https://doi.org/10.48047/AFJBS.6.12.2024.352-371

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Unveiling the Digital Deception: A Comprehensive Legal Examination of Identifying and Preventing Internet Fraud

First Author
Ms. Gazal Gupta,
Master of Laws,
London School of Economics,
United Kingdome.
E-mail: guptagazal08@gmail.com
Orcid id: https://orcid.org/0000-0002-7232-5133

Corresponding Author
Dr. Amit Yadav
Assistant Professor (Senior Scale)
Faculty of Law, Manipal University Jaipur
Email- amit.yadav@jaipur.manipal.edu
ORCID :https://orcid.org/0000-0001-9310-0112

Co-Author
Ms. Neha Garg,
Advocate, High of Court of Judicature,
Rajasthan.
Email - nikki.ngarg2017@gmail.com

Article History

Volume Issue 12, 2024
Received: 25 May 2024
Accepted : 25 June 2024
doi:
10.48047/AFJBS.6.12.2024.352-371

Abstract

The paper discusses various aspects of cybercrime and spamming. It emphasizes the need for international cooperation to combat cybercrime, educates people about internet scams, and provides prevention tips. It also highlights different types of spam, such as blank spam and backscatter spam, and the industries that are most affected by fraud. The document also mentions the lack of awareness among people about online scams and the need for clear communication of warnings. Lastly, it talks about the laws related to spamming and how spammers take advantage of people's lack of knowledge about technology.

Introduction

Internet fraud is a subset of cybercrime that involves deceit and the use of the Internet. It may involve the hiding of facts or the dissemination of false information in order to defraud individuals of their hard-earned money, assets, and inheritance. The authors have conversed with various people who have mentioned incidents like false Amazon messages for jobs, creating fake IDs and stealing people's information, selling someone else's accommodation and taking money for it. There are various other types of fraud, like when in order to raise money for victims of a natural catastrophe, terrorist attack (like the 9/11 attacks), local strife, or pandemic, the con artist assumes the identity of a humanitarian organisation. Xclusive Leisure and Hospitality, a US-registered company, sold tickets for the 2008 Olympic Games in Beijing using a well-designed website called "Beijing 2008 Ticketing." It was soon revealed that bogus tickets had been sold on the internet for more than A$50 million.[i] Cybercriminals may approach prospective victims via personal or professional email accounts, social networking sites, dating apps, or other avenues in order to gather financial or other essential personal information. Many good internet con games end in the same way: the victim either loses their own money or does not receive the promised money from the con artist.[ii] However, it differs from stealing as the victim knows and deliberately gives the offender the information, money, or property in this instance.[iii] In a survey the authors conducted in 2021, 62.8% of participants knew their legal rights and the laws applied to them, but there are still a significant number of individuals i.e. 37.2% who are unaware of scams and the rules that govern them. When the researchers filed an RTI for data on internet fraud in India affecting several states on 17/06/2021, the following response was given: This is in response to your request, which was recorded under Registration number NICHQ/R/E/21/00256. This office has dealt with your request. Action date: 21/06/2021 The following is my response to your RTI inquiry:

There is no evidence on the record. Under the RTI Act, 2005, only information that is available, existing, and held by the public authority or under its supervision may be provided.

The PIO is not permitted to produce information that is not part of the record.

Therefore, it is essential to educate people about online fraud and offer recommendations for reducing it.

Research Objectives

The research aims to analyze what online fraud is and the different types of it. The article also looks into a number of factors that contribute to online fraud and analyses incidents involving computers or the internet that have happened in Rajasthan. The paper will also go over a range of suggestions that might help cut down on these scams and raise internet users' awareness.

Research Methodology

The research in this area is complicated due to minimal literature on internet fraud. The approaches and methodologies to used in addressing the issue is varied and far-reaching. The following methods have been used, firstly, direct dbservation, the data has been collected from observing the environment. Secondly, the authors have scrutinisied the digital content including numerous articles and high quality papers published in numerous journals. Thirdly, data has been collected via surveys, the questions were related to whether they or their family members have faced online frauds and the solutions that they believe should be implemented. Lastly, interviews were taken of legal luminaries along with filing of an RTI. It is safe to conclude that both primary and secondary sources were used to conclude this research.

Internet Fraud

The phrase "Internet fraud" refers to a wide range of crimes, including identity theft i.e. phishing, health care fraud, and computer hacking to get personal information to commit crimes or demand ransom.[iv] It also includes the use of online tools and programmes with internet connection to deceive or exploit people.It is a catch-all term for online or email-based cybercrime such as identity theft, phishing, and other hacking-related crimes meant to mislead victims..[v]

The Internet allows you to contact a big number of people without spending a lot of time or money. A website, online message, or social media platform may reach a large number of people quickly.It might be challenging for investors to distinguish between reality and fiction since it is simple for con artists to make their communications seem authentic and genuine.[vi]

Another term that is closely linked to Internet Fraud is Computer Fraud.Computer fraud is described as the use of a computer or computer system to aid in the execution of a scheme or unlawful action, as well as the targeting of a computer with the intent to modify, damage, or disable it..[vii]There are various types of frauds using the internet i.e. Phishing, Spamming, identity theft, banking fraud etc. The research will mainly focus upon two common types of internet fraud i.e. Phishing and Spamming.

Types of Frauds

Phishing

Phishing is a popular sort of cyber-attack that everyone should be aware of in order to be protected. The term is an informal variation of fishing (ph is a popular substitution for f), and it relates to the employment of more sophisticated lures to "fish" for users' sensitive information. Fraudsters utilise this strategy to steal personal information.[viii] In this type of scam, criminals send emails posing as a legitimate or well-known firm. These emails often include a link or an attachment. If a user clicks on those links, he will be sent to a bogus website. The bogus website will request sensitive information such as credit card numbers, UPI codes, and other bank information. Furthermore, clicking on such URLs will result in a malware assault on his machine.[ix]The goal is to steal personal information like credit card numbers and login credentials, or to install malware on the victim's computer.[x]

When an institution is the target of such an attack, it frequently suffers significant financial losses as well as a loss of market share, reputation, and consumer confidence. A phishing effort, depending on its scope, may result in a security disaster from which a corporation would battle to recover.[xi]The proliferation of phishing kits makes it easier for cyber criminals, even those with low technical skill, to start phishing campaigns. A phishing kit is a bundle of phishing website resources and tools that just need to be hosted on a server. Once installed, the attacker just needs to send emails to innocent victims. Phishing kits and mailing lists may be found on the dark web. Phishtank and OpenPhish give crowd-sourced lists of known phishing kits. Some phishing kits allow attackers to imitate well-known companies, increasing the probability of someone responding on a fraudulent link[xii]. In order to prevent the phishing attacks anti-virus and spam filter software's are to be installed, firewalls should be on. Customers should access the website only through the Internet browser's status bar or the "https://" at the start of the URL in the address bar.[xiii]

Phishing can be through any technological device, one of them being Phone phishing. Phone phishing is one type of identity theft; identity theft is the theft of someone's identity in order to get access to their personal financial data, which is then exploited by fraudsters to conduct fraud. The phrase "phishing" was first mentioned in KoceilahRekouche's cracking toolkit AOHell in 1995, however it is likely that the phrase has been used previously in a print version of the hacker magazine 2600.[xiv]In a survey, conducted by the authors in 2021, an anonymous source mentioned that “My cousin clicked on a phishing email and her laptop's camera kept turning on randomly and a friend's parents were scammed by those spam lottery email things for some money”.

