420

Certificate of Publication

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | E-ISSN 2348-1269, P- ISSN 2349-5138

An International Open Access Journal

The Board of

International Journal of Research and Analytical Reviews (IJRAR)

Is hereby awarding this certificate to

Karthik Anand

In recognition of the publication of the paper entitled

IMPLICATIONS OF CYBER CRIME DURING LOCKDOWN

Published In IJRAR (www.ijrar.org) UGC Approved (Journal No : 43602) & 5.75 Impact Factor

Volume 8 Issue 3 , Date of Publication:September 2021 2021-09-05 02:17:29

PAPER ID : IJRAR21C1897

Registration ID : 237683

R.B.Joshi

EDITOR IN CHIEF

UGC and ISSN Approved - International Peer Reviewed Journal, Refereed Journal, Indexed Journal, Impact Factor: 5.75 Google Scholar

IJRAR | E-ISSN 2348-1269, P- ISSN 2349-5138

491

(http://www.ijrar.org)

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR.ORG)

International Peer Reviewed & Refereed Journal, Open Access Journal

ISSN Approved Journal No: E-ISSN 2348-1269, P- ISSN 2349-5138

Journal ESTD Year: 2014

Call For Paper - Volume 8 | Issue 4 | Month- October 2021

(https://ijrar.org/submitonline.php)

()

Read all new guidelines related publication before submission or publication. Scholarly open access journals, Peer-reviewed, and Refereed Journals, AI-Powered Research Tool , Multidisciplinary, Monthly, Indexing in all major database & Metadata, Citation Generator, Digital Object Identifier(DOI) ()

Login to Author Home

(http://www.ijrar.org/Authorhome/alogin.php)

IJRAR.COM Repository

(https://ijrar.org/archivelist.php)

Login to Author Home

(http://www.ijrar.org/Authorhome/alogin.php)

Communication Guidelines

(https://ijrar.org/Communication%20Guidelines.pdf)

(Communication Guidelines.pdf)

(https://wa.me/916354477117/?text=Hi IJRAR)

Contact Us
Click Here
WhatsApp
Contact
Click Here

Send message

IJRAR Search Xplore - Search all paper by Paper Name , Author Name, and Title

(all policy.php)

422

(http://ijrar.org/callforpaper.php)
AIMS AND SCOPE (HTTP://IJRAR.ORG/CALLFORPAPER.PHP)

(all policy.php)
ALL POLICY (ALL POLICY.PHP)

(http://ijrar.org/faq.php)

(http://ijrar.org/contact.php)

(http://ijrar.org/faq.php)
FAQ PAGE (HTTP://IJRAR.ORG/FAQ.PHP)

(http://ijrar.org/contact.php)
CONTACT US (HTTP://IJRAR.ORG/CONTACT.PHP)

About IJRAR (Refereed Journal, Peer Journal and Indexed Journal)

International Journal of Research and Analytical Reviews (IJRAR) is a Leading high quality open access & peer reviewed quarterly published research journal. IJRAR is providing a platform for the researchers, academicians, professional, practitioners and students to impart and share knowledge in the form of high quality empirical and theoretical research papers, case studies, literature reviews and book reviews. The aim of the journal is to provide platform for diversity of intellectual pursuit from all corners of the society for enrichment and enhancement of the group readers. The Journal welcomes and acknowledges high quality theoretical and empirical original research papers, case studies, review papers, literature reviews, book reviews, conceptual framework, analytical and simulation models, technical note from researchers, academicians, professional, practitioners and students from all over the world.

The journal is being published Quarterly and in the multi-lingual likewise English, Hindi, Gujarati, & Sanskrit.

IJRAR is Scholarly open access journals, Peer-reviewed, and Refereed Journal, AI-Powered Research Tool, Multidisciplinary, Quarterly, Indexing in all major database & Metadata, Citation Generator, Digital Object Identifier(DOI) with Open-Access Publications..

