



CYBER CRIMES

*Risks, Prevention
and Legal Remedies*

GUIDELINES FOR CYBER USERS



CYBER CRIME WING
FEDERAL INVESTIGATION AGENCY



Ministry of Interior, Government of Pakistan



FOREWORD

The modern world has witnessed an exponential rise in the use of the Internet. While cyberspace offers an endless service and opportunities, unfortunately, it is also accompanied by risks that many Internet users are unaware of. Thus, cybercrime is on a sharp rise resulting in substantial financial and other privacy concerns.



Federal Investigation Agency (FIA), being the lead agency to deal with cybercrime, is committed to combating it through enforcement actions and awareness-raising measures. FIA has adopted a holistic strategy to revamp the Cyber Crime Wing to respond to complaints of cybercrimes effectively and efficiently. A range of initiatives includes the establishment of 15 dedicated cyber police stations across the country, the launch of Rs. 2 billion revamping of cybercrime wing project, amendments in PECA rules to further strengthen the wing, the launch of complaint management and tracking system, liaison with social media giants such as Facebook, and community outreach to educate on cybercrimes. This booklet titled 'Cyber Crimes: Risks, Prevention & Legal Remedies' has been developed to make cyber users aware of major cyber-related offences. The primary purpose of this booklet is to enable Internet users to take proactive and preventive measures against the risks of cybercrimes.

In the end I would like to place my appreciation for Dr. Ehsan Sadiq, Additional Director General, Cyber Crime Wing, FIA and his team for meticulously producing this booklet. I hope it will enable cyber users to adopt preventive measures against online crimes and take recourse to legal remedies if they still fall victim to such crimes.

Dr. Sanaullah Abbassi, PSP
Director General,
Federal Investigation Agency





MESSAGE

The emergence of Information and Communication Technology (ICT) has changed the world around us, with personal spaces being transformed into cyber spaces. This revolution of technology has not only changed our cognitive process but it has also re-engineered human interactions as well. Unfortunately, these technologies can also provide avenues for the criminals to commit larger, more rewarding and sophisticated cyber crimes.




Realizing these emerging threats to safety of citizens using digital devices and ICT, Federal Investigation Agency established Cyber Crime Wing (CCW) to combat the misuse of cyber space. CCW is the only unit in the country that has the mandate to investigate and prosecute cyber crimes. Since its inception, CCW has performed considerably well despite challenges of ever growing complaints, limited international cooperation and resource inadequacy. During my tenure as Director General, FIA, we paid special attention to overcome these challenges. The present government deserves appreciation for allocating sufficient resources for this purpose.

Given the scale of cyber crime, it would be unrealistic to expect that law enforcement authorities alone can fight cyber crime. The continuous awareness and education of the Internet users can go a long way to prevent the growing cyber crime in Pakistan.

I hope this 'Booklet' will play an important role in raising the awareness among all Internet users and guide them to implement techniques in cyber space to prevent them from becoming victim of cybercrimes.

Wajid Zia, PSP

Former Director General,
Federal Investigation Agency





PREFACE

The fast-growing Internet technologies are transforming various spheres of our daily life that include business, work, governance, security and politics. Individuals and organizations have become increasingly dependent upon the Information and Communication Technology (ICT) networks. The increasing use of cyber space has resulted in both opportunities and vulnerabilities, which can be exploited by cyber criminals to pose cyber threats to both individuals and national security.



This booklet aims to create awareness among the readers about the range, magnitude and types of cyber crimes in Pakistan; possible preventive measures to be adopted by Internet users; and legal safeguards provided under Prevention of Electronic Crime Act, (PECA)-2016 if a person becomes victim of a cyber crime.

I take this opportunity to express my profound gratitude to Mr. Wajid Zia, Director General, Federal Investigation Agency, for valuable guidance and immense support in preparation of this booklet. I would also like to appreciate valuable inputs by Mr. Muhammad Jafer, Director Cyber Crime Wing (CCW), Mr. Abdur Rab, Director Operations, Ms. Sumera Azam Additional Director CCW, Mr. Mehmood-ul-Hassan Deputy Director, Mr. Ayaz Khan Deputy Director and Inspector Safia.

I sincerely hope that this booklet will be a useful and informative resource for the cyber users to keep them abreast of most common risks, educate them about appropriate precautionary measures against such risks, and help them to avail legal recourse if they become a victim of cyber criminals.

Dr. Ehsan Sadiq, PSP
Additional Director General,
Cyber Crime Wing,
Federal Investigation Agency





ACRONYMS AND CYBERCRIME TERMS

CCRC: Cyber Crime Reporting Centre

Cracking: the process of trying to overcome a security measure

Cybercrime: crime related to technology, computers, and the Internet

Cyber Bullying: The act of one individual harassing or intimidating another individual via the Internet

Hacker: a term sometimes used to describe a person who breaks into computer systems for the purpose of stealing or destroying data

Hacking: a term referred to a process of bypassing the security systems on a computer system or internet.

Information System: "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information

IP spoofing: an attack where the attacker disguises himself or herself as another user by means of a false IP network address

Login: A username and password used to identify an individual attempting to gain access to a restricted page or network.

Malicious code: any code that is intentionally included in software or hardware for an unauthorized purpose

Malware: Software used or created by hackers to disrupt computer operation, gather sensitive information or gain access to private computer systems. Short for malicious software, it is often contained within a website link or attachment.

Minor: means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

NACTA: National Counter Terrorism Authority

Phishing: Attempting to mimic an official email from a trusted organization to lure individuals into revealing login information or other personal information.

Risk assessment: the process of studying the vulnerabilities, threats to, and likelihood of attacks on a computer system or network

Spam: Unsolicited advertising or other information sent out via email or other messaging service.

Social engineering: term often used to describe the techniques virus writers and hackers utilize to trick computer users into revealing information.

Spoofing: When an unauthorized person makes a message (typically an email) appear to come from a legitimate sender by using either the genuine or a very similar address.

Spyware: Malware that secretly monitors a user's activity or scans for private information.

Virus: a computer program designed to make copies of itself and spread itself from one machine to another without the help of the user.



TABLE OF CONTENTS

| | | |
|-----------|---|-----------|
| 1) | Introduction | 04 |
| 2) | Major Cyber Offences | |
| I. | Electronic Financial Fraud | 13 |
| ii. | Cyber Harassment | 15 |
| iii. | Cyber Defaming | 17 |
| iv. | Cyber Blackmailing | 19 |
| v. | Hate Speech | 21 |
| vi. | Illegal SIMs | 22 |
| vii. | Child Pornography | 24 |
| viii. | Identity Theft | 26 |
| ix. | Cyber Terrorism | 28 |
| x. | Cryptocurrency | 30 |
| 3) | Common Cyber Crime Techniques | |
| i. | Spamming | 35 |
| ii. | Spoofing | 36 |
| iii. | Phishing | 37 |
| iv. | Pharming | 38 |
| v. | Hacking | 39 |
| vi. | Social Engineering | 40 |
| vii. | Denial of Service (DoS) attacks | 41 |
| viii. | Man-in-the-Middle attacks | 42 |
| ix. | Computer Virus | 43 |
| x. | Malware | 44 |
| xi. | Web Application | 45 |
| 4) | Common Types of Financial Frauds in Pakistan | 47 |
| 5) | Awareness Message for Cyber Users | 51 |



INTRODUCTION

Cyber-crime in general can be defined as a crime or an unlawful act through a information system. In a cyber crime, a computer or a mobile phone is often used either as a tool, a target or both. In simple words, cyber crime is an unauthorized access to information systems without the permission of rightful owner or use of one's own information system to commit crime on the cyberspace/internet.