Types of Phishing

1. E-mail: Bulk phishing is the delivery of phishing emails that are not tailored or targeted to a particular person or business.[xv]These emails are sent by hackers to any email address they can find. Oftentimes, the email notifies you of a breach in your account and urges that you respond immediately by clicking the link. Because emails commonly include grammatical and/or typographical errors, these attacks are usually easy to spot. Some emails may be difficult to detect as phishing efforts if the text and grammar are more carefully written.You can determine whether the source is reliable by scanning the email and the URL you're being sent to for any suspicious wording.[xvi]
2. Content Spoofing: An attack on a user made feasible by an injection vulnerability in a web application is called content spoofing, also known as content injection, "arbitrary text injection," or virtual defacement. An attacker can send material to a web application, generally via a parameter value, that is mirrored back to the user when an application improperly handles user-supplied data. In the context of the trusted domain, this displays the user with a changed page. Because it relies on a user's trust and a code-based vulnerability, this attack is frequently employed as, or in addition to, social engineering.[xvii]
3. Link Manipulation: The method used by the phisher to provide a link to a malicious website is known as link manipulation. When a user clicks on the false link, the phisher's website rather than the one that is specified in the link opens. Users are prevented from falling for link manipulation by hovering the mouse over the link to reveal the true URL.[xviii]
4. Mobile Phishing: One of the most common sub-types of phishing is mobile phishing, which you should be aware of. Due to users' frequent usage of mobile devices, it is one more method fraudsters employ to deceive victims into disclosing personal information. Smartphones and app use have the same phishing hazards as using any other internet system, but they also carry unique threats like SMiShing and Vishing that may occasionally be considerably more hazardous for victims.[xix]
5. Voice Phishing: Voice phishing assaults are often carried out via computerized text-to-speech systems that instruct their victims to contact a phone number belonging to the attacker, however some utilise live operators. The fraud aims to get confidential information of the victim as well as financial records on credit cards, bank accounts (such as the PIN), and certain other private details by acting as a representative of a reputable firm, such as the bank, police, telephone company, or internet service.A scammer might use the information to get access to the account that they have gotten and empty it or perform identity fraud.[xx]

Recognizing Phishing attacks

1. Malware in electronic devices: A virus in any electronic device within a person's grasp, whether it's a laptop, mobile phone, tablet, or even Wi-Fi routers, might be a phishing trail.
2. Data loss: A breach of the victim's sensitive information's security, or the disclosure of credit card numbers, pan card numbers, or other personal information.
3. Illegal use of the user's information: When a user's information is used for any reason without the user's knowledge or consent, it might be the outcome of a phishing effort.
4. Financial loss: Access to a person's financial account data, which results in unexpected transactions from an user's profile, might have been the consequence of phishing. Those transactions are either one-time large payments or recurrent little sums.

To defend oneself from phishing, an individual should enable his desktop or phone's software to regularly update so that it can deal with any access control risks. Secondly, some institutions add further security by requiring two or more credentials to log in. This is known as multi-factor authentication. If fraudsters gain the user's username and password, multi-factor authorization makes accessing the profiles more difficult. Lastly, backup your data and make sure it's not linked to any home networks. The information on a person's PC can be transferred to an alternative hard drive or cloud - based.This may keep him from falling victim to phishing.[xxi]

Phishing Laws and regulations

In India, the Information Technology Act of 2000 offers both defence and punishment against cybercriminals. One of the offences mentioned in Section 43 of the IT Act is unauthorised access to a computer resource. A breach of Section 43 of the Information Technology Act carries a maximum sentence of three years in imprisonment or a fine of INR 5,000,000..[xxii] Furthermore, using an electronic signature, passcode, or any other distinctive identifying feature illegally or dishonestly, as well as abusing a variety of software applications for scamming, is punishable by up to three years in prison and a fine of up to INR one lakh under the IT Act.[xxiii]

Organizations that handle personal data are subject to the Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules, 2011 (SPDI rules). According to the SDPI regulations, bodies corporate must only keep as much information as is required for the purposes for which it was collected. They must also uphold acceptable security policies and protocols and only send personal data to recipients that adhere to the same or higher security requirements.[xxiv]

Payments data may only be retained in India, according to a separate Reserve Bank of India (RBI) regulation on the preservation of payment system data. Although the primary objective of the directive is to grant the RBI access to all payment data so that it can monitor transactions, it will likely also make it easier for law enforcement to identify and penalise payment system operators who don't take the appropriate security safeguards.[xxv]

On November 23, 2001, the Convention on Cybercrime of the Council of Europe was made available for signing. The Convention is the first international agreement made with the intention of addressing various types of crimes perpetrated through the Internet and other computer networks.[xxvi]

Famous Phishing attacks

1. The Moscow World Cup vacation rental fraud is one of the largest and most recent in world history. The FIFA World Cup is a highly popular event that draws spectators from all around the world to watch it live. A similar line of events occurred at the 2018 FIFA World Cup in Moscow. Many individuals from other nations had planned to go to Moscow. This fueled the excitement of phishing fraudsters from all over the world, resulting in the financial loss of a large number of victims. This swindle cannot be attributed to a single entity conducting a systematic fraudulent endeavour. Many fraudsters attempted to make private financial gains at the expense of unsuspecting football fans. Email, WhatsApp, and SMS were the most often utilised means for accomplishing the same. These fraudsters sent many emails to various consumers. These emails frequently promised reduced hotel rooms, free flights to Moscow, and other perks. Bookings.com users were targeted via SMS and WhatsApp in another high-profile example. The communications delivered to their unwitting consumers contained real information gained by hacking into hotel systems.[xxvii]
2. Operation Phish Phry: The FBI labelled the largest international phishing case ever carried out as Operation Phish Phry in 2009. Hundreds of bank and credit card customers were sent official-looking emails that led them to bogus financial websites. The fraud squad was exceptionally well-organized. When it pertains to aggressive, large-scale cyber-attacks, Robert Mueller, the then-director, portrayed it as an example of how enormous organised crime syndicates are indistinguishable from national-state participants. There is just no way of knowing who the genuine offender is until the investigation is done. From the start, it was evident that Operation Phish Phry was a massive endeavour. In the end, the FBI prosecuted over 100 people, depending on Egyptian national defense authorities' assistance to imprison more than half of them outside the United States territory.The scheme was quite simple by today's standards, yet it managed to steal roughly $1.5 million from hundreds or maybe thousands of bank accounts.[xxviii]
3. RBI Phishing Scam: The Reserve Bank of India was not spared in a daring phishing assault of its sort. The phishing email, disguised as originating from the RBI, promised the receiver Rs.10 lakhs in winnings within 48 hours by giving a link to a website that seems identical to the RBI's main site, replete with a matching logo and website link. Following that, the user is required to enter personal details such as his passcode, I-pin number, and bank account number. The RBI, in contrast hand, published a warning on its official website about the phoney phishing e-mail.[xxix]

