Library Progress International *Print version ISSN 0970 1052*
Vol.43, No.2, Jul-Dec 2023: P.547-555 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Criminal Analysis of Phishing in Iran's Legal System

[1]Amir Mohammad Vasheghani Farahani*

[1]Ph.D. Candidate in Criminal Law and Criminology, Islamic Azad University, Shahre Qods Branch, Iran.

How to cite this article: Amir Mohammad Vasheghani Farahani (2023). Criminal Analysis of Phishing in Iran's Legal System. *Library Progress International,* 43(2), 547-555

ABSTRACT

Phishing is a cyberscam progressively committed by hackers in social media to fraudulently deceive victims into revealing their sensitive information. The hackers involved in phishing are called phishers, as they emulate fishing by alluring users and waiting for them to be betrayed for revealing their data intended in cyberattacks. Overall, phishing manifests into sending fake links via text messages under the title of judicial notifications, stock dividends, fake bank payment portals, and fake emails, among others. By these means, the phisher betrays the user to unwittingly reveal their critical data such as credit card information, passwords, and so forth, thereby pocketing from the victim's account. Importantly, phishing is not specifically criminalized in Iran's criminal laws. The Iranian criminal system protects the rights of both victims and society based on the phisher's action(s) and follows the Law of Computer Crimes to punish the phisher for being accused of illegal access, computer fraud, and computer theft. The measures taken so far to fight phishing include enhancing public awareness and compelling the user to use one-time passwords (PINs). However, this crime can be stringently prohibited by taking further actions such as criminalizing phishing as a defined crime deserving deterrent penalties, hiring cyberspace experts to propose solutions for diminishing cybercrimes (particularly phishing), strict control by the Iranian Cyber Police (FATA), preventive measures to protect vulnerable users, and so forth.

KEYWORDS

Phishing, Computer crimes, Cybercrimes.

Introduction

Technology has constantly played a vital role and noticeably impacted all the dimensions of human life. Upon technological breakthroughs, particularly the Internet, which has fostered borderless communication between individuals, crimes are developed tailored to the prevailing circumstances, a portion of which targets cyberspace worldwide. Phishing is a cybercrime that has been increasingly committed in past years and is currently occurring in the form of unprecedented criminal events. Phishing was earlier committed by sending emails to the user to fraudulently betray them for revealing their confidential information. Nonetheless, cyberspace evolution has propelled phishers (as offenders) to adopt unexplored techniques for deceiving users, such as delivering fake payment portals, sending fake links via text messages, and so forth. The high frequency of such crimes has mandated government officials to regularly send text messages to citizens to provide them with suppressive measures to avoid phishing.

Phishers are best characterized by their high intelligence and patience, with the former serving as the basis for committing computer offenses. Indeed, phishers bait the users and patiently wait for them to be deceived. After that, the phishers cyberattack the victim by accessing their account and stealing the intended crucial data. The present descriptive-analytical research explores the methods of phishing perpetration, legal judgments, criminal proceedings against this crime, suppressive measures to avoid phishing, and penalties for offenders. Specifically, this research aims to respond to the following questions:

1. How phishing is committed in Iran?
2. What is Iran's criminal policy toward phishing?
3. How to contest phishing?

The research goals are to criminally analyze phishing, explore the ways of phishing perpetration in Iran, determine the Iranian laws and regulations and criminal proceedings and judicial procedures against phishing, and propose solutions to avoid this scam.

The remainder of this research is organized as follows. Section 1 describes the concept of phishing, with paragraphs A and B respectively dealing with the lexical and idiomatic concepts of phishing, and paragraph C is dedicated to scrutinizing

similar crimes. This section, in turn, aims to define the concept of phishing and prepare the readers to perceive the following topics. Section 2 assesses phishing in Iran, with paragraph A explaining the ways of committing phishing and paragraph B outlining the Iranian rules towards this offense. This section aims to inform the reader about the ways of phishing perpetration and the Iranian legal approaches to avoid this cybercrime. Section 3 investigates the ways of combating phishing, which is critical after knowing how this crime is committed. Section 4 describes methods of dealing with phishing, with paragraph A determining inherent and territorial jurisdiction in enforcing the laws, and paragraph B describing the manner of criminal proceedings. In turn, this section scrutinizes criminal proceedings after discussing all the aspects of phishing. Ultimately, Section 5 has an academic background and is dedicated to the criminal analysis of phishing, covering aspects of victimology, crime prevention, and criminal sociology.

The concept of phishing

For phishing to be better perceived, its lexical and terminological concepts are first defined, aiming to allow readers to consider research topics.

