is overflowing into security preparing for remote representatives. As indicated by the report, albeit 56% said WFH expanded because of the infection, and 60% are utilizing their gadgets for work, about the portion of the respondents said they aren't offering security training that centres around remote work and there is no assurance that those individual gadgets have sufficient security to meet corporate rules [21].	Be wary about opening any connections or downloading records you get paying little heed to that sent them.
InfoStealers Weaponizing COVID-19	Malware	As per the examination, half of the business chiefs don't think there is an expansion in assaults due to Infostealers is intended to gather a wide scope of data, for example, usernames, passwords, and bank subtleties employing the utilization of run of the mill keyloggers. Some of them advanced into increasingly modern variants fit for taking WiFi passwords (like Agent Tesla), framework and system data (Trickbot), or the substance of cryptographic money wallets (for instance, Trickbot and	Always enter your username and the secret phrase just over a protected association. Search for the "https" prefix before the site URL, demonstrating the association with the site is secure. Never share your UPI MPIN with anybody.

		Hawkeye). In the same way as other assaults, these info stealers were commonly conveyed employing spam email battles (or mal-spam). To expand the disease rate, the on-screen characters behind the assaults typically use messages with topics dependent on ebb and flow news or occasions. COVID-19 is on truly everybody's psyche nowadays, so the odds of persuading a casualty to open a message might be generously expanded, or if nothing else that is the aggressor's expectation [22].	
DocuSign users targeted with COVID-19 themed phishing	Phishing	The assailant sent an email mimicking a mechanized email from Docusign, replicating the substance utilized by genuine messages from this organization. The email guarantees that there is a record sent to the client for a survey from CU #COVID19 Electronic Documents, with no further subtleties of what the report is [23].	Habituate by looking for the sender's email ID before you enter/part with any close to home data. Avoid tapping on obscure connections or sending any dubious SMS
Nigerian cyber criminals operate COVID-19 BEC schemes	BEC	Nigerian cybercriminal entertainers are indecently abusing the COVID-19 pandemic to taint government social insurance offices, scholastic clinical projects, clinical distributing firms and more with malware, generally to lead Business Email Compromise activities [24].	Use antivirus, antispyware, and firewall programming (update them consistently as well).
The exposure to compromised e-commerce websites is greater than ever. 26% increase in web skimming	Malware	As indicated by the most recent Malwarebytes measurements, web skimming expanded by 26 per cent in March over the earlier month. The subsequent perception is how the quantity of web skimming squares expanded respectably from January to February (2.5%) however then began to go up from February to March (26%). While this is as yet a moderate increment, Malwarebytes trusts it denotes a pattern that will be increasingly obvious in the coming months [25].	Always update your internet browser and empower a phishing channel. If dubious email arrived in mailbox, do call an organization to affirm if it is real or not.

5. Conclusion

Organizations, Business endeavours and people should execute procedures to shield themselves from digital assaults during the progressing pandemic. The motive is that cybercriminals have used COVID-19 to dispatch phishing, defrauding, spamming, and malware assaults on organizations and peoples. The best procedure for shielding working employees and employers from this unfriendly occasion is exploiting the proper remedy design plan and policy framework that fit into the security checking and remediation systems. The remediation systems incorporate validation, encryption, the utilization of VPN, and the training of individual clients.

References

[1] Interpol, “Global Landscape on Covid-19 Cyber threat”, INTERPOL General Secretariat, April 2020. (Online) Available: https://www.interpol.int/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

[2] Check Point Software technology, "Corona virus cyber-attacks update: beware of the phish", future of cyber security, May 2020. (Online) Available: https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

[3] WebARX, "COVID-19 Cyber Attacks," WebARX Security, 30 March 2020. [Online]. Available: https://www.webarxsecurity.com/COVID-19-cyber-attacks/

[4] T. F. Duffy, "Cyber Threat Actors Expected to Leverage Coronavirus Outbreak," Center for Internet Security, vol. 15, no. 2, 2020.

[5] A. Murray, "U.S. Attorney Andrew Murray Issues Warning For COVID-19 Scams," U.S. Department of Justice, Charlotte, NC, 2020.