Cyber threats vary in terms of degree of severity ranging from hacking, identity theft, cyber harassment, online child sexual abuse and cyber terrorism. In terms of motivation, they may be related to politics, security, economics, ethnicities or culture.

Citizens use Internet for a variety of purposes such as shopping, map directions, education, auction, games, medical assistance, information sharing, social networking, online banking, internet surfing, audio-video communication and entertainment. These activities may expose the internet users to various sorts of cybercrime that may include financial fraud, hacking, cyber harassment, cyber blackmailing, online abuse, cyber defamation, unauthorized access, identity theft, financial fraud, illegal SIMs, child pornography, hate speech, cyber terrorism, phishing, spoofing and spamming.

The advent of cyber-space and the resulting cyber-crimes imparted a whole new dimension to the dark world of crime. It is truly unique in nature being invisible, transnational, fast and ever evolving. Investigating cybercrime is a challenge for Law Enforcement Agencies (LEAs) across the world because of its highly technical nature and also because of transnational crime. This now requires an entirely new level of national and international cooperation to access the information, collect evidences, seize the equipment and arrest the accused.

The magnitude of cybercrime in Pakistan can be gauged from the complaints received in different categories. Cyber Crime Wing (CCW) received 84,764 complaints in 2020. The majority of the complaints were related to Financial Fraud (20,218), Hacking (7,966), Cyber Harassment/ threats (6,023), Fake Profiles/Identity Theft (4,456), Defamation (6,004), Cyber Blackmailing (3,447) and Hate Speech (892).

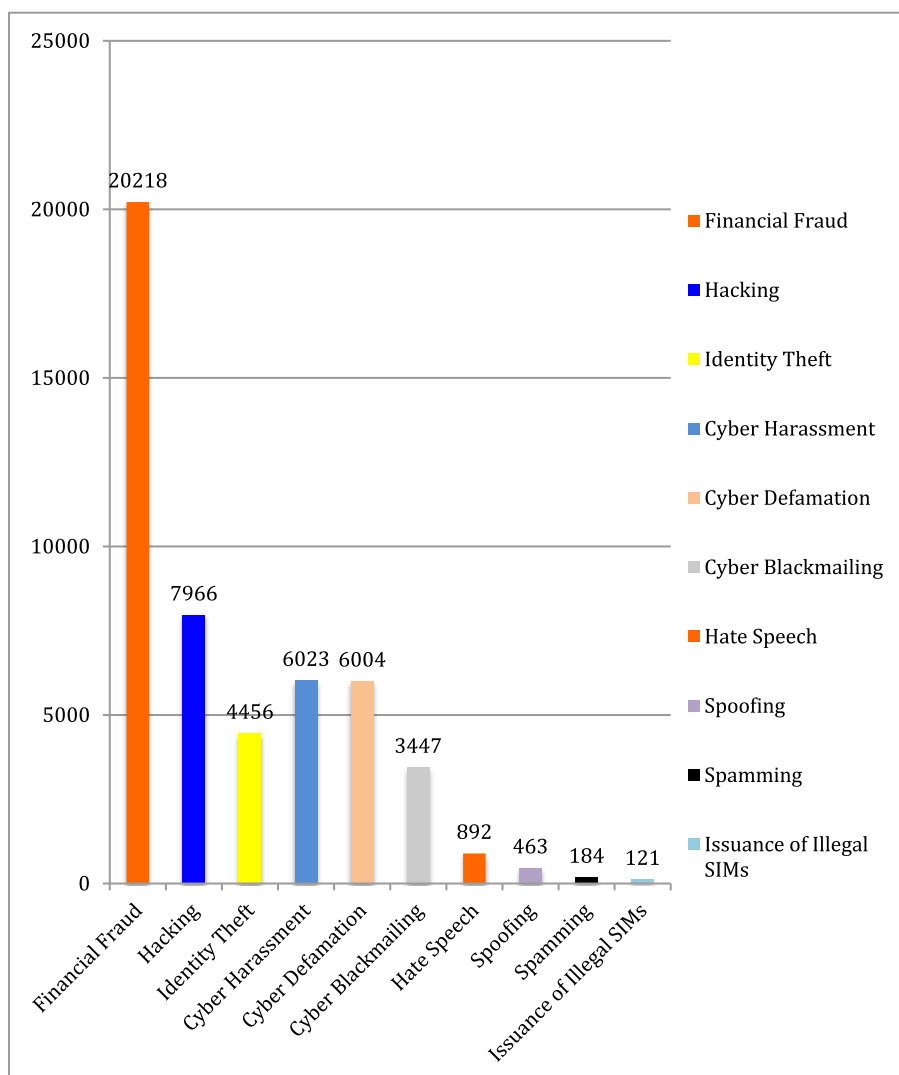
The purpose of this booklet is to educate the general public on major risks for cyber users in cyberspace and basic preventive measures to keep themselves safe. The booklet is divided into two parts: the first part covers the major offences related to cybercrime and the second part covers the common techniques used by cyber criminals to commit cybercrimes.



MAJOR CATEGORIES OF CYBERCRIME COMPLAINTS IN 2020

Cyber Crime Wing received (84,764) complaints in 2020. The majority of the complaints were related to:

| | | | |
|------------------------------|----------|---------------------------|---------|
| Financial Fraud | (20,218) | Hacking | (7,966) |
| Fake Profiles/Identity Theft | (4,456) | Cyber Harassment/ Threats | (6,023) |
| Defamation | (6,004) | Cyber Blackmailing | (3,447) |
| Hate Speech | (892) | | |





MAJOR CYBER OFFENCES

Digital Financial Fraud

Cyber Blackmailing

Cyber Harassment

Hate Speech

Illegal SIMs

Cyber Defaming

Child Pornography

Identity Theft

Cyber Terrorism

Cryptocurrency





RISK 01 ELECTRONIC FINANCIAL FRAUD

Electronic financial fraud refers to any fraudulent activity committed through online means (email, websites, social media, etc.) for gaining illegal financial benefit*.

Electronic financial fraud is a crime under Section 14 of PECA, 2016 which provides that:

“Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.”

FIA registered 32,324 complaints, 3706 enquiries and 154 cases related to electronic financial frauds in the year 2020.