Important Journal Details

Contact Us
Click Here
WhatsApp
Contact
Click Here

Journal Type: International Peer Reviewed, Open Access Journal, Scholarly open access journals, Peer-reviewed, and Refereed Journals, AI-Powered Research Tool , Multidisciplinary, Monthly, Indexing in all major database & Metadata, Citation Generator, Digital Object Identifier(DOI)

Issue Frequency: Quarterly (4 issue Annually)

Send messag

Publication Guidelines: Follow COPE Guidelines

ISSN: E-ISSN 2348-1269, P- ISSN 2349-5138 | ISSN Approved . ()

Current Issue Details (callforpaper.php): Call For Paper (Volume 8 | Issue (4) | Month- November 2021) (callforpaper.php)

Implications of Cybercrime during Lockdown

423

Mr. Karthik Anand[1]
Ms. Suremya SL
[1] BA.L.L.B, L.L.M, KSET, Asst. Prof of Law, SDM Law Mangaluru.

Abstract : The Novel COVID 19 virus has made various implications all over the world, India being one of them with over 80 lakh's people infected till date. Taking into consideration the risk of COVID19, the government announced an initial lockdown of 21 days across India which started from March 25, 2020. During this period all the private as well as government offices have remained closed and most employees are working from home, making security the next major concern. Security of companies is at stake as all data such as financial information, trade secrets, customer information and such other confidential information of the company is accessible to the employees from their homes with a click of a button. It is essential for employees to take utmost care of the company's data and secure it from other members of the family and friends in order to avoid misuse of data or breach of confidential information. Apart from company's information, personal sensitive information and financial information of an individual is also at risk in view of the increase in Cyber Attacks.

Key Terms & Definitions[2]

Anti-Malware—Software that prevents, detects and eliminates malicious programs on computing devices.
Antivirus—Software that prevents, detects and eliminates computer viruses.
Backdoor Trojan—A virus that enables remote control of an infected device, allowing virtually any command to be enacted by the attacker. Backdoor Trojans are often used to create botnets for criminal purposes.
Botnets—A group of Internet-connected devices configured to forward transmissions (such as spam or viruses) to other devices, despite their owners being unaware of it.
Cybercrime—Also known at computer crime or netcrime, cybercrime is loosely defined as any criminal activity that involves a computer and a network, whether in the commissioning of the crime or the target.
DoS—An attempt to interrupt or suspend host services of an Internet-connected machine causing network resources, servers, or websites to be unavailable or unable to function.

DDoS—Distributed denial of service attack. A DoS attack that occurs from multiple sources.

Malware—An overarching term describing hostile and/or intrusive software including (but not limited to) viruses, worms, Trojans, ransomware, spyware, adware, scareware, and other more, taking the form of executables, scripts, and active content.

[1] BA.L.L.B, L.L.M, KSET, Asst. Prof of Law, SDM Law Mangaluru.
[2]https://www.mondaq.com/india/operational-impacts-and-strategy/921026/cyber-crime-during-coronavirus-pandemic last visited on 13.10.2020

Phishing—An attempt to acquire sensitive information like usernames, passwords, and credit card details for malicious purposes by masquerading as a trustworthy entity in a digital environment.

Rootkit—Trojans that conceal objects or activities in a device's system, primarily to prevent other malicious programs from being detected and removed

Social Engineering—Non-technical malicious activity that exploits human interaction to subvert technical security policy, procedures, and programs, in order to gain access to secure devices and networks.

Trojan—Malicious, non-replicating programs that hide on a device as benign files and perform unauthorized actions on a device, such as deleting, blocking, modifying, or copying data, hindering performance, and more.

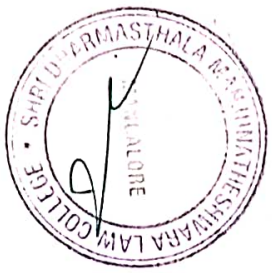
Zero-Day Vulnerability—a security gap in software that is unknown to its creators, which is hurriedly exploited before the software creator or vendor patches it.

Introduction

Cyber Crime : Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company or a nation's security and financial health.[3]

The Covid pandemic and lockdowns, which prompted people to stay inside the home and do their routine work using the computer, mobile and other electronic gadgets. This article concentrates mainly upon the following areas were Covid 19 had an adverse effect upon :

1. Cyber Crime and Social Media
2. Cyber Crime against women's
3. Financial Frauds
4. Cyber Fraud in banks
5. Data theft
6. Fake News or Rumours
7. Phishing Emails
8. E Commerce
9. Government
10. Healthcare : Fake medicines/Anti-Corona drugs



[3] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Cyber Crime and Online Platforms

More and more people, regardless of age and gender, are signing up for profiles on online social networks for connecting with each other in this virtual world. Some have hundreds or thousands of friends and followers spread across multiple profiles. But at the same time there is proliferation of fake profiles also. Fake profiles often spam legitimate users, posting inappropriate or illegal content. Fake profiles are also created while misrepresenting some known person to cause harassment to him/her.