Spam

Spam is a catch-all phrase for electronic 'junk mail' or unsolicited communications delivered to a person's email account or mobile phone. These messages differ, but they are primarily commercial and, due to their volume, can be unpleasant. They may attempt to persuade the user to purchase a product or service, or to visit a website where he or she may make transactions; or they may attempt to dupe a person into disclosing bank account or credit card information.[xxx]Unwanted emails sent in mass are referred to as email spam, spam mails, or just spam (spamming). The expression is a pun on a canned pork product name from a Monty Python sketch.[xxxi] Each country has its own definition and legal standing for spam, but neither legislation nor legal action have been particularly effective in getting rid of it. Spam emails predominately have a promotional bent. Many, whether they are commercial or not, are not only obnoxious as a form of attention-getting, but also risky since they may contain links to phishing websites, websites that host malware, or even files that contain malware.[xxxii] By exploiting chat rooms, websites, customer databases, newsgroups, and viruses that scan address books, spammers are able to collect email addresses from users. Sometimes, these gathered email addresses are sold to those further spammers.

Types of Spam

1. E-appending: It is also known as email appending, is a marketing technique that includes obtaining email addresses by matching pre-existing customer information (first name, last name, and postal address) with a vendor's database. Increasing one's email subscriber base is done with the intention of delivering consumers information via email rather than postal mail. In the field of email marketing, email appending is a contentious practise. Critics contend that sending email to recipients who have never expressly opted-in is against best practises. A consumer or business database of contacts, containing their name, address, and firm name [for business contacts], is used in the email appending process. The corporation can work with a service provider that has a database of email addresses to combine the data and add customer or business email addresses to their current file if they wish to grow into email communication. By doing this, they may maintain a database that has the most recent email addresses for everyone on the list. The quality of the two databases being joined determines how well email appending works. A marketer can pay to have their database compared to an external database that has email addresses if they have a database with names, addresses, and phone numbers for their consumers. The corporation then has the ability to email those who have not requested email, including those whose email addresses have been suppressed.[xxxiii]
2. Image Spam: The spam message text is inserted in images, which are then attached to spam emails, a process known as "image spam." Because the majority of email programmes display the picture file to the user right away, the spam message is transmitted as soon as the email is opened (there is no need to further open the attached image file).The purpose of picture spam is obviously to avoid being detected by the majority of spam filters, such as SpamAssassin, which analyse the email's textual content. As a result, for the same reason, spammers frequently include some "bogus" language to the email in addition to the attached image, namely a few phrases that are more likely to exist in valid emails than spam.[xxxiv]
3. Blank Spam: Spam without a payload advertisement is known as blank spam. Both the subject line and the message body are frequently completely absent.[xxxv]Still, because it is mass and unsolicited email, it satisfies the definition of spam. To transmit blank spam, a directory harvest attack, a sort of dictionary attack designed to capture valid email addresses from an email provider, might have been utilised. It might also happen if the spammer forgets to add the payload when configuring the spam operation. Many spam mails may look blank while in fact they are not. The email worm VBS.Davinia.B is an example of this, since it spreads through emails that appear to be blank and without a subject line but actually include HTML code that uploads further files.[xxxvi]
4. Backscatter Spammer: Backscatter is a byproduct of worms, viruses, and spam email. When email is rejected or quarantined, incorrect configuration on email servers causes a false bounce message to be sent to the sender of the envelope (rather than simply

> rejecting the attempt to send the message). Because they were not requested by the receivers, were sent in large numbers, and were very identical to one another, recipients of these communications see them as spam or unsolicited bulk email. Systems that produce email backscatter may be in violation of the terms of service of internet service providers and may be put on different email blacklists. Worms and spam communications frequently counterfeit their sender addresses, which causes backscatter. The majority of rejections can be made at the initial SMTP connection stage, avoiding the need for a bounce message. In other cases, bounce messages should only be sent to addresses that can be reliably judged not to have been forged. In those situations, the sender cannot be verified, so the message should be ignored.

First and foremost, health and medical services are where frauds are most regularly found. Spammers commonly pitch miracle cures, rapid weight loss solutions, dubious nutritional supplements, hair loss remedies, anti-aging procedures, and alternative pharmaceuticals. The majority of these items are nothing more than empty promises. Furthermore, there is dating and adult content, which can range from pornographic websites and bedroom performance enhancers to online dating and matching services. In conclusion, Spam from technology Spammers try to take advantage of the fact that so many people lack computer knowledge. Don't be taken in by advertisements for either software or hardware, internet or cellular technologies, or miscellaneous gadgets.

The “Spamming” Laws

Because the recipient of spam must pay the running expenses from internet service providers, spam may not be regarded as junk mail. Indian computers are frequently used with out-of-date or illegal software, leaving them particularly susceptible to malware attacks and spam produced by viruses. In a groundbreaking ruling in 2004, the Delhi High Court severely punished McCoy Company for sending unlicensed and unwanted email to VSNL.[xxxvii] While many nations across the world have criminalised spamming through different anti-spam legislation, spam mail or the resulting data loss are still viewed as tortious acts in India. The Information Technology (Amendment) Act, 2008, has Section 66A, which punishes the sender of dishonest e-mails with three years in prison in an effort to address the spam issue in India. Even while the clause did not specifically name spamming, phishing, or pharming, it was a sincere effort to curb spam in India. Law enforcement authorities started abusing this clause by erroneously prosecuting members of the public for voicing their thoughts.[xxxviii] In Shreya Singhal v. Union of India, the Supreme Court subsequently declared the clause to be "unconstitutional" and invalidated it. Despite the lack of clear anti-spam legislation, those who engage in the practise may nevertheless face legal action under other laws and regulations that control the illegal content shared online and impose penalties for fraud and deception.[xxxix]

A virus or trojan horse in spam e-mail might infect the recipient's machine and install itself there, exposing personal information to attackers. In that order, India, Brazil, West Africa, and Vietnam are the origins of "bad" ISPs.[xl] These cybercrime operations are mainly committed in nations that do not participate in multilateral agreements or that do not have laws specifically outlawing them. The timing is right for India to make spamming a crime by drawing inspiration from other nations across the world, despite the monumental burden of determining what constitutes offensive spam mail.[xli] In 1999, both Austria and Italy made spamming illegal in their respective nations.[xlii] Other laws and regulations governing spam include the Consumer Protection (Distance Selling) Regulations of 2000 in the UK, the Unsolicited Electronic Messages Act of 2007 in New Zealand, the Spam Act of 2003 in Australia, the Directive on Privacy and Electronic Communications of the European Union, and others.