Criminals use various methods / tactics to commit electronic financial fraud by:

- Pretending as an authorized caller from the respective bank, Benazir Income Support Programme, Army or Cellular Company Officials, etc. for seeking confidential information of conventional/ mobile bank account which includes victim's account number, mother name, date of birth, PIN, One Time Password (OTP) etc;
- Placing a device on the face of an ATM (which appears to be a part of the machine) to steal data of a card holder;
- Creating online shopping sites/pages with eye-catching discounts and offers with the intention to deceive the general public;
- Pretending as a representative of any charitable organization (NGO), with intention to disperse charity amount and demand money for clearance of shipment;
- Impersonating as a representative of game shows which include Jeeto Pakistan, BOL Game Show etc, for winning the prizes;
- Creating profiles on social media applications (dating / matrimonial websites) and build trust to seek money in the form of air tickets, custom / visa fee or investment, etc

Global losses regarding electronic payment frauds have tripled from \$9.84 billion to \$32.39 billion (From 2011 to 2020.)

Source:

www.merchantsavvy.co.uk

**(European Union Agency for Network and Information Security <https://www.enisa.europa.eu>)*



Prevent yourself from being a victim of electronic financial fraud by:

- Not sharing your confidential information like credit /debit card number, ATM PIN, OTP, CNIC number, date of birth, birthplace, mother's name, with anyone;
- Physically checking ATM machine, for any additional attachment of suspicious device on ATM Card Slot or hidden camera placed on ATM machine number pad;
- Reviewing the financial transactions record regularly to detect any suspicious/illegal transactions;
- Buying from online shopping sites/pages preferably with considerable rating and positive reviews.

Case Study



FIA CCRC (Cyber Crime Reporting Centre), Rawalpindi, registered an FIR in 2020 against the accused person pretending to be a legitimate online seller or spare parts of vehicles with a fake Facebook account. He extorted money on the promise of delivering spare parts by uploading / posting pictures of spare parts of different cars and asking people to send money to his bank accounts as an advance payment. The alleged person actively ran the Facebook page and removes all the comments against him. He was subsequently sentenced to 02 years of rigorous imprisonment and fine under PECA, 2016.



RISK 02 CYBER HARASSMENT

Cyber harassment involves threatening, insulting or unwanted messages through cyberspace with the intention to harm an individual or a group*.

Cyber harassment is a crime under Section 24 of PECA, 2016 which provides that:

(1) “A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to,

- a) Follow a person, contacts, or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;
- b) Monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication;
- c) Watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or
- d) Take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person.

(2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both. Provided that if victim of the cyber harassment under sub-section (1) is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both.

FIA registered 6,023 complaints, 2694 enquiries and 79 cases related to cyber harassment in the year 2020.

Criminals use various methods / tactics to commit the offence of cyber harassment by:

- Consistently and repeatedly sending obnoxious messages, e-mails, or any other form of electronic communication;
- Monitoring personal online accounts/contacts by hacking;
- Sharing and distributing personal pictures/videos on social media platforms with the intention to harm the reputation.

Almost 1.5 million people in the United States alone suffer from cyber stalking at least once every single year.

Source: (<https://brandongaille.com/20-provocative-cyberstalking-statistics>)

*(<https://definitions.uslegal.com/c/cyber-harassment/>)



To prevent yourself from being a victim of cyber harassment, you must:

- Block and report the suspect using the reporting mechanism available by social media platforms;
- Use a gender neutral e-mail address;
- Avoid sharing personal data with friends and acquaintances on social media or public chat rooms;
- Avoid using public chat rooms for making new friends;
- Limit your friends' list to the extent of your family members and closed acquaintances;
- Use the privacy and security settings on the social media platforms;
- Report to Cybercrime Wing of FIA, if the offender persists in his/her acts.

Case Study

FIA CCRC, Quetta registered an FIR in 2020 against a person who sent messages through SMS. The accused was sending text messages on WhatsApp to a woman without her consent containing information about her location and her daily life activities. He also sent a friendship request through Facebook ID, but she refused to accept it. Continuous and frequent attempts to contact her caused fear of insecurity. The accused was arrested, and sufficient evidence against him was collected. The court subsequently sentenced him to one-year rigorous imprisonment with a fine.





RISK 03 CYBER DEFAMATION

Cyber defamation is an act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace (through websites, blogs, forums, emails chat rooms and instant messaging applications and instant messaging, chat rooms and in the social networking)*.

Cyber defamation is a crime under Section 20 of PECA, 2016 which provides that:

“(1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

FIA registered 6009 complaints related to cyber defamation in the year 2020.

Criminals use various methods / tactics to commit the offence of cyber defamation by:

- Posting/ sharing defamatory, derogatory or insulting remarks/ comments on social media platforms (WhatsApp, Facebook, Twitter, YouTube etc.);
- Sharing/ uploading of speech/ videos/ pictures online in a manner which cause harm to the reputation of the person.

Actor Geoffrey Rush has been awarded the largest ever defamation payout to a single person in Australia.

The Oscar-winner was awarded A\$2.9m (£1.57m; US\$1.99m) after winning the case against Australia's Daily Telegraph.

Source:<https://www.bbc.com/news/world-australia-48379980>

*(psu.edu)



To prevent yourself from being an accused of cyber defamation, you must:

- Not post/ share/ upload any unauthentic/ fake news, defamatory or derogatory remarks on social media against any individual or groups;
- Cautiously choose words in your speech or arguments in order to refrain from hurting some one's dignity;
- Avoid posting or tweeting any comments which might affect someone's reputation;

Case Study



FIA CCRC, Karachi, registered an FIR against a person accused of making a video of his political rival and uploading it on WhatsApp to defame him. During the investigation, it transpired that the accused had made his video with derogatory, incriminating remarks to damage and defame his good reputation and making it viral on WhatsApp groups. The accused was sentenced to an imprisonment of two years.



RISK 04 CYBER BLACKMAILING

Cyber blackmailing is the act of threatening an individual to share private information to the public, friends or family via the Internet, unless a demand is met or money is paid. *

Cyber blackmailing is a crime under Section 21 of PECA,2016 which provides that:

- (1) Whoever intentionally and publicly exhibits or displays or transmits any information which,
 - a) Superimposes a photograph of the face of a natural person over any sexually explicit image or video; or
 - b) includes a photograph or a video of a natural person in sexually explicit conduct; or
 - c) intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or
 - d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.
- (2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term, which may extend to seven years and with fine which may extend to five million rupees:

Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.
- (3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

*(<https://www.bbc.com/news/newsbeat-23724703>).



FIA registered 3447 complaints, 1826 enquiries and 222 cases related to cyber blackmailing in the year 2020.