2.1. The lexical concept of phishing

The term phishing refers to the act of fishing (Bateni et al., 2013: 248) and was first coined by cyber attackers or hackers who are called phishers in the crime of phishing. Precisely, the term phishing refers to “password harvesting fishing”, which implies access to passwords via baiting. The term phishing was initially written as “fishing’, but was then altered to “phishing” by phishers. The reason for adopting this term from fishing lies in the shared features. Firstly, both highlight patience as a key prerequisite to attaining the targets and intentions. Secondly, both adopt a similar way of hunting which is setting some baits for the targets (i.e., fish for a fisherman and victim for a phisher). And thirdly, both attack vast targets which are a group of fish or multiple individuals to be drawn. Simply put, a fisherman targets all the fish in the lake, yet expects some fish to be accidentally trapped in a net or hook. The same applies to phishing, where phishers target numerous individuals while perceptively expecting only some to be hunted in the cyberattacks.

2.2. The terminological concept of phishing

Phishing is terminologically a cybercrime where hackers or phishers aim to fraudulently reach and then abuse the sensitive information of the deceived victim. Phishing is, in turn, a cybercrime mostly committed by sending a fake link via messages, particularly via email. When the user enters the fake website via the link, the phisher can easily access the intended information. This is the first step by phishers, as they subsequently use such sensitive data (e.g., credit and bank card information, passwords, card security codes, etc.) to illegally withdraw money from the victim's account. Phishing is frequently committed by altering the URL link (e.g., Adliraan.com instead of Adliran.ir), falsifying the main website (e.g., falsifying the bank's payment portals), and devising a fake application (e.g., some malware under the titles of SANA system, charging and internet, notification systems, and so on). Nonetheless, the era of phishing will be hastened over time along with progress in cyberspace, as smart phishers will perform more complicated cyberattacks shortly.

2.3. Similar crimes

Based on the crime type, the way of its perpetration, the way of victimizing, and the tools and equipment used to perform it (particularly computer and Internet crimes), some crimes are similar to phishing, which are listed in the following sections.

2.3.1. Computer Theft

The term theft refers to stealing the property of others (Article 267 of the Islamic Penal Code - IPC), which manifests into diverse types such as computer theft. Conceptually, computer theft is roughly similar to classic theft in which a person will be accused of stealing data belonging to others, regardless of whether the data remains in the hands of the owner or not (Article 740 of the IPC, and Article 12 of the Law of Computer Crimes - LCC). Thus, the act of a person copying data belonging to another person is further labeled as computer theft. By comparison, classic theft refers to kidnapping, taking, captivating, and any other similar actions toward the property of someone else without the consent and knowledge of the owner or occupier (Goldoozian, 2020 A: 411). Contrarily, computer theft is committed through a computer and by stealing the data belonging to others. When a computer file is cut or deleted by the offender and they save the stolen file for themselves, this action will be labeled as computer theft, even though deleting data is itself a crime in Article 736 of the LCC (Babaei, 2021: 128).

2.3.2. Computer fraud

Fraud is classically defined as the acquisition of the property of others fraudulently (Article 1 of the Law of Intensifying Punishments of the Perpetrators of Bribery, Embezzlement, and Fraud), manifesting into diverse scams such as computer fraud. The person is committed to computer fraud when they illegally use computer or telecommunication systems and perform acts like entering the computer, altering, erasing, creating, or stopping data, and/or disrupting the system to take money, property, interests, services, or financial items for themselves or others (Article 740 of the IPC, and Article 13 of the LCC). After the LCC approval, any fraudulent attack on computer data will no longer deemed as a simple fraud and, instead, will be labeled as a computer fraud (Mir Mohammad Sadeghi and Shayegan, 2010: 138). The act of a person taking their property will not be a fraud (Goldoozian, 2021: 560). Likewise, a mere claim for money is not fraudulent (Mir Mohammad Sadeghi, 2024: 82). In computer fraud, acquiring interests, services, and items for the offender or someone else is fraud, besides acquiring other's property.

2.3.3. Pharming

Pharming is an advanced type of phishing that aims to deceive the victim into visiting a fake site by confusing them via altering the correct IP address. The most notable pharming crime is when the offender (called pharmer) creates a fake bank payment portal and deludes the victim into delivering their sensitive data. As the fake portal resembles the true bank payment portal, the victim is tricked and thus enters their critical account data such as card number, card verification value 2 (CVV2), card expiration date, and most critically, the card PIN or one-time password (OTP), thereby allowing the pharmer to empty the victim's bank account. That is why the Iranian legal system mandates the users to work only with their OPTs.