The most common targeted websites/apps for creating 'Fake Profiles' are as under:

1. Facebook

2. Instagram

3. Twitter

4. LinkedIn

Below are the common crimes being committed on or as a result of Social Media:-

i. Online Threats, Stalking, Cyber bullying

The most commonly reported and seen crimes that occur on social media involve people making threats, bullying, harassing, and stalking others online. While much of this type of activity goes unpunished, or isn't taken seriously, victims of these types of crimes frequently don't know when to call the police.

ii. Hacking and Fraud

Although logging into a friend's social media account to post an embarrassing status message may be acceptable between friends, but technically, can be a serious crime. Additionally, creating fake accounts, or impersonation accounts, to trick people (as opposed to just remaining anonymous), can also be punished as fraud depending on the actions the fake/impersonation account holder takes.

iii. Buying Illegal Things

Connecting over social media to make business connections, or to buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled or banned products is probably illegal.

iv. Vacation Robberies

H26

Sadly, one common practice among burglars is to use social media to discover when a potential victim is on vacation. If your vacation status updates are publicly viewable, rather than restricted to friend groups, then potential burglars can easily see when you are going to be away for an extended period of time.

v. Creation of fake profile

Creation of fake profile of a person and posting offensive content including morphed photographs on the fake profile

vi. Fake online friendship

Developing online friendship over social media (with no real-life familiarity and using the emotional connect to trick you in transferring funds on some pretext such as medical emergency, legal troubles, problems in a foreign country etc.

Cyber Crime against women's

There has been a significant increase in cybercrime against women, especially sextortion, during the COVID-19-induced lockdown with "caged criminals" targeting them online, say experts. The nationwide lockdown imposed from March 25 to April 14, then extended to May 3, and again extended to May 15, aims at preventing the spread of the novel coronavirus that has claimed 1,147 lives and infected 35,043 people in the country.

According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April in comparison to 37 complaints - received online and by post - in March, and 21 complaints in February. The panel is taking complaints online due to the lockdown. Cyber experts, however, said the numbers are just the "tip of the iceberg". "We received a total of 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious ones from women, (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more," said the founder of the Akancha Foundation, Akancha Srivastava.

The organisation works for education and empowerment of people by imparting knowledge on cyber safety. Ms Srivastava said on an average she has been getting 20-25 such complaints daily, while before the lockdown the number was less than 10 per day. This is a "significant" increase, This is just the frustration and anger that is coming to the fore as there is no other release right now. This is a form of frustration as they (cyber criminals) are caged right now," Men are morphing images and threatening women. There is a whole racket going on where women are getting these emails that your phone and laptop has been hacked, and if you don"t deposit money my account I will send your morphed images, and share it with all your contacts," specially the cases of "sextortion" have increased during the lockdown.

Sextortion is extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity through means like morphed images."People are getting into relationships online as they are under lockdown and sextortion cases are being reported. In these times people are connecting through technology but forgetting the security component.

"Immediately after lockdown, rise in cases of misinformation, fake news and women getting duped online when they click on malware links which get all their information on the phone, turn on the camera and microphone, and capture their intimate moments. These are then used for blackmailing,"Many women do not want to make official complaints in these cases. "Cyber Peace has been receiving complaints through its channels and it has been seen that people are reluctant in filing complaints. Most of the complainants want to handle things unofficially," Whatever official figure that is being quoted is just the tip of the iceberg as a majority of women do not report cybercrime because they worry about the social stigma associated with it.

Vandana Verma, founder of InfoSec Girls[4], opinion about the whole country is locked down, people are working from home and spending a lot of time on the internet. So, even cyber criminals are becoming innovative and craftier in their techniques, she said. "Like sending specific phishing emails or themed emails for the current COVID-19e emails appear to have come from legitimate sources like the government in the form situation to people and getting their confidential details like address, phone numbers. Thes of advisories when they are not at all related to the government in any form,``"Creation of fake profiles, cyber bullying, online stalking are bigger challenges at this time. Insensitive comments on posts are also intimidating," she said.