Some of the popular spams are, first, One of Airbnb's founders, Nathan Blecharczyk, who financed himself through Harvard by lodging spammers, is an established spammer.[xliii] Second, Shane Atkinson, who was named in an interview with The New Zealand Herald, ran an operation in 2003 that sent out 100 million emails every day. Shane Atkinson asserted (and appeared to fulfil) unsubscribe requests, and he declared shortly after the interview that he was discontinuing spamming. American officials imposed a $2 million punishment on Lance. Third, Canter and Siegel, a married couple famous for sending one of the first business Usenet spam adverts to thousands of threads and defying 1000s of mail rebukes. They claimed that the advertisement netted them more than $100,000.[xliv] Fourth, the social networking site Tagged was eventually split out from Jumpstart Technologies, an incubator of the well-known social network Hi5 and the first company to pay a $900,000 penalty for breaking the CAN-SPAM statute. Tagged later paid more than $1.5 million in penalties and court settlements including both government agencies and private persons, and Time magazine dubbed it "the world's most irritating website."[xlv] Finally, Khan C. Smith emerged as the first important prolific spammer and tech pioneer to be sued by a prominent ISP, resulting in a $25 million penalty and the collapse of the world's largest spam network. As per court records, his illegal network delivered more than 25percent of total of all email transferred globally until 2001.[xlvi]

Intention of the spammer is what separates spamming from phishing (or phisher). Although they might be annoying, spammers often have no malicious intentions. They have a product or service to sell, and they have determined that spamming is a successful strategy for spreading the word about it. Phishers, on the other side, are cybercriminals who seek sensitive personal information by using malware or trickery. Like spam, phishing schemes are sometimes sent in quantity, but they have more sinister objectives, such as fraud, theft, and even corporate espionage.

Causes of internet fraud

Organizations have been anxious about online fraudulent transactions since the emergence of e-commerce in the nineties, and the problem is only growing with every passing year. Experian found that fraudulent identity losses had grown from 51% in 2017 to 57% in 2019. According to PwC[xlvii], the cost of these crimes to firms in the preceding 24 months was $42 billion[xlviii].

1. **The worldwide COVID-19 crisis has wreaked devastation.**
   Opportunistic hackers are using the global crisis to commit even more heinous crimes. Among the methods used include the robbery of stimulus checks and unemployment compensation, the collecting of cash for phoney COVID-19 treatments, the duping of Americans into donating to fraudulent charities, and others. In actuality, 1.1 billion fraud attempts were made in the first half of 2020, which was more than double the numerous attempts attempted in the second quarter of 2019. As reported by the Federal Trade Commission, COVID-19-related fraud cost Americans $145 million.

2. **The e-commerce landscape is changing.**

The transfer of retail transactions online is another element impacting the rise in fraud. Card not present (CNP) payments,[xlix] in particular, have grown rapidly In recent decades, card present transactions have accounted for 27% of all debit card transactions in 2019 and are growing at a rate ten times that of card refer to the amount. Clients are staying at home as a result of COVID-19, and more commerce is shifting online. This proclivity makes it easier for unscrupulous actors to undertake improper deals. Point-of-sale (POS) banking is also growing increasingly popular, allowing individuals to pay in instalments or obtain credit for both large and small purchases.

3. **New marketplace platforms are emerging.**

From social networks and dating applications to food delivery, substitute conveyance, and vacation rentals, streaming services have transformed practically every business.

Throughout this year, nationwide quarantines have resulted in even more smartphone app use, with consumers purchasing anything from food to distribution trucks. With the growing availability and popularity of marketplace applications and services, particularly in recent times, scammers have altered their strategies to capitalise on increased in-app and web services transactions.

4. **Electronic transactions are becoming more common.**

P2P and eWallet apps, in addition to retail websites, are becoming popular among users. These programmes are mainly popular in Europe and Asia, but they are gaining traction in the United States, with seventy one percent of Americans utilizing a peer-to-peer payment mechanism. Users use these platforms to send money to their family members across the world, purchase for local vendor services, and a lot more. However, the danger is high since more than half of all P2P payments are between clients and an unknown organization[l].

5. **Banking services are progressively being computerised.**

Today's consumers expect their financial institutions to provide more digital and mobile services. As a consequence, old banks are being digitized. They are expanding online account onboarding and transaction approvals while lowering in-person transactions, which makes credential validation more challenging. To meet client needs, a new breed of "challenger banks" has evolved, created, and done business entirely online, differentiating itself by offering user-friendly and cloud-based services. The vast majority of consumers of these banks have "thin file" credit histories (i.e., little credit data). The likelihood of fraud grows if there is less data.

6. **More sophisticated deception tactics.**

As the amount of data breaches has increased over time, fraudsters may now get personally identifiable information and exploit it against customers with greater ease. Fraudsters, for example, may combine genuine and phoney data (such as one person's location coupled with another's social security number) to construct new, synthesised identities which are more harder to identify.[li] Then, acting as actual consumers, they open bank accounts and credit cards. Once they've established good credit, the scammers will request better credit limits or larger debts, then just stop paying. Identity fraud is not only beneficial to people, but it also costs lenders $6 billion each year. Scammers also use PII to gain access to accounts. These actions can range from anything as basic as using a debit card to something as dangerous as taking out a mortgage using anybody else's accounts. Account takeover theft poses a severe threat to customers, with Juniper Research forecasting losses of much more than $200 billion between 2020 as well as 2024[lii].

Many worldwide groups, both governmental and non-governmental, are concentrating on cybercrime, including internet fraud.

1. ITU stands for International Telecommunications Union (ITU)[liii]

2. the European Council[liv]
3. Organization for International Criminal Police Cooperation (INTERPOL)[lv]
4.Office of the United Nations Office on Drugs and Crime (UNODC)[lvi]
5. Working Group on Anti-Phishing (APWG)[lvii]
6. Spamhaus[lviii]
7. Internet Hotlines International Association (INHOPE)[lix]
8. European Non-Governmental Organization Alliance for Child Safety Online (eNACSO)[lx]
9. Internet Watch Foundation, Inc. (IWF)[lxi]
10. Rand Corporation[lxii]

Effects

Loss of money is perhaps the most evident consequences of cybercrime, and it may be fairly severe. However, cybercrime has a number of additional devastating implications. After a security incident causes a decline in the value of a company, shareholder perception may turn into a major issue. Businesses may also suffer higher borrowing rates, and acquiring more funding may be difficult following a security incident. Charges and penalties for failing to secure sensitive customer data might occur from the compromise of sensitive consumer data. Businesses may face legal action as a result of data breaches. Customers' trust in a company will dwindle as a result of a cyberattack's loss of credibility and weakened brand identification[lxiii]. Corporations not only lose present customers but also have difficulty gaining new customers. Financial expenditures such as engaging cybersecurity professionals for cleanup, higher insurance healthcare premiums, public affair, and some other services linked to the assault may also be incurred[lxiv].