2.3.4. Wangiri

Wangiri is similar to phishing, but they slightly differ regarding crime perpetration strategy. Overall, both these scams share three similar aspects:

Firstly, both emphasize the patience of the offenders and target bulks of users to make some thoughtless and reckless users their victims. Secondly, both target the users mentally and psychologically, disposing them toward criminal traps as a result of fear, greed, curiosity, witlessness, and other causes. Thirdly, both scams initiatively draw the attention of users to victimize them. In Wangiri, the offender makes a "one-and-cut" premium call in which the call is cut off after one ring. The target user will, thereby, have a missed call on their phone, and curiously phone the number back. Since the calls are from international premium numbers, as soon as the user is connected, they start paying heavy costs for that premium call dialed. Importantly, the fraudsters hang up after just one ring, and the time the user dials back the unknown number, the process of victimizing the user begins. Upon connection, a recorded message starts playing, thereby imposing heavy phone bills on the victim. The Wangari calls targeting Iranian users come mostly from African and Southeast Asian countries. Next, any call from Iran will be costly for the Telecommunication Company of Iran (TCI), where the TCI shall pay the calling bill to the destination country. For compensation, the TCI will issue a heavy phone bill to the victim of the missed call.

Phishing in Iran

After perceiving the concepts of phishing, this section describes the relevant scams committed in Iran and the associated laws governing such crimes. As such, diverse ways phishers adopt to perform phishing scams are discussed first. Next, the Iranian laws and procedures dealing with this scam are described.

3.1. Phishing perpetration

As stated earlier and arriving from its name, phishing is similar to fishing. As such, the phishers patiently target a large population of victims at first. Then, they follow defined steps to trick victims (even if they are handful in number) by creating baits and waiting for them to be hunted. Presently, phishers are more interested in scam actions such as sending fake links via text messages under the titles of legal complaints, stock dividends, lottery, calls arriving with the Islamic Republic of Iranian Broadcasting (IRIB) logos, software installation, creating a fake payment portal, counterfeit point-of-sale (POS) equipment, and similar actions. Notably, scams regarding fake payment portals are further known as pharming, as was described earlier.

Regarding constant technological breakthroughs and the dynamics of phishing crimes that are committed tailored to the latest social settings, such scams are almost certainly to be performed in the future through engaging tricks. Likewise, the phishers are principally intelligent and those involved in cybercrimes are claimed to be even smarter than those interested in other crimes (Bahremand, 2016: 60). These phishers, in turn, walk parallel to the latest events and utilize novel techniques and innovative ways to commit crimes on their targeted victims. Importantly, phishing stands against theft, regarding the perpetrator's characteristics. As such, while phishers are more dependent on their intelligence, thieves need

to be physically prepared to (for example) run away and rapidly carry out abduction when necessary. For example, elderly, injured individuals, and those with disabilities fail to commit theft, while easily attending phishing scams with no physical strength required and simply by having intelligence and computer skills.

3.2. Iranian laws on phishing

The Iranian legal system has not precisely defined laws and rules regarding phishing scams. Nonetheless, phishing frauds are dealt with in the courts following the Iranian LCCs under judicial procedures. Based on the deterrence of criminal offending (Principle 36 of the IPC) that makes punishments conditional to governing laws, the phishers shall be penalized legally. There exist three articles in the Iranian LCC defined to punish phishers:

A) Article 1 of the LCC applies to phishing initiation which is any unauthorized access to data or computer or telecommunication systems that are securely protected. As such, the person committing this action will be penalized for one or both "91 days to one year in prison" and "paying 50 million IR Rials". Thus, this article applies to those phishers who gain access to protected data and systems but do not acquire money.

B) Article 12 of the LCC applies to computer theft. That is, when the phisher steals other data, they will be penalized for computer theft. Based on this article, if the data is owned by the owner and the phisher gains a copy of the data, the legal system will penalize the phisher for 6 to 50 million IR Rials. Otherwise, when the data are not owned by the owner and (i.e.,) the phisher cuts the intended data, the legal system will penalize the phisher for one or both "91 days to one year in prison" and/or "paying 20 to 80 million IR Rials".

C) Article 13 of the LCC that criminalizes fraud. Accordingly, when the phisher illegally enters, alters, deletes, creates, or halts data, and/or disrupts the system to ultimately steal money, properties, interest, services, or privileges belonging to other persons for themselves or someone else (e.g., by creating a fake bank payment portal), the legal system will penalize the phisher for one or both "1 to 5 years in prison" and/or "paying 50 to 250 million IR Rials".