How to securely use the digital media, creating strong passwords and spreading awareness on phishing emails, fake videos and securely sharing content on the internet can help a lot in safeguarding women. 'There is cyber police in every district who they can contact. They can reach out to us also if they need help. Always women to remain careful in cyberspace. "How women protect themselves in cyberspace. Women do not share their personal pictures or details on social media as it's not safe. Women should realise that at times people known to them can also take advantage[5]

Financial Frauds

Financial fraud happens when someone deprives you of your money, capital, or otherwise harms your financial health through deceptive, misleading, or other illegal practices. This can be done through a variety of methods such as identity theft or investment fraud. For all types of financial fraud it is important to report the crimes to the appropriate agencies and law enforcement as soon as possible. Fraudulent charges should also be disputed or cancelled as soon as they are discovered as well. Furthermore victims

[4] Global Board of Directors at OWASP & InfosecGirls

[5]https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352#:~:text=There%20has%20been%20a%20significant,targeting%20them%20online%2C%20say%20experts.&text=complaints%20in%20February.-,The%20panel%20is%20taking%20complaints%20online%20due%20to%20the%20lockdown,%22tip%20of%20the%20iceberg%22. last visited october 13, 2020

© 2021 IJRAR September 2021, Volume 8, Issue 3 www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138)

should gather all documentation related to the crime (e.g. bank statements, credit reports, tax form from current and previous years) and continue to file important information throughout the reporting process.

Unfortunately most victim compensation programs do not cover money lost to fraud or fraudulent schemes. Check your specific state laws regarding victim compensation to make sure. Civil justice may be the only legal option to recover lost money.

Common Types of Financial Crimes

i. Identity theft: Someone steals your personal financial information (e.g. credit card number, social security number, bank account number) to make fraudulent charges or withdrawals from your accounts. Sometimes people will use the information to open credit or bank accounts and leave the victim liable for all the charges.Identity theft often results in damaged credit rating, bounced checks/denied payments, and being pursued by collections agencies.

Examples:
Unfamiliar charges or purchases on your credit card or bank account statements. Perpetrators posing as a bank, government office, or official institution in order to steal your personal financial information

ii. Investment Fraud: Selling investments or securities with false, misleading, or fraudulent information. This may be false/grandiose promises, hiding/omitting key facts, and insider trading tips among other things.

Examples:
Ponzi schemes: Investment fraud scheme where returns are paid to investors using new capital from newly recruited investors as opposed to interest and profits from legitimate investments.
Pump & Dump schemes: Stock traders or stock brokers purchase a stock at a low value then entice other clients to buy the same stock in order to inflate its price. Those who bought the stock at its low value then sell their shares and pocket the profit.
Selling a business or real estate opportunity investment with bad, inaccurate, or false information. Also includes omitting or hiding information that is important investment decision.

iii. Mortgage and Lending Fraud: Someone else (often a friend or family member's) opens a mortgage or loan using your information or using false information
or
Lenders selling you mortgage or loans with inaccurate information, deceptive practices, and other high pressure sales tactics.

Examples:

- Mortgage and loan modification services
- Predatory lending practices such as:
- Unjustified risk-based pricing
- Single-premium credit insurance
- Failure to present the loan price as negotiable
- Failure to clearly and accurately disclose terms and conditions
- Short-term loans with disproportionately high fees
- "Bait and switch" contract negotiations
- Servicing agent and securitization abuses

iv. Mass Marketing Fraud: Often committed using mass mailings, telephone calls, or spam emails. Mass marketing fraud typically involves fake checks, charities, sweepstakes, lotteries, and exclusive club or honor society invitations. These offers and letters are used to steal your personal financial information or solicit contributions and fees to fraudulent organizations.

Examples:

Fake charity donation solicitations

Exclusive Club or Honor Society invites. Usually invitations are sent through mail or emailed and promise membership in a particular organization for a small fee or setting up a recurring charge with no discernable service provided. Also used to steal personal financial information.