The harmonization of legislation on international level

The main points of global harmonization to assess the key challenges of these international institutions based on prior representation on global internet fraud and anti-cybercrime activities.[lxv]

1. **Raising security awareness on a global scale.**

The UN has taken the required steps in this respect. The United States' two Resolutions on Trying to combat the Criminal Misuse of Computer Technology (55/63 (2000) and 56/121 (2001)) highlighted the relevance of the Group of Eight principles and asked nations to consider them.[lxvi] Other resolutions urged member countries to encourage multilateral examination of present and prospective information security vulnerabilities, as well as feasible solutions to these problems. Several international bodies have also worked to raise public awareness of global security. Aftermath of the 9/11 attacks, for instance, APEC leaders proposed that APEC activities be tightened to protect key infrastructure.

2. **Promotion of state-level security awareness**

Every global organization has attempted to raise local and regional awareness. For instance, the Asia-Pacific Economic Cooperation[lxvii] has directed its member countries and regions to strengthen cybersecurity and combat cybercrime and internet fraud. The APEC also had a mechanism in place for wealthier countries to help poorer countries train staff. The Shanghai Declaration of 2002 called for actions to combat information abuse.

3. Harmonization of legislation

Numerous international organizations' activities have placed a heavy emphasis on legal harmonization. Harmonization in Europe began in the 1980s, with the Convention on Cybercrime being the most recent achievement. Other international organizations have also tried to establish legal equality.Interpol performed a study of member nations' criminal laws in early 1981 in order to find weaknesses in present legislation and to seek to harmonize the laws[lxviii]. Interpol's African Working Party on Information Technology Crime Initiatives is now working to obtain African countries to join and accept the Cybercrime Convention. APEC also made measures to study regulations and encourage economies to establish comprehensive legislation in accordance with the Cybercrime Convention and relevant UN resolutions. The 2002 EU Framework Decision expressly entrusted national governments with criminalizing unauthorized entry to and monitoring of data systems. The REMJA recommended that countries prosecute cybercrime, regulate their legislation, and eventually join the Cybercrime Convention. The Commonwealth Model Law on Computer and Computer-Related Crime broadened the criminal liability under the Convention against Cybercrime to include reckless irresponsibility. The Commonwealth takes steps to combat cybercrime in member nations through its Model Law.The Group of Eight Paris Conference looked at how the public and private sectors may work together to create a global criminal code to tackle cybercrime. The Okinawa Charter on Global Information Society also agreed on international engagement and harmonized in the battle against fraud.[lxix]

4. Coordination and collaboration among law enforcement

The Computer Crime Handbook was produced by Interpol's European Working Group on Information Technology Crime to give technical support to enforcement agencies. The Convention on Cybercrime also outlines ways for law enforcement coordination in cybercrime. In 2001, the EU explored retaining traffic information. The Expert Group on Cybersecurity (REMJA) of the Americas' Ministers of Justice or Ministers or Attorneys General has been attempting to identify solutions for the Inter-American system to work in combating cybercrime. The Group of Eight examined existing collaboration channels and limitations, attempting to overcome these gaps.The Group advised countries to increase crime, punishment, investigations, and international collaboration. The Denver Summit urged governments to strengthen their technical and legal ability to combat transnational computer crimes. In order to tackle a wide range of criminal offenses, particularly cyberattacks, the Birmingham Summit urged for consensus on a legislative framework for proof preservation and online privacy, as well as agreements on worldwide record sharing[lxx].

5. Direct cybercrime and online fraud prevention methods

International direct anti-cybercrime and online fraud initiatives are divided into two categories: cybercrime prevention and cybercrime investigation. They were more advantageous before the possibility of worldwide legal standardization. Individual projects with diverse focuses have been implemented by various groups. Interpol, for example, has worked closely with card issuers to combat payment fraud. In the OECD's Guidelines for Consumer Safety in the Context of Electronic Commerce 1999[lxxi], consumer protection was emphasized for both traditional and e-commerce. The 2002 Recommendations for the Security of Systems and Networks recommended member nations to "raise the importance of security development and readiness," in addition to "encourage a security culture amongst participants as a method of preserving networks and systems."

REMEDIES

A. General Retail Disputes in Online Auctions

The second most prevalent type of Internet fraud is Internet auction scam[lxxii]. This scam is not restricted to one type of sale and affects the great majority of auction platforms. Internet auction fraud can take many different forms, however it is often divided into two groups. For instance, some sellers misrepresent their products, resulting in an unhappy consumer obtaining counterfeit goods or goods that are significantly different from the items he sought.

Second, some vendors accept merely money and never provide items. Online auction fraud accounts for around 10% of all Internet fraud.[lxxiii]

B. General Retail Disputes Other Than Auction

Non-auction general merchandise claims, like bidding grievances, may be the consequence of malfeasance or an honest error. These charges are often identical to auctioned concerns wherein the purchasers never get items or obtain counterfeit stuff instead of authentic merchandise. Non-auction fraud, as opposed to auction fraud, might take the shape of pricey services or an inaccurate or imaginary delivery schedule.[lxxiv]

1. **Distinctive Websites**

Clients have voiced reservations about doing business with "unfamiliar e-commerce."

Indeed, 67% of consumers "are not confident undertaking business with an organization that can only be accessible on the internet," according to a national Technology Readiness study.[lxxv]

Despite these drawbacks, some websites continue to lure users by providing things or services at absurdly low prices.

2**. Recognized Websites**

When a customer purchases an item from a national or regional chain of department stores online and the merchant overspends the client or fails to provide the item, it may look to be a case of fraud. If these suppliers participate in fraudulent or misleading practices, they risk losing customers and earnings. When establishing whether a well-known website is fraudulent, the legal components of deceit must be considered, most notably the considerations of "likely to mislead" and "regarding a key fact." Consumers are inherently skeptical of organizations that can only be accessed over the internet since these businesses can close their webpages at any point or fail to react to public concerns." These activities do not qualify as deceit or fraud since merchants don't really intend to mislead or dupe their consumers.[lxxvi]

3. **Expired emails**

As a result of "spamming,"[lxxvii] many consumers receive a high number of emails from unknown writers in their inboxes every day.

When a seller of an item or service sends a blanket email to a large number of email addresses, this is referred to as spamming. The majority of these mails are sent by "sellers" who swindle consumers.[lxxviii]