However, the above articles need to be reflected regarding some points:

First, the legislator shall consider the dynamics and dimensions of phishing to criminalize it and define tailored punishments for each phishing scam. By this, all the phishing aspects will be accurately and integratedly covered by the judicial authorities, thereby leaving no ambiguity behind.

Second, restitution has not so far been predicted in computer theft but has been foreseen to be penalized in fraud, as can be seen in Article 12 of the LCC.

Third, if the phisher fails to acquire property at any unauthorized access but can successfully destroy the data, they will be accused of computer destruction crime and penalized for one or both "6 months to 2 years in prison" and/or "paying 10 to 40 million IR Rials".

How to deal with phishing

A multitude of measures have so far been taken to deal with phishing. A sought-after measure is using OTPs, which was first decided collectively by the Iranian Central Bank, FATA Police, and the Attorney General's Office. Before enforcing OTPs, numerous individuals have been victims of fake bank payment portals. Furthermore, there were countless reports on phishing resulting in the significant loss of properties of the victims. Before OTPs, due to huge cases of phishing and a marked jump in the loss of victims' properties, the users attempted to avoid fraud by intentionally writing the wrong CVV2 codes. As such, if the payment portal was correct and legitimate, the users would get an error implying the wrong CVV2 number, otherwise (in cases of phishing trap) they could proceed without any problem, thereby knowing that the payment portal is counterfeit. Next, a versatile way to avoid phishing is to enhance public awareness. For example, they can be informed of not linking to sites without the https:// URL.

Importantly, the next potent way to decline phishing is to employ those ready-to-be-phisher talented persons in cyberspace settings or support them to furnish their abilities in legal areas. By these, the rate of phishing perpetration will be, although trivially, diminished. Since the phishers are creative in performing such scams and constantly work parallel to the dominant surroundings, legal systems, and the users must be proactive in fighting these offenses and predict the next step taken by the phisher. For example, a social media application that is popular in a country and holds a marked number of subscribers will pave the way for computer scams. Thus, such application needs to be strictly controlled by all the tools to avoid potential crimes.

Next, since computer crimes are often reported to be committed by young adults (Jalali Farahani, 2004: 103), an effective way is to inform criminals of this age group about the consequences of such delinquencies. When a talented youngster with potent technological skills become aware of penalties set for computer crimes, they will become cautious about performing such actions and may even no longer be involved in these events.

Most importantly, though such measures can measurably reduce the chance of committing these crimes, it is a daunting task and even unattainable to eradicate these scams. However, they can be largely prohibited by taking tailored procedures.

How to trial phishing

After the concept of phishing, its perpetration ways, and the Iranian laws and rules against this crime, the next critical step is to punish criminals tailored to their scams.

5.1. Criminal jurisdiction

Jurisdiction is the power of a court to judge crimes regarding inherent (i.e., exclusive authority) and territorial jurisdiction of the court, where inherent jurisdiction is under peremptory norms (Shams, 2018: 159) and territorial jurisdiction is under peremptory criminal matters. Regarding the dimensions of computer crimes and the boundless virtual space on social media that intensifies the chance of crime perpetration abroad, the concept of jurisdiction is paramount when aiming to trial phishing cases. This section discusses the scope of on-site law enforcement and the inherent and territorial jurisdiction of the courts.

5.1.1. The scope of on-site law enforcement

This section deals with the jurisdiction of Iranian criminal authorities to trial phishing crimes. In Iran, the courts can judge phishing crime cases under jurisdictional principles. Phishing is a computer scam, in which some illegal actions are made to automatically process or transfer intended data (Zobeyr, 2004: 18).

Articles 3 to 9 of the IPC have defined some relevant rules regarding jurisdiction. Furthermore, the Criminal Justice Act (CJA) in Article 664 of the IPC has defined the jurisdiction of Iranian courts regarding computer crimes. As such, when one of the clauses listed in the paragraphs of these articles applies to phishing, Iranian courts will be allowed to trial the relevant case. As with this article, the Iranian courts are allowed to judge phishing cases under the following conditions:

- When data utilized for phishing scams are stored in the territory of Iran;
- When the phishing scam occurs through a website with a ".ir: domain;
- When the crime is committed abroad but against the Iranian computer and telecommunication systems and websites which are controlled by the "Three Powers" of Iran (i.e., the executive, legislative, and judicial branches), the leadership body, the official government representative, or any institution that provides public services, or against websites with the ".ir" domain;
- And, when a computer crime is committed against individuals under 18 years and the phisher is living in Iran;

Notably, the domain is the last part of an address, including ".org", ".ir", and so forth (Rahimi and Rahimi Dehsuri, 2020: 518).

