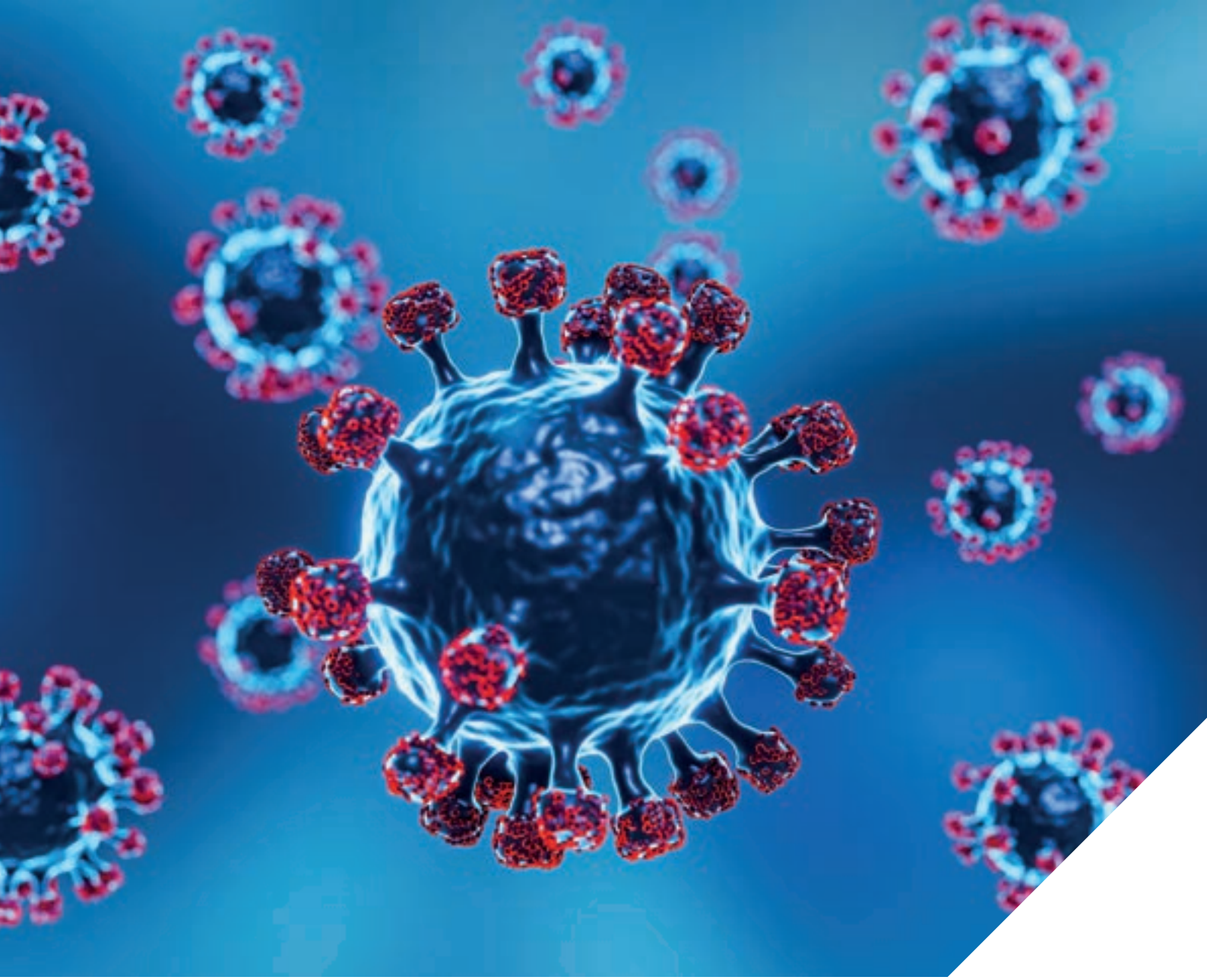


Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

# Impact of COVID19 on Cybersecurity:

## Learnings and Best Practices

## COVID-19 and the rise of Cybercrimes:

The International Data Corporation, which is the premier global provider of market intelligence, reports that IT environments are becoming more complex, and cybercriminals are getting better at identifying and targeting weaknesses. Nearly 40% of IT security specialists have reported that cyber security incidents in 2020 had become more sophisticated, and the increased complexity of managing and supporting security products is more challenging than ever before.

The major spikes in fraudulent activity during lockdowns were largely driven by automation. Most cybersecurity incidents attacks that gained traction during COVID19 were Phishing, Malware, Identity cloning, Identity theft and man in the middle. One of the incidental examples of rise in cyberattacks has been visible in the use of video conferencing. One of the popular video conferencing platforms is Zoom. The Zoom App was another recent cyber security incident which was attacked this year, and people with bad intentions gained access to private meetings, conversations, and managed to share shocking and inappropriate videos.

COVID-19 presented the cyber attackers an opportunity as bait by impersonating popular brands thereby misleading online users and thus infecting computers and stealing critical information. In addition, many legitimate applications that are providing authentic COVID-19 related information for caution, safeguards and travel restrictions are also being targeted by cyber criminals as online users are being tricked into downloading ransomware disguised as legitimate COVID-19 applications.