To prevent yourself from being a victim of cyber blackmailing, you must not:

- Make available or store any private (obscene) pictures/ videos in your electronic devices;
- Share private pictures/videos online with anyone even when asked by your close friends;
- Sell your mobile phone/ computer/ memory cards etc. without deleting/ formatting personal data;
- Post personal information online i.e. your home address, phone number and email address.

To prevent yourself from being an accused of cyber blackmailing, you must not:

- Share/ post/ upload anyone's personal/ private information (videos, messages, pictures) online;
- Blackmail individual on the basis of possessing of any private information to gain illegal favours.

The Internet Crime Complaint Centre (IC3) has seen an increase in reports of online extortion scams during the current "stay-at-home" orders due to the COVID-19 crisis.

Source: <https://www.ic3.gov/Media/Y2020/PSA200420>

Case Study

FIA Cyber Crime Reporting Centre, Karachi registered an FIR in 2019 against a person for his alleged involvement in blackmailing a woman. The man was arrested, and a court subsequently sentenced him to one-year imprisonment with Rs. 50,000/- fine





RISK 05 HATE SPEECH

A public speech that expresses hate or encourages violence towards a person or group based on something such as religion or racial hatred through information system (social media platforms like Facebook, WhatsApp, Twitter, Instagram etc)*

Hate speech is a crime under Section 11 of PECA, 2016 which provides that:

“Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.”

FIA registered 892 complaints, 51 enquiries and 54 cases related to hate speech in the year 2020.

To prevent yourself from being an accused of hate speech, you must not:

- Upload, post or share any video/audio clips, text messages on social media platforms/websites, which incite hatred towards a religion, sect, race or faith of a particular group;

As per FBI's Uniform Crime Reporting (UCR) Program there were 7,314 hate crime incidents involving 8,559 offenses in the year 2019.

Source:<https://ucr.fbi.gov/hate-crime/2019>.

Case Study

FIA CCRC, Rawalpindi, in 2017 registered an FIR against several unknown people/groups disseminating/spreading blasphemous material through social media, i.e., Facebook, Twitter, websites, etc. for willfully defiling and outraging religious feeling, belief, by using derogatory words/remarks/graphic designs/images/sketches/visual representations in respect of the sacred names. ATA court subsequently sentenced three accused persons to death for the said offences.





RISK 06

SALE & PROVISION OF ILLEGAL SIMS

Sale and issuance of a SIM (Subscriber Identity Module), which carries an identification number unique to the owner without proper verification/authentication of the subscriber's credentials as prescribed by the Pakistan Telecommunication Authority is illegal.

Sale and provision of illegal SIMs, is a crime under Section 17 of PECA, 2016 which provides that:

“Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.”

FIA registered 195 complaints, 174 enquiries and 29 cases related to unauthorized sale and provision of SIMs, in the year 2020.

A Three-member gang was arrested in Dubai for illegal issuance of hundreds of SIM cards which were used for phone scam.

Source: The Khaleej Times, 22nd May 2020).

Criminals use various methods /tactics for the provision of illegal SIMs by:


- Collecting thumb data on biometric devices from innocent citizens especially elderly women on the pretext of issuing Ehsas card, Benazir Income Support Programme (BISP) card, Free SIM etc.;
- Carrying thumb impression in soft form, refined through software and printed on silicon sheets which are later used for issuance of illegal SIMs.

To prevent yourself from issuance of illegal SIMs, you must:

- Purchase SIMs from Cellular Franchise, rather than KIOSK (portable van, stand-alone booth, door-to-door sale);
- Periodically check number of SIMs issued in your name by sending CNIC Number at 668 and block the illegally issued SIMs.



Case Study



FIA CCRC, Peshawar, registered an FIR against an accused for involvement in issuance of illegal SIMs. The accused was sentenced to an imprisonment of (04) years along with Rs.0.8 Million fine.



RISK 07 CHILD PORNOGRAPHY

Child pornography refers to visual depiction of sexually explicit conduct involving a minor with possession and transmission through cyber space*.

Child pornography is crime under Section 22 of PECA, 2016 which provides that:

“(1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts,

- (a) a minor engaged in sexually explicit conduct;
- (b) a person appearing to be a minor engaged in sexually explicit conduct; or
- (c) realistic images representing a minor engaged in sexually explicit conduct; or
- (d) discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both.

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.”

FIA registered 83 child-pornography and 173 other age-related pornography complaints and 24 cases in the year 2020

Criminals use various methods / tactics to commit the offence of child pornography by:

- Sharing / surfing / downloading / recording / possessing / distributing/ transmitting child sexually explicit videos / pictures through computer, mobile phone, social media etc.

INTERPOL's Child Sexual Exploitation database holds more than 2.7 million images and videos and has helped identify 23,500 victims worldwide.

Source :

<https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>

*(<https://www.justice.gov>)



To prevent your children from being a victim of child pornography you must:

- Monitor your children friendship network closely.
- Maintain strict parental control over internet usage of children;
- Observe any unexpected change in a child's behavior;
- Wisely utilize social media applications' privacy and security settings to limit your children's online interaction with strangers;
- Regular checking of the children's online presence to prevent any child from sexual abuse or exposure to harmful content;
- Conduct regular counseling of children regarding safe use of internet;

To prevent yourself from being an accused you should not:

- Surf/visit websites/online groups/social media accounts containing contents of child sexual exploitation; well-known mailing servers and search engines have algorithms that can automatically detect child sexual exploitation contents and report to LEAs for legal action;
- Possess or share any sexually explicit pictures/videos of minor (with anyone).

Case Study

FIA CCRC, Lahore, registered an FIR in 2017 against one person from whom more than 650,000 child pornography content in the form of digital data was recovered. Subsequently, a court sentenced him to 07 years rigorous imprisonment and Rs1.2 million fine.





RISK 08 IDENTITY THEFT

Identity theft refers to all types of crime in which someone wrongfully obtains another's personal data and uses it in a way that involves fraud or deception, typically for economic gain*.

Identity theft is crime under Section 16 of PECA, 2016 which provides that:

“(1) Whoever obtains sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term, which may extend to three years or with fine, which may extend to five million rupees, or with both.

(2) any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.”

FIA registered 4,456 complaints, 174 enquiries and 29 cases related to identity theft in the year 2020.

Criminals use various methods / tactics to commit the offence of identify theft by:

- Collecting personal information of victim through calls, impersonating as Bank / State Bank officials and uses it for financial gains;
- Sending fraudulent emails or texts that may look legitimate. The links in these emails or texts may be used to download malicious software for collecting personal information;

To prevent yourself from being a victim of identity theft, do not share:

- Bank account number, ATM PIN, credit/debit card number, email password with anyone;
- Personal information (birthdate, CNIC number, CNIC/Passport Picture, mother's name) with anyone online;
- Personal/private or family pictures publicly.

According to 2019 Internet Security Threat report by Symantec, one in ten people are now victim of identity fraud annually, with 21% of these individuals having been victimized multiple times.