Besides this which is specific to computer crimes, phishing cases can further be trialed by other jurisdictions. The international law of criminal jurisdiction covers four principles (Khaleghi, 2023: 48), whereas the IPC covers six principles to distinguish active and passive personal jurisdiction from each other and to deal with the crimes committed by government staff. Nonetheless, this section merely describes the jurisdictions that apply to phishing scams. When the whole or part of a phishing crime occurs in the territory of Iran and/or its consequence(s) affect Iranian interests (i.e., the Iranian ships, planes, submarines, embassies, sky, water territories, etc.), the Iranian side will then have jurisdiction to trial the committed crime, according to the Territoriality Principle (TP) (Article 3 of the IPC). The TP applies to phishing where the phisher commits all the phishing steps in Iran. One example is sending a fake link via a short message to users living in Iran and then deceiving them to open the link, thereby gaining access to their data and emptying their accounts. The TP further applies to a phishing crime that part of it takes place in Iran. One example of this kind is when a phisher living abroad sends an e-mail to a user residing in Iran. Similarly, the TP further applies to a crime occurring abroad but its consequence(s) affect Iran and Iranian interests. For example, a phisher living abroad sends a link via e-mail to diverse Iranian users and upon accessing their account information, transfers money to an account in Iran.

The second principle of jurisdiction that allows Iranian courts to trial phishing crimes is Real Jurisdiction (RJ) (Article 5 of the IPC). In the principle of RJ, the phishing crime is committed outside Iran's sovereign territory to avoid being reprimanded by the Iranian TP. When a crime is committed abroad by Iranians or foreign nationals but threatens the Iranian supreme interests, it will be dealt with under the RJ principle (Goldoozian, 2020-b: 200). Regarding the principle of RJ, the Iranian courts hold the jurisdiction to trial phishing crimes only under Paragraph A of Article 5 of the IPC. As with this paragraph, when phishers abroad commit phishing to target Iranian domestic and international security and direction, the Iranian courts will have jurisdiction to judge the issue under the RJ principle.

The third principle regarding phishing crime trials is the principle of active personal jurisdiction (APJ) (Article 7 of the IPC). According to the APJ principle, when a phisher is an Iranian national and commits phishing outside the territory of Iran, the Iranian courts are allowed to judge such crimes only when the phisher is recognized and arrested in Iran.

The fourth and final principle of jurisdiction regarding phishing crimes is the principle of passive personal jurisdiction (PPJ). The PPJ principle is about Iranian victims outside the territory of Iran. According to this principle, the Iranian courts are allowed to trial phishing crimes targeting Iranian victims living abroad. Some scholars imply that the PPJ principle is a proof-of-concept advocating skepticism in the foreign criminal systems (Mir Mohammad Sadeghi, 2021: 83). As with the PPJ principle, when phishing committed abroad by foreign nationals against Iranians if the phisher is arrested in Iran or consigned to Iranian legal bodies, the Iranian courts will have jurisdiction to address the crime committed.

5.1.2. Inherent jurisdiction

This section discusses the inherent jurisdiction of Iranian courts in trialing phishing scams. When Iranian courts are allowed to trial a phishing crime according to the jurisdiction principles, their inherent jurisdiction shall be confirmed initially. As with Article 301 of the CJA and regarding the extent of penalties set for phishing crimes, the criminal court No. 2 (CC2) will have inherent jurisdiction to judge the committed crime.

5.1.3. Territorial jurisdiction

The most challenging step to trial phishing scams is to verify the territorial jurisdiction of criminal courts. As with Article 310 of the CJA, a competent court regarding criminal crimes is the court located where the crime has been committed. When all the crime steps from its very beginning to outcomes are in a judicial district, the criminal court of that judicial district has jurisdiction to judge the crime. Likewise, when phishing is a computer fraud committed in a judicial district but the consequences affect another judicial district, the court of a judicial district where the victim has a bank account will have jurisdiction to trial the case (the precedent 729 enacted on 2013-2-19). For example, when a fake link via text message under the title of judicial notification is sent by a phisher in Tehran to a person living in the same place and the phisher gains access to the user's information and then acts to empty the victim's account, the criminal court in Tehran will have jurisdiction to trial the case. However, when the phisher lives in Shiraz, the user lives in Tehran, and the user has an account in a bank in Isfahan, the Isfahan court will have jurisdiction to judge the case based on the issued precedent. Ultimately, when the place of phishing is unidentified, the office of the public prosecutor and the court in the crime district will have inherent jurisdiction to judge the case.