Suggestions

1. **Double check:** Cyberlaw cases are distinctive and honourable, according to Advocate Satish Mishra, Practicing, Advocate, Chandigarh, who was interviewed by the writers. The majority of individuals are unaware of phone trickery. They lose money because they are so gullible. According to his observations, in order to commit online fraud, a person must be from another state, and the fight to recover the money is a protracted one. He advised internet users to double-check each and every transaction they carry out, without exception.
2. **Privacy should be the first priority of the people:** Since privacy is now more important than ever, it should be encouraged. First, use secure passwords or passphrases for all of your accounts.[lxxix] Passphrases, which are longer than passwords, must to be robust and particular to each website. It may become sophisticated and impossible to hack by adding some randomization and unique characters. A user is only permitted access to a website or application after successfully submitting two or more pieces of evidence to an authentication system, including knowledge, ownership, and inherence. The second step is to enable multi-factor authentication. Additionally, it may protect a person's privacy. Lastly, it can stop hackers from accessing data on any device by downloading the most recent security updates.
3. **Acquiring an antivirus software:** Since keeping their customers safe is in their best interest, all internet service providers provide their customers a free subscription to antivirus software. One must contact their provider for installation instructions. Free memberships, it should be noted, could not be sufficient for small organisations that might want extra security.
4. **Stricter penalties:** The prosecution of those who engage in unlawful acts while using the internet should be one of the primary focuses of any cyber legislation. Significant efforts should be made in order to effectively prosecute these types of crimes, such as cyber abuse, frauds, disrupting every company's online workflow, and other criminal activities. As a result, the government should imply sizable and stricter penalties in order to discourage people from committing internet frauds.
5. **Steer clear of connections that aren't secure:** Giving in to the temptation to use the free WiFi at a restaurant, hotel lobby, or airport might put a person at risk for financial theft. When performing a financial transaction, consumers should avoid utilising public hotspots wherever possible. As a result of the ease with which their encryption may be broken, public networks are more likely to experience data theft than private ones. This is because essential account information can be accessed over public networks.
6. **Accurate location of businesses:** while making an online transaction to a business, check the accuracy of business addresses by doing a search for the place on an online map and seeing it using the street-level view. A large number of fraudulent websites will employ false addresses, which are simple to identify when paying them a visit virtually.
7. **Awareness is the key:** Before revealing their sensitive information online, internet users should be provided many warnings and recommendations. Furthermore, if this information is communicated to the commons in the clearest and most understandable manner possible, providing warnings alone would not be sufficient. One of the main issues our society is presently facing is understanding these warnings, and because our culture's low literacy rate makes this issue much worse, a system that is intelligently

designed and simple to understand must be created to spread the word about prevalent online scams.

8. **Greater productivity and efficacy** in computer crimes detection, prosecution, and resolution, particularly online child exploitation of children, within one strong human-rights foundation.
9. **Protracted through the entire response to cyberattacks** that is efficient and successful, encompassing nationwide coordination, extracting information, and strong statutory provisions, resulting in changes in the system and increased deterrent[lxxx].
10. **Improved international and national interaction** among administration, police departments, and the corporate sector, as well as improved education and awareness of cybercrime threats.

Conclusion

Globalization does not mean worldwide prosperity. Globalised information networks are accommodating an increasing number of international crimes. Because of the network environment in which cybercrime operates, it is one of the most international offences of the current and among the most modernised hazards of the future. To solve this dilemma, we have two options. There should be no such expectations to be kept from any internationally recognized organization since their emphasis and interests are not fully focused on the matter of crime, especially cybercrime. While these institutions are preoccupied with more pressing international concerns, threats to vital IT will become ultimately more catastrophic unless addressed at the peak of these institutions' agendas. This method is unlikely to penalise offences committed in information systems. Instead, they are penalised by the countries whose territory they pass through. The construction of a multilateral organizations framework for punishing cybercrime is growing more severe and vital. Several international organisations have made efforts to address the issue at various settings and levels. In a study conducted by the authors in 2021, 62.8% of individuals recognised their rights under the law and the rules that applied to them, yet a significant proportion of individuals, 37.2%, are ignorant of scams and the laws that apply to them. As a result, it is vital to educate people about internet scams and provide prevention tips. When the researchers filed an RTI for data on internet fraud in India affecting several states on 17/06/2021, the following response was given: This is in response to your request, which was recorded under Registration number NICHQ/R/E/21/00256. This office has dealt with your request. Action date: 21/06/2021 The following is my response to your RTI inquiry:

There is no evidence on the record. Under the RTI Act, 2005, only information that is available, existing, and held by the public authority or under its supervision may be provided.

The PIO is not permitted to produce information that is not part of the record.

Without a physical location, information management becomes such a one-of-a-kind dominion.

Finally, the Reserve Bank of India stipulates in a separate rule on the storage of payment processing data that payments data must only be kept in India. While the directive's primary purpose is to grant the RBI accessibility to any and all payment data so it can supervise transactions, it will almost certainly make it easier for law enforcement to discover and sanction payment system administrators who fail to take adequate security steps. Spam generated by technology Spammers attempt to exploit the reality that numerous individuals lack computer competence. Don't fall for commercials for software or hardware, internet or cellular technology, or various devices.

The authorities should play an important role, but individuals' privacy shouldn't be jeopardized in the process of reducing fraudulent activity. As a consequence, the establishment of a global level of awareness and the desire for the development of an international degree of consciousness are still the foundations for effective operations. The present international legal frameworks must be evaluated and, if necessary, revised, while also creating a forum for larger international debate with the goal of improving and enhancing international law-enforcement cooperation among federal governments. In order to prevent a futureless future of information chaos, this evolution should take into consideration the implications of new and developing challenges in existing international cooperation, with capacity-building proposals that showcase equal level of concerned circumstances in nations at varying stages of development.

References :

1. [i]*Ticket swindle leaves trail of losers*. (2008, August 4). The Sydney Morning Herald. Retrieved December 14, 2022, from https://www.smh.com.au/national/ticket-swindle-leaves-trail-of-losers-20080804-gdsoyj.html
2. [ii]*Online scams: An overview + 20 internet scams to avoid in 2023*. (n.d.). Online Scams: Avoiding Internet Scams in 2023 - Norton. Retrieved December 14, 2022, from https://us.norton.com/blog/emerging-threats/internet-scams
3. [iii] Brenner, S. W. (2009, January 16). Cyberthreats. In *The Emerging Fault Lines of the Nation State*.
4. [iv]*What Is Internet Fraud? The Defenses? The Punishment? :: Redondo Beach, California Internet Fraud Lawyers Greg Hill & Associates*. (n.d.). What Is Internet Fraud? The Defenses? The Punishment? :: Redondo Beach, California Internet Fraud Lawyers Greg Hill & Associates. Retrieved December 14, 2022, from https://www.greghillassociates.com/what-is-internet-fraud-the-defenses-the-punishment.html
5. [v]*What Is Internet Fraud? Types of Internet Fraud | Fortinet*. (n.d.). Fortinet. Retrieved December 14, 2022, from https:///resources/cyberglossary/internet-fraud
6. [vi]*Internet and Social Media Fraud | Investor.gov*. (n.d.). Internet and Social Media Fraud | Investor.gov. Retrieved December 14, 2022, from https://www.investor.gov/protect-your-investments/fraud/types-fraud/internet-and-social-media-fraud
7. [vii]*White Collar Crime - Non-violent Crimes - Embezzlement - Impact Law*. (n.d.). White Collar Crime - Non-violent Crimes - Embezzlement - Impact Law. Retrieved December 14, 2022, from https://www.impactlaw.com/criminal-law/white-collar
8. [viii] Wright, A., Aaron, S., & Bates, D. W. (2016, May 13). The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *Journal of General Internal Medicine*, *31*(10), 1115–1118. https://doi.org/10.1007/s11606-016-3741-z
9. [ix]*Online Consumer Complaints Forum | IamCheated.com*. (1950, January 1). Online Consumer Complaints Forum | IamCheated.com. Retrieved December 14, 2022, from https://iamcheated.indianmoney.com/
10. [x]*What Is a Phishing Attack? Definition and Types*. (n.d.). Cisco. Retrieved December 14, 2022, from https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html
11. [xi]*What is phishing | Attack techniques & scam examples | Imperva*. Learning Center. Retrieved December 14, 2022, from https://www.imperva.com/learn/application-security/phishing-attack-scam/
12. [xii] Fruhlinger, J. *What is phishing? Examples, types, and techniques*. CSO Online. Retrieved December 14, 2022, from https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html
13. [xiii] Jha, M., C S, A., Mahawar, Y., Kalyan, U., & Verma, V. (2021, December). Cyber Security: Terms, Laws, Threats and Protection. *2021 International Conference on Computing Sciences (ICCS)*. https://doi.org/10.1109/iccs54944.2021.00037