Source:

<https://www.cnn.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html>



Case Study

FIA CCRC, Multan, registered an FIR in 2020 against a person who created a government officer's fake Facebook ID and uploaded his pictures to trap girls on the pretext of marrying them. During the investigation, it transpired that the accused is a habitual criminal. He illegally obtained the Caller Data Record of the government officer, contacted his family members, i.e., sisters and fiancé, and uploaded his sister's pictures with derogatory remarks on the fake Facebook ID. Sufficient incriminating evidence related to said offences were recovered from the cell phone of the accused. The accused was imprisoned by the Court for two years with Rs. 0.5 million fine.



RISK 09 CYBER TERRORISM

Cyber terrorism is defined as a cyber-dependent crime perpetrated to provoke fear, intimidate and/or coerce a government or population, and cause or threaten to cause harm*.

Cyber terrorism is a crime under Section 10 of PECA, 2016 which provides that:

Whoever commits or threatens to commits unauthorized access to information system, copying, transmission, or interference with critical infrastructure, or glorifying an offence, where the commission or threat is with the intent to. -

(a) coerce, intimidate. Create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society: or

(b) advance inter-faith, sectarian or ethnic hatred; or

(c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

FIA registered 26 enquiries and 4 cases related to cyber terrorism in the year 2020.

Criminals use various methods/ tactics to commit the offence of cyber terrorism by:

- Uploading and glorifying the activities of proscribed organizations;
- Propagating and glorification of terrorist activities against state;
- Collecting online funds on the behalf of proscribed organizations;
- Publishing violent videos on social media by terrorists intending to spread fear and fright among general public.

The incident of killing an Iranian scientists through a satellite-controlled machine gun has changed the dynamics of attack on individual which resulted in killing of person using the communications.

Source:

<https://www.bbc.com/news/world-middle-east-55214359>


**(Denning, 2001; Jarvis, Macdonald, and Nouri, 2014; Jarvis and Macdonald, 2015)*



To prevent yourself from being an accused you must:

- Avoid commenting / liking or sharing on anti-state/violent statements;
- Avoid sharing or glorifying the proscribed organizations on social media;
- Refrain from collecting funds on behalf of any banned outfit on the internet;
- Not share, like or retweet social media posts promoting violence or containing anti-state material;
- Not access critical infrastructure websites for hacking/illicit purpose.

Case Study



FIA CCRC, Rawalpindi, registered an FIR in 2018 under PECA, 2016 against a person who created a Facebook account and uploaded blasphemous/sectarian material on Facebook to cause interfaith sectarian violence and a sense of fear in public. The accused has been sentenced to (10) years of imprisonment by the Court.



RISK 10 MISUSE OF CRYPTO CURRENCY

A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Most common examples of crypto currency are Bitcoin, Ethereum, Litecoins, and Ripple.

State Bank of Pakistan circular for prohibition of dealing in Virtual Currencies.

| BPRD Circular No. 03 of 2018 | April |
|--|--------------|
| 06, 2018 | |
| The Presidents/ Chief Executive Officers, All Banks/ DFIs/ Microfinance Banks/ PSOs/ PSPs, Dear Sir/Madam, Prohibition of Dealing in Virtual Currencies/Tokens Virtual Currencies (VCs) like Bitcoin, Litecoin, Pakcoin, OneCoin, DasCoin, Pay Diamond etc. or Initial Coin Offerings (ICO) tokens are not legal tender, issued or guaranteed by the Government of Pakistan. SBP has not authorized or licensed any individual or entity for the issuance, sale, purchase, exchange or investment in any such Virtual Currencies/Coins/Tokens in Pakistan. In view of the foregoing, all Banks/ DFIs/ Microfinance Banks and Payment System Operators (PSOs)/Payment Service Providers (PSPs) are advised to refrain from processing, using, trading, holding, transferring value, promoting and investing in Virtual Currencies/Tokens. Further, banks/DFIs/Microfinance Banks and PSOs/PSPs will not facilitate their customers/account holders to transact in VCs/ICO Tokens. Any transaction in this regard shall immediately be reported to Financial Monitoring Unit (FMU) as a suspicious transaction. Please acknowledge receipt. | |
| Yours truly, Sd/- (Muhammad Akhtar Javed) Director | |

FIA registered 20 complaints related to misuse of crypto currency in the year 2020

The criminals use crypto currency to:

- Finance illegal activities to evade conventional banking financial channels;
- Transfer money on pattern of Hundi/Hawala system.

To prevent the misuse of Crypto current, you must

- Avoid investment / trading in any form of crypto currencies since it is not permitted in Pakistan by the State Bank of Pakistan;
- Not use the crypto currency as mode of payment for any business transactions.



Case Study

FIA CCRC, Lahore, registered an FIR in 2020 against two persons for online trade of Cryptocurrency/ E-Currency under PECA-2016, FER Act-1947, AML Act-2010, and PPC. The accused used to acquire virtual currency from freelancers and other virtual currency dealers. In exchange, they gave the dealers cash or transfer money into their bank accounts, which they received from Dubai through Hawala/Hundi. Both of the accused persons were arrested, and an amount of Rs. 5 million and digital equipment was attached on court orders.



COMMON TECHNIQUES USED BY CYBER CRIMINALS

Spamming

Spoofing

Phishing

Pharming

Hacking

Social Engineering

Denial of Service (DoS) Attack

Man-in-the-Middle Attack (MITM)

Computer Virus

Malware

Web Application





TECH 01 SPAMMING

Spamming is an unwanted commercial message received via email, social media message/posts or mobile SMS, pretending to advertise products, offer services, prize winning opportunity or create sense of urgency by warning you of a security breach and asks to change your password via link provided in the message. In response innocent people mistakenly share their confidential data like credit card number, passwords etc, which are then exploited to gain financial benefits by the spammer.

TYPES OF SPAMMING



Email spam: Your garden-variety spam. It clogs up your inbox and distracts you from the emails you actually want to read. Rest assured, it's all extremely ignorable.



Social networking spam: As the internet grows ever more social, spammers are quick to take advantage, spreading their spam via fake "throwaway" accounts on popular social networking platforms.



SEO spam: Also known as spamdexing, this is the abuse of Search Engine Optimization (SEO) methods to improve search rankings for the spammer's website. SEO spam can be divided into two broad categories i.e. Content Spam. and Link Spam.



Mobile spam: It's spam in SMS form. In addition to spammy text messages, some spammers also utilize push notifications to draw your attention to their offers.



Messaging spam: Like email spam, but quicker. Spammers blast their messages out on instant messaging platforms including WhatsApp, Skype, and Snapchat.

SPAMMING PREVENTION

- i. Never give out or post your email address publicly
- ii. Do not reply to spam email
- iii. Install spam-filtering tool
- iv. Avoid using your personal email address when registering in any online contest.
- v. Keep your computer operating system and security software up to date
- vi. User awareness & training



TECH 02 SPOOFING

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites. Spoofing can be done by installing computer malicious code and social engineering or creating scam website looking like a website you use regularly such as Facebook, Alabama, bank or Amazon. i.e. receive an email with address seems to be similar to the original from the bank but is not exactly the same.