5.2. The way of criminal proceedings

According to Article 28 of the CJA, crime exposure is the duty of an executive officer. One example is computer crimes exposed by the Iranian FATA police, where the victim of phishing can file a complaint through FATA police or electronic judicial service offices. If the Tehran court has jurisdiction, the criminal prosecution will be performed in the prosecutor's office for computer crimes. Conversely, when the criminal court of another judicial district has jurisdiction, criminal prosecution will be taken in the public prosecutor's office. After issuing the indictment, the case will be sent to the CC2 for the trial of the accused phisher. As with Article 666 of the CJA, the judiciary shall allocate a branch in the prosecutor's office and court for computer crimes. If the convict objects to the court decision, they can appeal within 20 days in the provincial appeals court.

Criminological analysis

This section analyzes phishing criminologically and covers victimology, crime prevention, and criminal sociology regarding the dimensions of its phishing perpetration.

6.1. Victimology

A critical aspect of phishing to consider is the unique role the victim plays in phishing perpetration. Phishing, in turn, will not be committed until the victim is caught by the set trap. One strategy to victimize the user is financial victimization mostly committed in society in the form of crimes targeting properties and ownership. There exist two theories regarding the ideology of phishing. The first theory regarding the topology of the victim known as victimology was first reported by Benjamin Mendelsohn, who classified victims as 1) completely innocent victims, 2) victims with minor guilt, 3) a guilty victim, and 4) victims who alone are guilty (Najafi and Hashem Beygi, 2014: 292). In this classification, a victim with minor guilt is ignorant and uninformed of how phishing is committed. This class of victims is more targeted by phishing scams. The second theory is supported victimology, by which the victim is supported and receives assistance to compensate for their damages and losses from the crime (Rayjian Asli, 2011: 15). Phishing is a widely occurring crime in society. Since the offender acquires the victim's property, this crime is paramount necessitating special attention to the victim. For example, a person receives a message regarding a criminal complaint and instantly clicks on the link to know what is happening, Shortly after, they find their account has been fully empty. The victim, thus, finds the situation hard to handle, and this is where society and the justice system shall pursue the rights of the victim based on the models of victimology.

6.2. Crime prevention

The next key and vast aspect of criminology is crime prevention. Crime prevention refers to the prediction, identification, and evaluation of crime risk and the adoption of crucial strategies for its elimination or reduction (Article 1 of the Law on Crime Prevention). There are three patterns of phishing prevention.

The first pattern is triple prevention which includes three levels of prevention: primary, secondary, and tertiary. Primary prevention refers to adopting special strategies to prevent individuals in society from committing crimes. One example of such a strategy is social welfare enhancement, which prevents crime by improving living conditions (Najafi, 1999: 128). Secondary prevention deals with ready-to-commit-crime individuals and necessitates taking political actions to socialize them in society. These two levels of prevention are non-criminal, implying no need for any punishment to avoid crime (Niyazpour, 2021-a; 78). The tertiary prevention aims to train the offender and acclimatize them to social settings to avoid crime repetition (Najafi, Idem, 29). This level of prevention is criminal, necessitating degrees of sentence to avoid crime. Importantly, all three levels of prevention can efficiently reduce the frequency of crime. Social welfare enhancement affords more items to the offender to shift toward them instead of committing a crime. Likewise, expeditious suppressive measures against those inclined toward cybercrimes can effectively make them socialized. Furthermore, tailored criminal and non-criminal reactions toward phishers can markedly reduce the frequency of phishing.

The second pattern of crime prevention is individual-oriented. This pattern highlights the personality of individuals, aiming to adopt measures tailored to each personality to promote the sociability of these groups. Individual-oriented prevention is investigated from two distinct aspects: development-oriented and community-oriented prevention. The development-oriented prevention aims to psychologically and sociologically support children with problems to ultimately make them socialized (Niyazpour, Idem.: 152). One example is to identify factors triggering crime perpetration and taking measures to eliminate risk and other underlying factors. The community-oriented prevention accentuates the environment for executing preventive measures (Jandali and Ebrahimi, 2014: 63), and ponders family, school, friends, colleagues, living environment, media, and so forth as potent targets to be improved for crime prevention. However, individual-oriented prevention outperforms community-oriented measures in crime prevention, as it 1) identifies children inclined toward delinquency, 2) takes effective psychological measures to socialize these groups, 3) identifies individuals with computer intelligence and skills that are likely to perform cyber scams, 4) informs individuals on social media about crime prevention and ways of victimization, and 5) creates a platform for those with computer skills to furnish their capabilities in right areas.