Award or Prize notifications. Also seen on the internet as "10,000th Visitor" type notifications. Usually ask for personal financial information or fee to be paid in order for the prize to be delivered or the award to be made official. If you do not remember applying or entering a competition for the award or prize being given to you it is probably fraudulent. Phone calls claiming to be from the government, your bank, or other "official" agency.[6]

Cyber Fraud in banks

Amid pandemic when people are active online more than ever, the risk of them being targeted through cyberattacks has also increased. In order to make people aware, banks are now making aware customers and sending alert messages asking them not to share confidential information.

Since the lockdown has pushed people shiting to the online mode of transactions more than ever in the past, the vulnerability of their confidential information is also at high risk as cyber-criminals make take the advantage of lack of information by luring people by offering them free COVID-19 tests and other fraudulent means.

[6] https://victimconnect.org/learn/types-of-crime/financial-fraud/ last visited on 15.101.2020

Earlier, State Bank of India (SBI) also alerted customers. Taking to Twitter, SBI said, "Attention! It has come to our notice that a cyber attack is going to take place in major cities of India. Kindly refrain yourself from clicking on emails coming from ncov2019@gov.in with a subject line Free COVID-19 Testing."

Meanwhile, Standard Chartered Bank has also asked its customers to remain vigilant. In one of the alert messages, Bank said, "do not share any PIN, MPIN, OTP, Login Ids, passwords, debit/credit card no, CVV, expiry date etc with anyone. Standard Chartered Bank will never ask for such details. Also, do not click on suspicious links sent via email or SMS. They may mirror your device to steal confidential information such as OTPs."

In another message, the bank said, "As per the Computer Emergency Response Team are planning to send malicious emails promising free COVID-19 testing. Beware and do not click on suspicious links via email or SMS. They may mirror your device to steal confidential information such as OTPs. Please do not share any PIN, MPIN, OTP, Login Ids, passwords, debit/credit card no, CVV, expiry date etc with anyone."

Data theft[7]

Data theft is the act of stealing information stored on corporate databases, devices, and servers. This form of corporate theft is a significant risk for businesses of all sizes and can originate both inside and outside an organization.

The term data theft can give the impression that this kind of breach is based on malicious intent, but this is not always the case: data theft can also be an unintentional act: An employee may, for example, take home information on an unsecured flash drive or retain access to information after their contract has ended.

The malicious theft of employee data often occurs without the victims ever knowing about it, as a result of their accounts or personal devices being compromised by hackers capitalizing on poor password management or unsecure networks. Bad actors that gain access to companies' systems can lurk inside networks, pretending to be a legitimate user for days, weeks, or years. By remaining undetected, they can gain additional access rights to increasingly sensitive corporate datasets and pose a growing threat to unaware businesses.

Fake News or Rumours[8]

When the term "fake news" comes up, people usually think of social media posts with rather fantastic, implausible stories. While posts shared on social media is its most visible aspect, there is so much more to fake news than exaggerated article titles on social media feeds.

[7] https://www.okta.com/blog/2020/07/data-theft/

[8] https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media last visited 05.01.2020

431

a) Fake News and Cyber Propaganda

Fake news may seem new, but the platform used is the only new thing about it. Propaganda has been around for centuries, and the internet is only the latest means of communication to be abused to spread lies and misinformation.

The fire triangle represents the three elements a fire needs to burn: oxygen, heat, and a fuel. Similarly, fake news requires three different items to succeed. These collectively represent the Fake News Triangle: without any one of these factors, it is unable to spread and reach its target audience.

The first requirement: tools and services for manipulating and spreading the message across relevant social media networks, many of which are sold in various online communities from across the globe. A wide variety of tools and services are available; some are relatively simple (paid likes/followers, etc.), while some are more unusual—some services promise to stuff online polls, while some force site owners to take down stories. In any case, the tools and services for social media promotion are readily available, both inside and outside the underground scene.

Of course, for these tools to be of any use, social networks have to exist as a platform for spreading propaganda. With people spending more time on these sites as a way to get the latest news and information, their importance in spreading fake news cannot be underestimated. However, there's a difference between simply posting propaganda and actually turning it into something that the target audience consumes. We show what kinds of techniques are used by spammers in order to lure users into viewing their stories.