WHAT DOES EMAIL SPOOFING LOOK LIKE?

- Incorrect grammar
- Poor spelling
- Badly written sentences or phrases
- Incorrect URL: This can be deceptive and look correct--until you hover over it to uncover the actual URL.
- Misspelled email sender address: The name of the sender or domain--or both--may be misspelled. This can be hard to recognize when viewed quickly and may, for instance, contain the number "1" instead of the letter "l."

SPOOFING PREVENTION

- i. Implement technical controls and procedure to protect against spoofing.
- ii. Multi-factor authentication that protects against credential theft
- iii. Malware protection that can spot risky files in attachments and provide sandboxing
- iv. The email should be signed and mailed by the same platform, for example, if the email is coming from a Gmail account then it should be signed by and mailed by gmail.com.
- v. The return path and email address of the sender should be the same.
- vi. "Pass" should be written after DKIM, DMARC, and SPF fields.



TECH 03 PHISHING

Phishing is a type of social engineering attack often used to steal individual data, including login credentials, passwords, banking, and credit card numbers, by criminals posing as a legitimate institution. An attacker may copy email by using the same logos, phrases, signatures which make the messages appear to be legitimate from banks, Federal Board of Revenue, and send them from a spoofed email to thousands of recipients, and gather essential financial information, even if only a small proportion of recipients fall for the scam.

TYPES OF PHISHING ATTACKS

- Spear phishing: Spear phishing attacks a specific person or organization, often with content that is tailor made for the victim or victims. It requires pre-attack reconnaissance to uncover names, job titles, email addresses, and the like.
- 419/Nigerian Scams: A verbose phishing email from someone claiming to be a Nigerian prince is one of the Internet's earliest and longest-running scams. Incidentally, the number "419" is associated with this scam. It refers to the section of the Nigerian Criminal Code dealing with fraud, the charges, and penalties for offenders.
- Phone Phishing: With phone-based phishing attempts, sometimes called voice phishing or "vishing," the phisher calls claiming to represent your local bank or by the police.

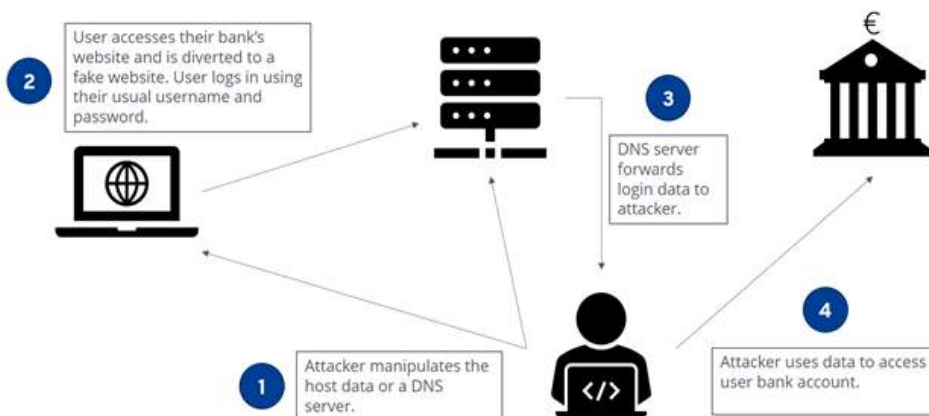
PHISHING PREVENTION

- i. Don't open e-mails from senders you are not familiar with.
- ii. Don't ever click on a link inside of an e-mail unless you know exactly where it is going.
- iii. To layer that protection, if you get an e-mail from a source you are unsure of, navigate to the provided link manually by entering the legitimate website address into your browser.
- iv. Lookout for the digital certificate of a website.
- v. If you are asked to provide sensitive information, check that the URL of the page starts with "HTTPS" instead of just "HTTP." The "S" stands for "secure." It's not a guarantee that a site is legitimate, but most legitimate sites use HTTPS because it's more secure. HTTP sites, even legitimate ones, are vulnerable to hackers.
- vi. If you suspect an e-mail isn't legitimate, take a name or some text from the message and put it into a search engine to see if any known phishing attacks exist using the same methods.
- vii. Mouseover the link to see if it's a legitimate link.

TECH 04 PHARMING

Pharming is an attack intended to redirect your website traffic to another, probably bogus website. Pharming is usually done by infecting DNS servers which is beyond control and remains undetectable for a large part. The only way pharming could have been done on your computer is by modifying the hosts file. If that file contains bogus entries then some program has tried to perform pharming on your computer. Some site blocking software use the hosts file to map addresses to localhost. Hence, if a web address is being mapped to anything other than 127.0.0.1 (IPv4 loopback address) or ::1 (IPv6 loopback address) in the hosts file, it's indicative of pharming.

SUCCESION OF A PHARMING ATTACK



PHARMING PREVENTION

- Ensure you are using secure web connections (look for https in the web address)
- Be cautious when opening links or attachments that you weren't expecting or that are from an unfamiliar sender
- Avoid suspicious websites
- Enable two-factor authentication on sites
- Security software should be regularly updated
- Regular antivirus checks and anti-spyware software should be installed.
- The default passwords of the router should be changed.



TECH 05 HACKING

Hacking is unauthorized access to any digital medium for some illicit purpose such as digital financial fraud, cyber blackmailing, cyber harassment, cyber defamation and identity theft etc. Hacking is done by cracking the passwords or installing malicious softwares or by collecting confidential information of user from online sources. Hacking is done through social engineering techniques to get the confidential information from user or Installing virus to gain access to email account/smart phone/computer or Installing keylogger/monitoring software through sending email containing software link to record keystrokes made by a user.

MOTIVES OF HACKING ATTACKS

Broadly speaking, hackers attempt to break into computers and networks for any of four reasons.

- i. There's criminal financial gain, meaning the theft of credit card numbers or defrauding banking systems.
- ii. Next, gaining street cred and burnishing one's reputation within hacker subculture motivates some hackers as they leave their mark on websites they vandalize as proof that they pulled off the hack.
- iii. Then there's corporate espionage, when one company's hackers seek to steal information on a competitor's products and services to gain a marketplace advantage.
- iv. There's even another category of cybercriminals: the hacker who is politically or socially motivated for some cause. Such hacker-activists, or “hacktivists,” strive to focus public attention on an issue by garnering unflattering attention on the target usually by making sensitive information public.

HACKING PREVENTION

- i. Don't access personal or financial data with public Wi-Fi.
- ii. Turn off all programmes you don't need.
- iii. Use a password, lock code or encryption.
- iv. Make sure your data is secure if your mobile device is stolen or lost. You can set up your device to reset itself after a pre-set number of failed log-in attempts.
- viii. Restrict settings on social media profiles.