14. [xiv] Ollmann. (2007). The Phishing Guide Understanding & Preventing Phishing Attacks. https://docplayer.net/7691290-The-phishing-guide-understanding-preventing-phishing-attacks-by-gunter-ollmann-director-of-security-strategy-ibm-internet-security-systems.html
15. [xv]*Verizon 2019 Data Breach Investigations Report*. Retrieved December 14, 2022, from https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf
16. [xvi]*What Are the Different Types of Phishing?* (n.d.). Trend Micro. Retrieved December 14, 2022, from https://www.trendmicro.com/en_in/what-is/phishing/types-of-phishing.html
17. [xvii]*Content Spoofing | OWASP Foundation*. (n.d.). Content Spoofing | OWASP Foundation. Retrieved December 14, 2022, from https://owasp.org/www-community/attacks/Content_Spoofing
18. [xviii] K. *Phishing | Phishing Techniques*. Phishing | Phishing Techniques. Retrieved December 14, 2022, from https://www.phishing.org/phishing-techniques
19. [xix] Fraudwatch, A. (2021, March 24). *Expert Explanation: What is Mobile Phishing & Why is it on The Rise? - Digital Brand Protection – FraudWatch*. Digital Brand Protection – FraudWatch. Retrieved December 14, 2022, from https://fraudwatch.com/expert-explanation-what-is-mobile-phishing-why-is-it-on-the-rise/
20. [xx] ACM Digital Library. Retrieved December 14, 2022, from https://www.acm.org/publications/digital-library
21. [xxi]*How to Recognize and Avoid Phishing Scams*. (2019, May 3). Consumer Advice. Retrieved December 14, 2022, from https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
22. [xxii] Information Technology Act, 2000, Section 43
23. [xxiii] Information Technology Act 2000, Section 66C
24. [xxiv] Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules, 2011
25. [xxv]*Storage of Payment System Data*. Reserve Bank of India - Notifications. Retrieved December 14, 2022, from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244
26. [xxvi] Convention of the Council of Europe on Cybercrime
27. [xxvii]*World Cup, Vacation Scams Lead in Phishing Trips this Summer*. (2018, June 6). World Cup, Vacation Scams Lead in Phishing Trips This Summer | Threatpost. Retrieved December 14, 2022, from https://threatpost.com/world-cup-vacation-scams-lead-in-phishing-trips-this-summer/132543/
28. [xxviii]*Update your software now*. (2019, June 13). Consumer Advice. Retrieved December 14, 2022, from https://consumer.ftc.gov/consumer-alerts/2019/06/update-your-software-now
29. [xxix]*RBI cautions Public Once Again against Fictitious Offers*. (n.d.). Reserve Bank of India. Retrieved December 14, 2022, from https://www.rbi.org.in/commonman/English/Scripts/PressReleases.aspx?Id=2440#:~:text=The%20Reserve%20Bank%20has%20urged,the%20Reserve%20Bank%20of%20India.&text=RBI%20does%20not%20hold%20any%20accounts%20for%20individuals.&text=RBI%20does%20not%20send%20any,award%20of%20lottery%20funds%2C%20etc
30. [xxx] Internet fraud - Australian Capital Territory Policing, Retrieved December 14, 2022, from https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf
31. [xxxi]*Definition of SPAM*. (2022, December 13). Spam Definition & Meaning - Merriam-Webster. Retrieved December 14, 2022, from https://www.merriam-webster.com/dictionary/spam
32. [xxxii]*ClickZ: Make Spammers Pay Before You Do*. (2002, July 26). Retrieved December 14, 2022, from https://web.archive.org/web/20070807113021/http://www.clickz.com/showPage.html?page=1432751
33. [xxxiii]*archive.ph*. (n.d.). archive.ph. Retrieved December 14, 2022, from https://archive.ph/20130414114546/http://www.cluelessmailers.org/articles/2008-01-19-gettingitwrong.html
34. [xxxiv] Fumera, Pillai, & Roli. Spam filtering based on the analysis of text information embedded into images. *ACM Digital Library*. https://dl.acm.org/doi/10.5555/1248547.1248645
35. [xxxv] staff, C. (2009, September 2). *Dealing with blank spam*. CNET. Retrieved December 14, 2022, from https://www.cnet.com/tech/computing/dealing-with-blank-spam/
36. [xxxvi]*Risk Detected*. Symantec Security Center, Broadcom Inc. Retrieved December 14, 2022, from https://www.broadcom.com/support/security-center/detected-writeup?docid=2001-020713-3220-99