Studying social media also gives us a view of the relationships between bots and the recipients of social media promotion on Twitter. This gives us an idea of the scope and organization of the campaigns that attempt to manipulate public opinion.

Finally, propaganda campaigns always come with the question: *why*. We discuss the motivations behind fake news: sometimes it's simply a desire for monetary gain via advertising. In other cases, the goals can vary from the criminal to the political. Regardless of the motive, the success of any propaganda campaign will ultimately be based on how much it affects the real world.

Phishing Emails[9]

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to

[9] https://www.imperva.com/learn/application-security/phishing-attack-scam/ last visited on 05.01.2021

the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identity theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Phishing attack examples

The following illustrates a common phishing scam attempt:

A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible. The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

08. E Commerce[10]

The coronavirus pandemic set in motion many behavioral changes that are likely to stick, even after social-distancing requirements relax and businesses reopen. In just a few months, virtual fitness classes, video conferences and grocery delivery became ubiquitous—along with a new age of online retail shopping.

One of the most profound shifts for retail has been in softlines—apparel, footwear, linens and other segments—that prior to the pandemic, still thrived in brick-and-mortar stores. While e-commerce sales for these categories had already been ticking higher in recent years, lockdowns may have accelerated digital penetration for this segment by two years—and investors would be wise to note the shift.

[10] https://www.morganstanley.com/ideas/coronavirus-ecommerce-retail-shopping last visited on 05.01.2021

© 2021 IJRAR September 2021, Volume 8, Issue 3 www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138)

"Months of lockdown forced more consumers online. For the foreseeable future, will they now think twice before shopping in crowded stores, particularly if they can easily acquire those same goods online?" asks Kimberly Greenberger, who covers North American specialty apparel and department store retailers.

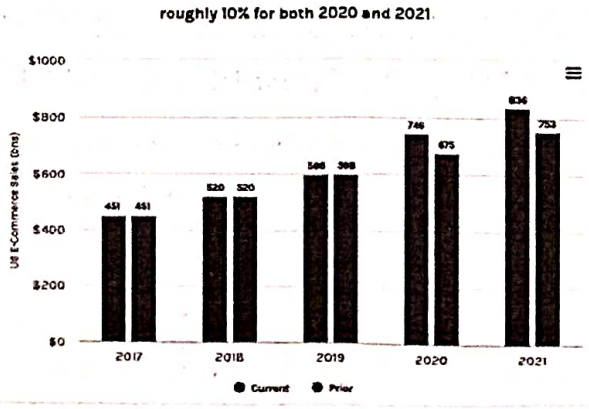
For 2020, Greenberger and her colleagues expect e-commerce to account for 32% of all softline retail sales—a 9% annualized increase. While she expects the share of online sales to drop slightly to 30% in 2021, a surge in digital adoption likely will have a material impact on retail brick-and-mortar margins that some investors don't seem to fully appreciate.

The upshot: E-commerce giants could stand to gain an even greater share of consumer wallets, at the expense of department stores and specialty retailers that rely heavily on in-store traffic. Among wholesale apparel and footwear brands with strong direct-to-consumer businesses, however, the outlook is upbeat, but nuanced.

Sheltering In and Shopping Online Consumers aren't spending as freely as they did before the pandemic. Among many households, a pattern has emerged. After initially stocking up on necessities, such as cleaning supplies and toilet paper, they began shopping online for discretionary items, such as clothing, household goods and outdoor equipment—purchases they rationalized because they weren't spending on travel or dining. "This year is setting up to be an e-commerce inflection, as the combination of sheltering-in-place, lower spending on experiences, and government stimulus have all driven more dollars online," says Brian Nowak, equity analyst covering the U.S. Internet industry. His team estimates that e-commerce grew 58% year-over-year in April, four times faster than in 2019 and in the first quarter of 2020.

All told, e-commerce could grow 25% annually in 2020, even if consumer spending weakens in the second half. "We believe that changes in consumer behavior mean more spending dollars are up for grabs," says Nowak. "Consequently, we're raising our U.S. e-commerce estimate by roughly 10% over what was previously modeled for both 2020 and 2021."

Morgan Stanley Research has raised their U.S. E-commerce estimates by roughly 10% for both 2020 and 2021



434

9. Government [11]

The current cybersecurity policy was established in 2013 with a vision to build secure and resilient cyberspace for citizens, businesses and the government.