TECH 06 SOCIAL ENGINEERING

Social engineering scammers are looking for the right target and the right emotional trigger. Social engineering is a technique used by cyber criminals to get access to confidential information. With social engineering, attackers use manipulation and deceit to trick victims into giving out confidential information.

Some of the social engineering methods used by attackers:

- i. Sending messages that contain dangerous attachments (e.g. malware) with text that encourage people to open the attachments.
- ii. Pretending to be the main administrator of a local network and asking for the victim's password in order to perform a maintenance check.
- iii. Telling a victim over the phone that he/she has won a prize, in return they ask for a credit card number to deliver it.
- iv. Asking for a user's password for a certain Internet service, such as a blog, and later use the same password to access user's computer. This technique works because users often use the same passwords for many different portals.

“

If cybercriminals use malware and computer viruses to hack our computers, then social engineering is how they hack our minds.”

SOCIAL ENGINEERING PREVENTION

- i. Turn your spam filter on
- ii. Learn how to spot phishing emails
- iii. Turn macros off
- iv. Use multi-factor authentication
- vi. Do not share your personal information publicly.
- viii. When any Facebook, Instagram or any other social platform link requires a person to log in with personal credentials, it is advised to enter fake credentials to view the response of the web page.

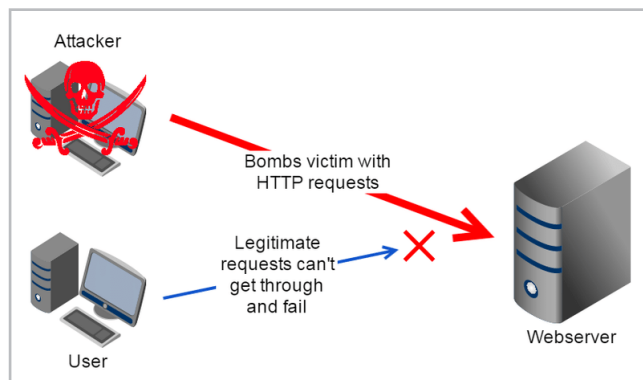
TECH 07

DENIAL OF SERVICE (DOS) ATTACK

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. It is also known as a network saturation attack or bandwidth consumption attack. Using modern security technologies to defend against most forms of DoS attacks. The motivations behind attacking a website or service vary. Hactivists will use a DDoS to make a political statement against an organization or government. There are criminals who do it to hold a commercial website hostage until they receive a ransom payment. Unscrupulous competitors have employed a DDoS to play dirty against rival companies. Sometimes, a DDoS is also a strategy to distract website administrators, allowing the attacker to plant other malware such as adware, spyware, ransomware, or even a legacy virus.

Effects of a DoS/DDoS include:

- Disappointed users who may never return
- Data loss
- Loss of revenue
- Compensation of damages
- Lost work hours/productivity
- Damage to the business's reputation



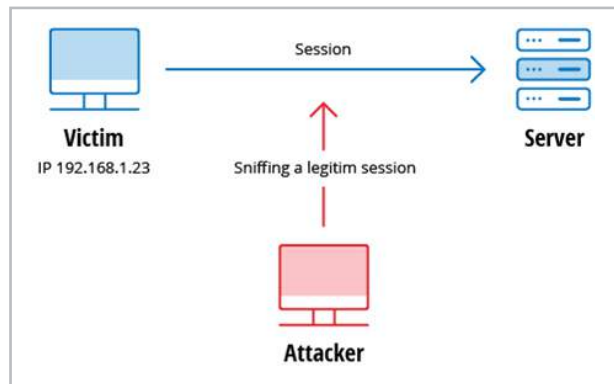
DOS / DDoS PREVENTION

- i. Don't keep passwords written on notes on desks or monitors
- ii. Change passwords on IoT devices
- iii. Lock your computer when stepping away
- iv. Log off at the end of the day
- v. Don't reveal your login credentials to anyone
- vi. To avoid becoming an unwilling and unwitting participant in a botnet-fueled DDoS, practice the same good computer hygiene for preventing all malware infections: keep your operating system and apps up to date, and don't click on unknown links and unexpected attachments.
- vii. Regularly check resources being used with the help of the task manager.

TECH 08 MAN-IN-THE-MIDDLE ATTACK (MITM)

A Man-in-the-middle (MITM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use man-in-the-middle attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

MITM encompass a broad range of techniques and potential outcomes, depending on the target and the goal. For example, in SSL stripping, attackers establish an HTTPS connection between themselves and the server, but with an unsecured HTTP connection with the user, which means information is sent in plain text without encryption. Evil Twin attacks mirror legitimate Wi-Fi access points but are entirely controlled by malicious actors, who can now monitor, collect or manipulate all information the user sends.



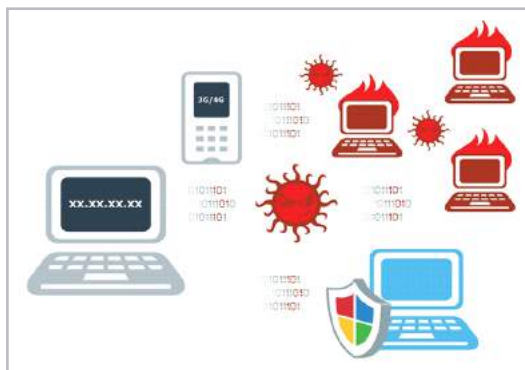
MITM PREVENTION

- i. Strong WEP/WAP encryption on access points
- ii. Strong Router Login Credentials
- iii. Use of Virtual Private Network
- iv. Public Key Pair Based Authentication
- vi. Refrain from using the free Wi-Fi at public places
- vii. Use the latest version of high-security web browsers
- viii. Regular firmware update should be done
- x. Use end-to-end encryption for your emails, chat, and video communication (Zoom, Teams, etc.)
- xi. Employ DNS over HTTPS



TECH 09 COMPUTER VIRUS

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term “worm” is sometimes used to mean self-replicating “malware” (Malicious software). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate.