The third pattern is situational crime prevention, aiming to reduce crime perpetration by targeting crime-contributing factors (Safari, 2011: 292). Situational crime prevention avoids underlining the offender but highlights crime targets, spotlights the costs (and declines the profits) for offenders, diminishes the targets for criminal events, and so forth. Examples of situational prevention regarding phishing are using OTPs, defining filters to make phishing a daunting task for offenders, broadcasting blacklists, public awareness, and other similar actions.

6.3. Criminal sociology

Criminal sociology studies the offender's non-biological and psychological background (i.e., the society) deriving crime perpetration are studied. There are multiple theories of criminal sociology in phishing, of which three are discussed in this section.

The first theory is Merton's Theory of Strain, implying that individuals are inclined toward delinquent actions due to society's emphasis on attaining certain socially accepted goals and dreams, as well as due to economic injustice. Merton believes that the theory of strain refers to a standing ambiguity between legal demands and the means to realize them (Niyazpour, 2021-b: 137). Simply put, one side of phishing is a person with cyber skills and multiple dreams such as earning money, purchasing a car and house and similar items, but finds them fairly unattainable due to chaotic economic conditions, unemployment, impatience, and hurry up in fulfilling the dreams, imposing huge pressure on them. The other side of phishing is the tools available to achieve these goals where such a person is triggered to achieve their dreams through illegal ways.

The second theory is the rational choice theory of Jeremy Bentham. According to his concept of hedonic calculus, Bentham believes that profits and losses constitute human behavior, and individuals measure potential profits and benefits from performing their actions and further reflect other factors such as pleasure and attainability of goals when performing a crime (Salehi, 2014: 136). Accordingly, the penalizes shall be adequately excruciating and deterrent such that the offender finds it irrational and less beneficial. Based on this theory, Derek Cornish believes that the offender will commit a crime if they rationally find it beneficial, which is made if there is a benefit. As such, he emphasizes multiplying the costs and penalizing them to avoid such crimes. Additionally, phishing's usefulness for phishers can be doubted by applying deterrent penalties.

The third theory is Howard Becker's theory of labeling. Based on this theory, society rejects and defames the offender by labeling them as a criminal, thereby triggering the offender to repeat the crime as they accept that they are a guilty person.

This theory pursues a reaction against crime beyond the scope of criminal justice, as it ponders the criminal justice to be the cause of the offender's stigma and their tendency to secondary deviance. Since the phisher has superb computer skills and is adequately intelligent, and regarding the consequences of phishing in society, it is crucial to launch training seasons based on the labeling theory and support the criminal to avoid re-committing the scam. Likewise, the offender can be dealt with in a permissive manner concerning the criminal's characteristics such as criminal history, factors triggering crime perpetration, regret, efforts to compensate for the damage, family background, social status, and other means, and further provided with platforms to furnish their talent in right directions.

Conclusion and prospects

The Iranian criminal laws fail to precisely criminalize phishing and merely act according to Articles 1, 12, and 13 of the LCC to protect the victim's rights and realize criminal justice based on the crime dimensions and tailored to the extent of crime committed by the offender. Notably, Articles 1, 12, and 13 deal respectively with illegal access, computer theft, and computer fraud. When phishing is a complete offense, it will be dealt with according to Article 1 of the LCC which criminalizes illegal access. Importantly, phishing differs from classic fraud and theft, as phishers are intelligent, and if properly socialized, they can furnish their talents in cyberspace areas to serve themselves and society. Accordingly, the socialization of phishers and those talented ones with computer skills can foster primary prevention (for those who are not exposed to committing crime) and secondary prevention (for those who are exposed to crime). In the long term, it can measurably reduce the frequency of phishing and boost the talent of this group of individuals.

Most importantly, the victims play decisive roles in the incidence of phishing, as this crime will not be committed until the victim is trapped by the offenders. To avoid this, all capacities shall be exploited to enhance public awareness about how phishers act in such scams.

At the same time, the Iranian FATA police shall be strongly involved in preventing phishing by employing experts and taking all the necessary measures to deter and disrupt this scam. Phishing is, in turn, a crime that can be markedly prohibited by suppressive actions, with more efforts regarding this culminating in a sharp decline in phishing occurrence.

The special court for computer crimes in Tehran stands for the prosecution and trial of phishing cases. However, such a court is lacking in other cities and such cases are inevitably dealt with in public and revolutionary courts. This same applies to the courts. In the Iranian CJA, specialized branches are currently foreseen for computer crimes, which require expert judges for the trial of phishing cases.