Anticipating the boom in the IT industry and the resulting need of a cyberspace policy, the document was published with a mission to protect information and information structures, prevent and respond to cyber threats, and minimise the damage from cyber incidents.

Briefly, the policy tries to create a secure cyber ecosystem in the country with an assurance regulatory framework and establish a mechanism that can monitor and respond to threats. It also asks for the development of indigenous security technologies and the creation of a workforce of professionals skilled in cybersecurity.

The policy document tries to lower the risk of cyber threats by formulating several strategies to reduce supply chain risk, create cybersecurity awareness, develop private-public partnerships, and enhance bilateral and multilateral cooperation at a national and global level.

Cybersecurity after the onset of COVID-19

The onset of COVID-19 exposed the weaknesses in the current cybersecurity policy even further. With everyone needing to work from home, not within the firewalls of their firms, led to increased security incidents.

According to a survey conducted with employees across organisations in India, 66% of them faced at least one data breach. Security experts observed a 500% rise in the number of cyber attacks and security breaches and 3 to 4 times rise in the number of phishing attacks from March when the lockdown started in June.

There was also an increase in the number of financial transactions resulting in a rise of fraudulent attacks according to a report by the Data Security Council of India. A similar rise was also seen in the healthcare sector with fraudulent behaviour leading to theft identification, among other things. Over a thousand attacks were also reported in the education sector.

As a response to the rising number of attacks, the Home Ministry of India issued an advisory, with suggestions on prevention of cyber thefts, especially for those working from home. The Computer Emergency Response Team – India (CERT-In) also published the possible sources of cyber attacks and best practices that could be followed to ensure safety.

CERT-In also successfully conducted 'Black Swan – Cyber Security Breach Tabletop Exercise', to deal with cyber crisis and incidents emerging due to COVID-19 pandemic, resulting from lowered security controls as people work from home.

[11] https://analyticsindiamag.com/what-is-the-current-cybersecurity-policy-in-india-how-it-has-been-impacted-by-covid/ last visited on 05.01.2021

To account for the fraudulent behaviour in the finance sector, the government is also considering the setting up of a Computer Emergency Response Team for the Financial Sector (CERT-Fin).

Finally, the Prime Minister of India also announced a new cybersecurity policy for safe and secure cyberspace in India on Independence Day this year.

Direction of the new cybersecurity policy

As India comes up with a new cybersecurity policy in 2020, experts recommend a focus on domestic demands and greater incentives for the private sector to participate in government contracts.

There should also be greater engagement between the information security community and government. The policy should further facilitate an environment to encourage research in cybersecurity innovation.

10. Health Care: Fake medicines/Anti-Corona drugs

In this pandemic situation, and until the time an effective medicine or vaccine is discovered, there will be many advertisements, websites, and other forms of communication on medications, which may claim to cure COVID-19 completely. Further, platforms promoting counterfeit medicines to boost immunity level will also appear in the online market. Those fake websites ultimately lure people with the prospect of COVID-19 cure and compel them to pay online in advance. Either, there will be no delivery or bogus things/ toxic products that will be delivered in place of legitimate medicines.[12]

Exploiting the fear among the general public

Everybody who has been trapped inside their house amidst this lockdown is trying to stay on top of any information related to COVID 19 in an attempt to remain safe and away from infected people. The authors of malwares are taking advantage of this situation.

One such app which was available in Google Play Store was "corona live 1.1", which claimed to be a live tracker of cases of Coronavirus. The people using the app were of the view that they are keeping a track of the pandemic, but the malicious app was actually invading their privacy: getting access to the device's photos, videos, location and camera.

The information collected can be used in multiple ways, they can be used to compromise your bank accounts or even blackmail the owner of the pictures and videos.

The Android Playstore, to curb the rise of the fake apps, has removed many such apps from the Playstore and also have set rules for these types of applications and have put all such apps in the 'sensitive events' category.

[12]https://www.cnbctv18.com/information-technology/cyber-crime-in-times-of-covid-19-6-types-of-frauds-you-should-watch-out-for-in-coming-months-6287931.html last visted on 13.10.2020

Now the apps are available on fake websites, one such being 'coronavirus app.site', where the link to download the app is listed. These instances adequately demonstrate the rise in cyber crime on account of coronavirus.