COVID-19 lockdown came as a shock to a lot many small and medium sized business who had to rush into transforming digitally at a mind-boggling pace and in this effort paid little or no attention to security and privacy controls and thus suffered due to targeted phishing attacks and retrieval of personally identifiable information (PII). COVID-19 brought the reality for re- examination and higher prioritization for cyber security technology environment and keeping a check on establishing more control for the critical information.

## Making Cybersecurity measures a Habit:

The rise of Cybercrimes during the COVID-19 are profoundly the same as before, but are themed around COVID-19 and thus catch our attentive and inquisitiveness when an email relating to curing or preventing COVID-19 reaches one's inbox, we become tempted to open it. The COVID-19 emergency has reinforced the requirement for imbibing good cyber security practices and understanding the reason behind them and how to make good cyber practices an everyday habit.

In addition, with the General Data Protection Regulation (GDPR), and other legal frameworks, it has become paramount and responsibility of employees to read in detail the privacy policies of every website that are visited and ability to look for technical jargons and importance of identifying a privacy policy that could be considered a potential red flag.

Remote working requires more training and better security measures in place for an employee from the beginning as face-to-face compliance and security trainings had to be switched to online mode. Thus, many companies installed standardised anti-virus and anti- malware software's that helped and enhanced the security of at home systems from the backend. As the custom of employees to work from home continues, it is should become customary that robust collaboration tools and virtual infrastructure is put in place by companies that are secure new channels of data and are adopted to the new model of remote working. Lastly with cost pressures mounting with every layer and new security technology function costing money, the responsibility of the employees at inculcating security measures have become ever more critical and the need for regular cyber awareness sessions have become important that are simple and agile at practice

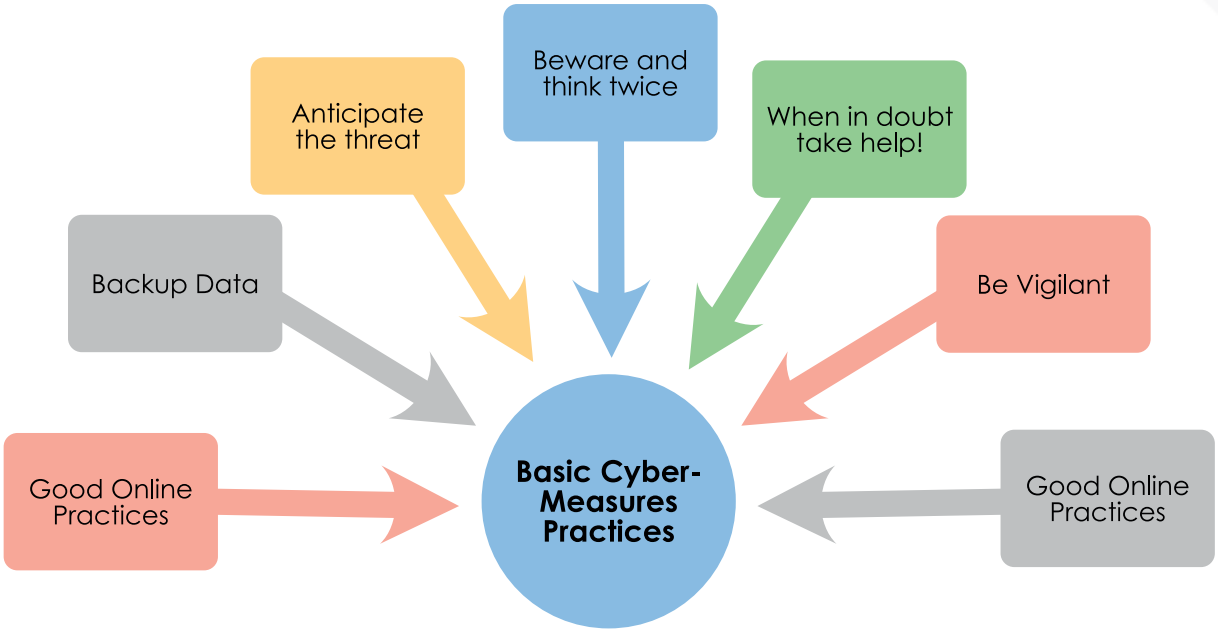
level.

## Seven Best Cybersecurity practices that can help prevent loss of important data:

The general measures at an individual level are important and one's responsibility at minimising and avoiding cyber threats and reporting any suspicious cyber activity and one can prevent her / his data from cyber criminals by undertaking some of the underlying fundamental best security practices.

1. **Good online practices:** Strong cyber ethics: In order to understand the fundamentals of cyber security practices one can start small and invest in measures such as adopting strong passwords. Making oneself aware of the term 'pwned' is to become aware, if one's password and email has been breached.