The following are recommended to deter and disrupt phishing scams and support the victims:

1) Criminalizing phishing as a distinct criminal action and foreseeing its diverse dimensions
2) Upgrading public awareness on social media and by mass communication tools, and delivering informative content to deter this crime
3) Strict cyberspace oversight (particularly by FATA police) to prevent phishing
4) Supporting ready-to-commit crime individuals as a secondary crime prevention strategy
5) Supporting phishers who are under trial, punishment, or prestige restoration. This measure is a type of tertiary crime prevention and is attainable by cooperating with phishers and providing them with platforms and programs to furnish their skills in the right direction.
6) Offering abatements for offenders with no criminal background who regret their behavior, but applying more severe penalizes for them if they persist in phishing perpetration.
7) Enforcing deterrent sentences for phishers, socializing them, and allowing them to regain their social standing.
8) Enhancing cyberspace security to restrict phishing cases.
9) Introducing the blacklist of phishing sites to enhance public awareness.
10) Training the right ways of searching websites to detect phishing sites.
11) Working with experts to diminish cases of cybercrime, particularly phishing.
12) Alarming ready-to-commit crime individuals, especially young adults and teenagers who have access to computers.
13) Launching special courts for the prosecution of computer crimes in other cities.

References

[1] Babaei, Javad, (2021); Computer crimes and the governing procedures, Tehran, General Directorate of Judiciary Education, 6th edition
[2] Bateni et al. (2013); Persian Contemporary Dictionary, Tehran, Contemporary Dictionary Press, 25th edition
[3] Bahremand, Hamid, (2017); Challenges of Multiplicity of Crimes Regulations in Cyber Crimes, Journal of Judicial Law, 81 (100), 53-66
[4] Jalali Farahani, Amir Hossein, (2004); Prevention of computer crimes, Journal of Judicial Law, 67 (47), 87-119

[5] Jandali, Menon, (2014); An introduction to crime prevention, translated by Shahram Ebrahimi, Tehran, Mizan Publications, 1st edition
[6] Khaleghi, Ali, (2023), Essays on International Criminal Law, Tehran, Shahr Danesh Publications, 7th edition
[7] Rajian Asli, Mehrdad, (2011); Supportive Victimology, Tehran, Judges Publications, 2ndedition
[8] Rahimi, Moosa, Rahimi Dehsuri, Reza, (2020); Statements of the Criminal Justice Act, Tehran, Chatre Danesh Publications, 1st edition
[9] Zubair, Ulrish, (2004); Computer Crimes, translated by Ahmad Rafiei Moghadam et al., Tehran, Ganje Danesh Publications
[10] Shams, Abdullah, (2018); Laws of the Criminal Justice Act, 1st volume, Tehran, Derak Publishing House, 50th edition
[11] Safari, Ali, (2001), Theoretical Foundations of Crime Prevention, Journal of Legal Research, 4(33&34), 267-321
[12] Salahi, Javid, (2014), General Criminology and New Theories, Majd Publications, 1stedition.
[13] Goldoozian, Iraj, (2020-b), Iranian special penal laws, Tehran, Tehran University Press, 24thedition
[14] Goldoozian, Iraj, (2020); Iranian public penal laws, Tehran, Tehran University Press, 17thedition
[15] Goldoozian, Iraj, (2021), Annotation of the Islamic Penal Code, Tehran, Majid Publishing House, 11th edition
[16] Mir Mohammad Sadeghi, Hossein, (2024), Iranian special penal laws against property and ownership, Tehran, Mizan Publications, 64th edition
[17] Mir Mohammad Sadeghi, Hossein, (2021), Iranian public penal laws, Tehran, Judge's Press, 3rd edition
[18] Mir Mohammad Sadeghi, Hossein, Shayegan, Mohammad Rasool, (2017), Strategies to judge computer fraud cases in Iran's criminal law, Journal of Legal Perspectives, No. 42 and 43, 109-126
[19] Najafi, Ali Hossein, Hashem Beygi, Majid, (2014), Encyclopedia of Criminology, Tehran, Ganje Danesh Press, 3rd edition
[20] Najafi, Ali Hossein, (1999); Crime Prevention and Local Police, Legal Research, No. 25 and 26, 129-149
[21] Niazpour, Amir Hasan, (2021-a), Prevention of crime, Tehran, Justice's publication, 1stedition
[22] Niazpour, Amirhasan, (2021-b), Criminal Sociology Discourse, prepared and edited by Ali Taghizadeh, Tuba Mojarrad, and Sadigheh Karjoo Rafee, Shahid Beheshti University, Master's program.