[6] G. Archibald, K. Robins and I. Gray, "COVID-19: Protect your team from phishing and cyber scams," KPMG, 26 March 2020. [Online]. Available: https://home.kpmg/au/en/home/insights/2020/03/coronavirus-COVID-1 9-phishing-cyber-scams-protection.html

[7] Imperva, "Imperva Research Labs Shows Significant Changes in Web Traffic During COVID-19 Pandemic," Imperva Inc. Research Lab, 26 March 2020. [Online]. Available: https://www.imperva.com/company/press_releases/imperva-research-la bs-shows-significant-changes-in-web-traffic-during-covid-19-pandemic /

[8] World Economic Forum. Hackers are using coronavirus maps to spread malware. Accessed: 20 March 2020. Available: URL: https://www.weforum.org/agenda/2020/03/hackers-are-using-coronavirus-maps-to-spread-malware/

[9] M Christie. Online scammers target vulnerable Internet users during coronavirus outbreak. Accessed: 20 March 2020. Available: URL: https://abcnews.go.com/US/online-scammers-target-vulnerable-internet-users-coronavirusoutbreak/story?id=69675134

[10] Coronavirus disease (COVID-19) pandemic Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019?gclid=Cj0KCQjwirz3BRD_ARIsAImf7LNELh942XopyuuC_3j_KXqYZBC05UXZk9Xbmskufk oghOjJ-fdGgvQaAp4dEALw_wcB

[11] Google Registers a 350% Increase in Phishing Websites Amid Quarantine, Available: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine

[12] Trend micro research,Available:https://twitter.com/trendmicrorsrch/status/1249651921855508481

[13] World Health Orginization. WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. Accessed: 20 March 2020. Available: URL: https://www.who.int/dg/speeches/detail/who-director-generals-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[14] Fake COVID 19 app, Available: https://economictimes.indiatimes.com/topic/fake-covid-19-apps

[15] 4 Ways To Prevent UPI Fraud Amid The COVID-19 Crisis, Available: https://blog.bankbazaar.com/4-ways-to-prevent-upi-fraud-amid-the-covid-19-crisis/

[16] Ransomware and DDoS attacks: Cybercrooks are stepping up their activities in the midst of coronavirus, Available: https://www.zdnet.com/article/ransomware-and-ddos-attacks-cybercrooks-are-stepping-up-their-activities-in-the-midst-of-coronavirus/

[17] The Cyber Security Hub.com, Available: https://www.facebook.com/TheCyberSecHub/posts/cyber-safety-checklist-interpol-cybersecurity-infosec-riskmanagement-encryption-/1121676081517056/

[18] World Economic Forum, "How to protect yourself from cyber attacks when working from home during COVID-19"https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[19] Brad Casey, "How ISP services can improve enterprise cybersecurity"https://searchsecurity.techtarget.com/answer/How-ISP-services-can-improve-enterprise-cybersecurity

[20] Alex R.Mathew, "Cybersecurity Pros Warn – Covid – 19 Pandemic as a Tool", International Journal of Engineering and Advanced Technology, Vol.9 (4), April 2020, pp. 2441 – 2443.

[21] Sue Poremba, “Businesses Underestimate COVID-19 Cybersecurity Risks”, Security Bouulevard, May 2020. Available Online: https://securityboulevard.com/2020/05/businesses-underestimate-covid-19-cybersecurity-risks/

[22] Subrat Sarkar, Jason Zhang And Stefano Ortolani, “InfoStealers Weaponizing COVID-19”, May 2020. Available Online: https://llstager.wpengine.com/labsblog/infostealers-weaponizing-covid-19/

[23] “Abnormal Attack Stories: DocuSign Phishing”, May 2020. Available Online: https://abnormalsecurity.com/blog/abnormal-attack-stories-docusign-phishing/

[24] Peter Renals, “SilverTerrier: New COVID-19 Themed Business Email Compromise Schemes”, Paloalto Networks, May 2020. Available Online: https://unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise/

[25] Jérôme Segura, “Online credit card skimming increased by 26 percent in March”, Malware bytes labs, May 2020. Available Online: https://blog.malwarebytes.com/cybercrime/2020/04/online-credit-card-skimming-increases-by-26-in-march/