37. [xxxvii]*Delhi HC raps firm over spam mail*. rediff.com. Retrieved December 14, 2022, from https://www.rediff.com/money/2004/jan/13spam.htm
38. [xxxviii] Information Technology (Amendment) Act, 2008, Section 66A.
39. [xxxix] Shreya Singhal v. Union of India, AIR 2015 SC 1523
40. [xl] *Drahos, P. (Ed.).* (2017). *Regulatory Theory: Foundations and applications*. ANU Press. Retrieved December 14, 2022 http://www.jstor.org/stable/j.ctt1q1crtm
41. [xli] India, L. S. *Spam: Is it time to legislate - Internet law in India*. Spam: Is It Time to Legislate - Internet Law in India. Retrieved December 14, 2022, from http://www.legalservicesindia.com/articles/spamli.htm
42. [xlii]*Austria, Italy Outlaw Spam - ClickZ.* (1999, July 23). ClickZ. Retrieved December 14, 2022, from https://www.clickz.com/austria-italy-outlaw-spam/85373/
43. [xliii] Tate, R. (2011, October 27). *The Seedy, Spammy Past of Airbnb's Co-Founder*. Gawker. Retrieved December 14, 2022, from https://www.gawker.com/5853754/the-seedy-spammy-past-of-airbnbs-co-founder
44. [xliv] Nast, C., & W. (2010, April 12). *April 12, 1994: Immigration Lawyers Invent Commercial Spam*. WIRED. Retrieved December 14, 2022, from https://www.wired.com/2010/04/0412canter-siegel-usenet-spam/
45. [xlv] Legal Newsline. *Tagged.com gets slapped by San Francisco DA*. (2022, December 14). Retrieved December 14, 2022, from https://legalnewsline.com/
46. [xlvi] Credeur. *EarthLink wins $25 million lawsuit against junk e-mailer*. Atlanta Business Chronicle. Retrieved December 14, 2022, from https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html
47. [xlvii] P. *PwC Global Economic Crime and Fraud Survey 2022*. PwC. Retrieved December 14, 2022, from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
48. [xlviii] Reynolds, J. (2020, November 12). *9 reasons digital fraud is on the rise*| 2020-11-12 | Security Magazine. Retrieved December 14, 2022, from https://www.securitymagazine.com/articles/93912-reasons-digital-fraud-is-on-the-rise
49. [xlix]Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales. (2021, May 3). UNCTAD. Retrieved December 17, 2022, from https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales
50. [l]P. (n.d.). *Payments 2025 & beyond*. PwC. Retrieved December 17, 2022, from https://www.pwc.com/gx/en/industries/financial-services/publications/financial-services-in-2025/payments-in-2025.html
51. [li]*How Data Breaches Happen. (2021, August 23). www.kaspersky.com. Retrieved December 17, 2022, from https://www.kaspersky.com/resource-center/definitions/data-breach*
52. [lii]*Online Payment Fraud*. (2022, July 1). Online Payment Fraud Market Report 2022-27: Size, Share, Trends. Retrieved December 17, 2022, from https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report
53. [liii]ITU. (n.d.). ITU. Retrieved December 17, 2022, from https://www.itu.int/en/about/Pages/default.aspx
54. [liv] European Council. (2022, December 15). European Council - Consilium. Retrieved December 17, 2022, from https://www.consilium.europa.eu/en/european-council/
55. [lv]INTERPOL | The International Criminal Police Organization. (n.d.). INTERPOL | the International Criminal Police Organization. Retrieved December 17, 2022, from https://www.interpol.int/en
56. [lvi] United Nations Office on Drugs and Crime. (2022, September 12). United Nations : Office on Drugs and Crime. Retrieved December 17, 2022, from https:////www.unodc.org/unodc/en/index.html
57. [lvii]*APWG | Unifying The Global Response To Cybercrime*. (2022, October 28). APWG | Unifying the Global Response to Cybercrime. Retrieved December 17, 2022, from https://apwg.org/
58. [lviii] Project Webteam, T. S. (n.d.). *The Spamhaus Project*. The Spamhaus Project. Retrieved December 17, 2022, from https://www.spamhaus.org/
59. [lix]*INHOPE | Home*. (n.d.). INHOPE | Home. Retrieved December 17, 2022, from https://www.inhope.org/EN
60. [lx]*eNACSO - The European NGO Alliance for Child Safety Online*. (2011, October 18). European Economic and Social Committee. Retrieved December 17, 2022, from https://www.eesc.europa.eu/en/documents/enacso-european-ngo-alliance-child-safety-online

61. [lxi]*The Internet Watch Foundation - Eliminating Child Sexual Abuse Online*. (n.d.). Eliminating Child Sexual Abuse Online – Internet Watch Foundation. Retrieved December 17, 2022, from https://www.iwf.org.uk/
62. [lxii]*RAND Corporation Provides Objective Research Services and Public Policy Analysis*. (n.d.). RAND Corporation Provides Objective Research Services and Public Policy Analysis | RAND. Retrieved December 17, 2022, from https://www.rand.org
63. [lxiii]*What is Cybercrime? Different Types and Prevention*. (2021, July 2). Intellipaat Blog. Retrieved December 14, 2022, from https://intellipaat.com/blog/what-is-cybercrime/
64. [lxiv]*Cybersecurity Is Critical for all Organizations – Large and Small*. (2019, November 4). IFAC. Retrieved December 17, 2022, from https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small
65. [lxv] K. M. (n.d.). Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations. Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations. Retrieved December 17, 2022, from https:////www.unodc.org
66. [lxvi]*The United Nations*. (n.d.). Un. Retrieved December 17, 2022, from https://www.cybercrimelaw.net/un.html
67. [lxvii] Asia-Pacific Economic Cooperation. (2022, November 17). APEC. Retrieved December 17, 2022, from http://www.apec.org
68. [lxviii] Financial and cybercrimes top global police concerns, says new INTERPOL report. (2022, October 19). Financial and Cybercrimes Top Global Police Concerns, Says New INTERPOL Report. Retrieved December 17, 2022, from https://www.interpol.int/en/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report
69. [lxix]*A Critical Look at the Regulation of Cybercrime*. (n.d.). Retrieved December 17, 2022, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi6-J7414D8AhVfT2wGHV9gA7IQFnoECA4QAQ&url=https%3A%2F%2Fwww.crime-research.org%2Flibrary%2FCritical.doc&usg=AOvVaw1HqfRS99uTMSrJG0iXMdUT
70. [lxx]*Cyberlaw on cyber law and investment*. (n.d.). Retrieved December 17, 2022, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiyksqv2ID8AhXWS2wGHewSDJgQFnoECAsQAQ&url=https%3A%2F%2Fzenodo.org%2Frecord%2F7325613&usg=AOvVaw1cvaCJMP83XU1yH51ySCGk
71. [lxxi]OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) - OECD. (n.d.). OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) - OECD. Retrieved December 17, 2022, from https://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm#:~:text=The%20Guidelines%20for%20Consumer%20Protection,or%20order%20from%20a%20catalogue.
72. [lxxii]*Auction Fraud*. (n.d.). New York Criminal Attorney: NY Criminal Defense - Bukh Law Firm. Retrieved December 17, 2022, from https://nyccriminallawyer.com/fraud-charge/auction-fraud/
73. [lxxiii] Watch Out for These Top Internet Scams. (2022, June 11). Investopedia. Retrieved December 17, 2022, from https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp
74. [lxxiv]*5 types of fraud that is used to target e-commerce retailers*. (n.d.). Ravelin. Retrieved December 17, 2022, from https://www.ravelin.com/blog/5-types-of-fraud-that-is-used-to-target-e-commerce-retailers
75. [lxxv] Thompson. (1999). *The Challenges of Law in Cyberspace - Fostering the Safety and Growth of E-Commerce*.
76. [lxxvi]Nohe, P. (2018, November 2). *5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam in 2018*. Hashed Out by the SSL Store™. Retrieved December 17, 2022, from https://www.thesslstore.com/blog/5-ways-to-determine-if-a-website-is-fake-fraudulent-or-a-scam/
77. [lxxvii] What Is Spam: The Essential Guide to Detecting and Preventing Spam. (2022, November 11). What Is Spam? Types of Spam & How to Stay Protected | Avast. Retrieved December 17, 2022, from https://www.avast.com/c-spam

78. [lxxviii] Weisse. (2002). *Remedies for Internet Fraud: Consumers Need All the Help They Can Get*. Loyola Consumer Law Review. Retrieved December 14, 2022, from https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1318&context=lclr
79. [lxxix] Internet Safety: Creating Strong Passwords. (n.d.). GCFGlobal.org. Retrieved December 17, 2022, from https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/
80. [lxxx]*Global Programme on Cybercrime. (n.d.). Retrieved December 17, 2022, from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html*