Exploiting the 'work from home' policies

Every organisation, big or small, has been compelled to work remotely due to the lockdown. This will lead to increase in security risk as the proprietary data is being accessed from laptops and home PCs that may or may not have the same level of firewall and security as an in-office setup.

You may have noticed an increase in the number of emails in your Junk Folder, pretending to be an advisory relating to the COVID-19. These emails will entice the user to open the attachments, which are malicious in nature and the moment you open them the malware author will be able to access your system.

Once the malware has attacked one of the systems, there is a potential risk of the security of the systems of your colleagues also being compromised. This can affect the whole grid of systems by which the organization is staying connected and there can be a huge loss of confidential data. Thereby, leading to a spurt of cyber crime cases due to the coronavirus outbreak in India and worldwide.

At such times, the organisations can rely on the ISO/IEC 27000 family. The ISO/IEC 27000 is a global benchmark certificate which is given to the organisations which follow the Information Security Management System (ISMS). In addition to providing improvements in structure and focus of the organisations, the ISMS helps you to safeguard you and your client's confidential data from cyber attacks.

How to keep yourself safe

You can keep yourself safe from such scams and frauds with the help of Vigilance and Diligence. Here are a few pointers which should be kept in mind while accessing the above mentioned data:

- Check the App details on Playstore before downloading it, this includes, details of the developer, their website (if any), reviews and ratings given by other users.
- Avoid downloading apps from third-party stores and websites, and download the apps only available in the App Store for Apple IOs users and Google Playstore for Android users.
- Use reliable mobile and desktop antivirus, these can prevent fake and malicious apps from being installed.

Advisories are also issued by the Delhi Police and WHO due to rise of such frauds. Some of the DO's and DON'T's from the said advisories are as follows:

- Do not open email attachments that you have not asked for. In case you receive an attachment, it is always safer to open the same from WHO's official website and not the attachment in the mail.
- Always pay attention to the type of personal information you are asked to share. There is always a reason why your personal information is needed. In no circumstances, there would be a need for your passwords.
- Do not believe any emails that come with a sense of panic. Legitimate organizations will never want you to panic and they always take the processes step by step.

- Do not believe that WHO or any other organization conducts lotteries or offer prizes, grants or certificates through emails.

Steps to check authenticity of website

- HTTP = Bad, HTTPS = Good: The 'S' in https:// stands for 'secure'. It indicates that the website uses encryption to transfer data, protecting it from hackers.
- Check for easy markers such as spelling mistakes, typos and broken links. It is highly improbable for a legitimate business to have such mistakes on their website.
- Domain age: The imposters usually register a domain name just for a few months before changing the name of the domain and registering a new one. You can us search engines such as Whois.com to look up the information such as the date of registration of the Domain name.
- Look for reliable contact information: Try to do a background check. There is no harm in double checking with the company itself through alternate contact numbers.
- If you are a good Samaritan of the society and want to donate and help the needy then always donate only to the websites/apps whose authenticity is corroborated by the Government.

[13]Preventive Measures/Precautions

1. Block profiles from public searches.

2. Restrict who can find you via online search.

3. Limit what people can learn about you through searching on net.

4. Log out after each session.

5. Don't share social media credentials.

6. Don't accept friend requests from unknowns.

7. Don't click suspicious links.

8. Keep the privacy settings of your social media profile at the most restricted levels, esp. for public/others

9. Remember that information scattered over multiple posts, photographs, status, comments etc. may together reveal enough about you to enable a fraudster to steal your identity and defraud you. So, apply maximum caution while sharing anything online.

Conclusion

It is certain that the security standards have deteriorated as many organizations were not ready to work remotely and a rise has been witnessed in cyber crime due to coronavirus. With a little vigilance and due diligence we can protect our data and privacy. It is always better to stay on the side of precaution but if, even after taking all the precautions, we fall into a trap then a quick action can salvage the loss. It is advisable to lodge a complaint with the appropriate authority.

[13]https://www.mondaq.com/india/operational-impacts-and-strategy/921026/cyber-crime-during-coronavirus-pandemic last visited on 14.10.2020