*Figure 1: Cybersecurity measures at an individual level*




2. **Back-up your data:** Regular back-up of data should be made a general practice across the organisation and individuals must know how to rank the data in terms of importance and which reliable hardware or cloud network the company authorises to store back-up copies of the data. Regular back – up of data must take place on a timeline basis. Automatic backups must be enabled and it would be good to have clear cut policies for updates.
3. **Anticipating the threats:** Some of the most common formats of cybercrimes are fake phone calls, multiple forms of phishing, Bluetooth vulnerabilities and email generated threats. Phishing has evolved as one of the best, most effective and effective cybercrime practices. Phishing targets an individual's hobbies, interests, friend circle and lucrative wealth schemes. Phishing in form of text messages has also become a common practice. The most effective against phishing is taking a deeper look at every message or email that seems suspicious and look for key words, spelling mistakes, the type of email from which the message has been generated, and asking questions such as why is one contacting you with regards to huge amount of wealth or popular company rewards. Email signatures and suspecting phone number is a good step first identification.

4. **Beware and think twice:** The best guard against cyberattacks is being aware, utilising the common sense and think before taking action. One must not succumb to impulse and get lured to making quick buck. An email and a message is the simple and most alluring way at getting access to the personal identifiable information (PII). Cybercriminals are good at registering fake domains and add characters before or after for example @happy@un-safety.net. This has become much critical as with the start of the COVID-19, many fake websites and portals started to emerge promising information regarding COVID-19. Whenever in doubt using website security check services is a good practice to scan for URL and email addresses. For example, all new files must be isolated and scanned and making sure files are safe to open and do not have any known malware signatures.
5. **When in doubt take help:** There are many resources that are available online to learn about hackers, understand details regarding various types of phishing formats, how to identify suspicious links and general cyber sanitary practices, that are helpful in minimising online risks from cyber criminals. In addition, taking fundamental courses in cybersecurity and compliance such as turning off automatic downloading of attachments and installing the latest software whenever possible are good practices. Knowing where to find help is also important and its simple, whenever in doubt, dig deeper, spend more time, and assure yourself that action is legitimate.
6. **Be vigilant:** Being vigilant is to learn from others mistakes, maintaining communication with one's employer, staying up to date about misinformation and informing others and relevant authorities about suspicious online content. In today's age of bombardment of misinformation, knowing what is authentic and what is fake is most important. In addition, it is always advisable to have a scanning software and scan any new file or information received. Use of public wi-fi networks is not advisable and avoid as much as possible. Stress on using applications, networks and any online content that has been reviewed and verified and not to open apps that seem attractive. Lastly, one has the choice to say 'NO' and wait until more information is available to certify the email or the message. There is no need to rush into opening- up everything that one receives.
7. Implement Two-Factor Authentication: Two-factor authentication mechanism helps in minimizing access to critical information as two different information types are required for granting access to an account. One of the fundamental examples is the generation of 'One Time Digital Code' delivered to the phone, in addition to the password entered for any banking transactions. This added layer of security makes it harder for account access to be compromised. Use of two – factor authentication for as many applications as possible must be encouraged and enabled. In addition, there are three factor and four-factor authentication also available as part of some critical applications.

## Cybersecurity Tools and Updates as essentials:

1. Basic Cybersecurity Tools: In addition to the above basic cybersecurity practices, the need for a basic security apparatus is necessary for protecting any form of digital information and systems. The security system is required to have a suite of defences like anti-virus, anti-spyware, and a strong firewall. Each of these cyber security defences are a necessary part of protecting the information and a lot of good anti-virus and anti-spyware tools are available for free and thus can act as first line of defence. Depending upon the criticality of the information, the cybersecurity measures vary in price, complexity, and usage.

2. Firmware and software's Update: Firmware is another important software that helps evade cybercrimes. Firmware is embedded on the hardware to help it run. It is recommended to keep the firmware up to date on routers, as hackers can assess network security flaws to exploit the remote user. Automatic updates to firmware are highly recommended. All devices that are linked to each other must undergo software and patch updates as interlinking of information happens over the cloud and any loophole in software patches that happens between devices say an application running on a mobile and a laptop, provides a window of opportunity for attackers to use the vulnerability. One must update all optional software updates as well.

*Figure 2: Cybersecurity Tools and Updates*


## Conclusion:

COVID-19 has erupted the cyberspace and the need for being online and connected has never been more whether it is with our family, friends or colleagues. Being more online is being more vulnerable to cybercriminals. It is a recommended best practice to log-off whenever possible. The better we govern our online ethics and making it a priority to understand and practice privacy and data concerns as to where, why and to whom are we providing or opening-up or personal data? Using encryption when in doubt and understanding the correlation between one's everyday processes at preventing, detecting, and responding with best intentions and keeping in mind, how one's action impacts or triggers action for anyone else. Appreciate technology but get inspired to learn about it and assist others whenever possible, it is possible to pe prepared in advance and thwart cyberattacks. The key to securing and feeling secured about one's data is to keep a vigil on one's everyday cyber practices, and making sure we make judicious choices regarding important information. This would make us sail through the vast cyberspace of malpractices.