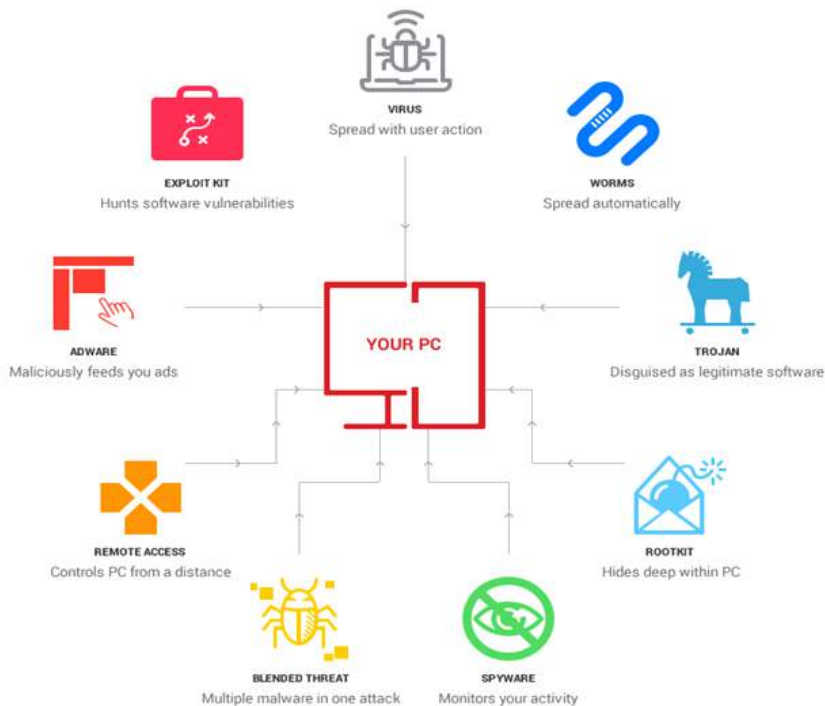
VIRUS PREVENTION

- i. Use Antivirus Software
- ii. Use a Firewall
- iii. Install a Popup Blocker
- iv. Keep Everything up to Date
- v. Beware of Email Phishing Scams
- vi. Regularly check resources being used with the help of Task Manager
- vii. Backup data regularly using external Hard Drive
- viii. Do not open email attachments or click on hyperlinks from unknown senders
- ix. Exercise caution when downloading files from the Internet. Only download from trusted sources.
- x. Do not share access to your computer with strangers and turn off file-sharing.
- xi. Avoid the use of pirated software.

TECH 10 MALWARE

Malware attacks had a devastating effect on Critical Infrastructures in 2020. With ransomware as the weapon of choice for many hackers. It's unlikely the trend will let up going into 2021. Attacks on U.S. cities in 2019, including Pensacola, Riviera Beach and Lake City, shut down public services, like government email and even emergency services.

Malware can result in data loss, cripple devices, and shut administrators out of systems in return for an oftentimes large ransom sum. Just a few examples of malicious malware include NotPetya, Stuxnet, Shamoon, and Dark Seoul.



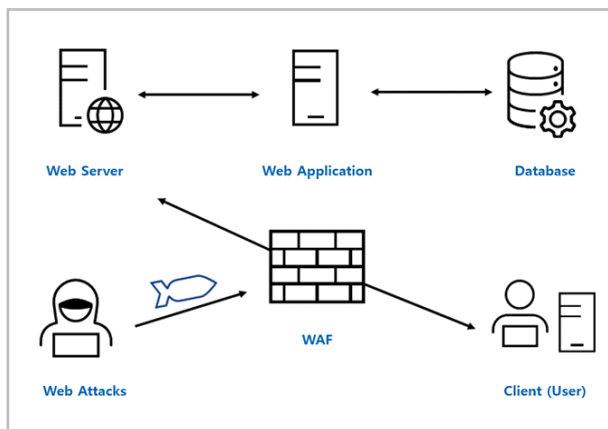
MALWARE PREVENTION

- I. Install anti-virus/malware software
- li. Keep your anti-virus software up to date
- lii. Run regularly scheduled scans with your anti-virus software
- lv. Secure your network
- v. Think before you click
- vi. Regularly check task manager to find any abnormality in the use of resources
- vii. Regularly install updates of OS



TECH 11 WEB APPLICATION ATTACK

Since traditional Operational technology (OT) systems such as human-management interfaces (HMI) and programmable logic computers (PLC) are increasingly connected to the network they are also accessible via remote access making them particularly vulnerable. Unprotected and exposed systems are vulnerable to cross-site scripting and SQL injection attacks.



WEB APPLICATION ATTACK PREVENTION

Organizations are recommended to use Content Delivery Networks (CDN) and Web Application Firewalls (WAF), as well as share crucial resources with administrators while performing regular security audits in order to identify vulnerabilities

- i. Clearing stored cookies from your browser regularly
- ii. Avoid signing up for sites and or newsletters that you don't trust
- iii. Scan your website for vulnerabilities often
- iv. Use a web application security platform
- v. Use very strong password policy in place
- vi. Secure Your Network
- vii. Think Before You Click
- viii. Make sure that the web application is secure and that the user is not able to execute any command on the server. Filter all the functions that can help the attacker execute code on the server
- ix. Use input validation and input sanitization techniques
- x. Implement weak-password checks for better password security.
- xi. Keep your applications up to date
- xii. Use anti-malware and antivirus software



Beware! Nowadays, there are some gangs active in Punjab and other provinces of the country, which often target general public or retired people, as they retire at a relatively younger age and possess cash amounts received as pension benefits and gratuities. Hence they are under a sort of compulsion to find a new job, or to invest their recently acquired pension / gratuity to a profitable venture.

A brief description of some of such frauds is given on next page.



BEWARE! BEWARE! BEWARE!



FRAUD OF SECURITY DEPOSIT

People are targeted through emails / calls or lured through advertisements on websites offering jobs with attractive perks and privileges followed by a fabricated hiring process. The fraudsters charge a nominal amount as registration and service charges. As the process continues a security deposit is demanded as surety with the condition of refund once the hiring process is completed. The deposit is never refunded nor is he ever provided any job.



FRAUD OF JOB OFFER IN FOREIGN COUNTRY

Job opportunities in foreign countries are advertised through social media or newspapers. A nominal amount is charged as registration fee / service charges in the beginning. After a fake process of job interview and scrutiny of papers, victim is informed of his selection and his passport details are taken. Later he is advised to transfer money for medical and afterwards for visa and passport processing. This process of money extraction on one pretext or the other continues till the victims stop paying any more. After some time, the company closes their office and vanishes.



FAKE CURRENCY MAKING MACHINE FRAUD

The victim is lured under the pretext of investment opportunities of good profit margin in some businesses. After gaining his confidence, a drama is created in front of him in which a person claims that he has spent his life savings and efforts in developing a fake currency making machine. A demo is demanded in which he makes them believe that the machine can make currency notes which are not differentiable from original notes. Victim is persuaded to invest in making fake currency notes with the promise of multiplying his investment manifold as compared to any other legitimate business. Initially he is asked to invest in the ink or paper for fake currency. During the operation of the machine the victim is tricked into believing that the machine has developed a fault. So requires further amount for its repair or spare parts. To safeguard his initial investment, victim brings more money which is also looted and eventually the gang vanishes which results in the victim losing all his money.



GAMBLING FRAUD

A fraud is also committed by gambling. Through job advertisements, people are called for interviews and befriended. A group of people play cards in the office premises in the presence of the victim. In a friendly environment the target is inclined to play cards and if he agrees then they let him win in the beginning to increase his confidence and greed, this motivates him to place high bets and eventually he is somehow made to lose the game and all his money.

TRANSPORT/ AUTO MOBILE BUSINESS FRAUD



Targeting people by eye-catching investment and partnership offers in which investment money is asked for in cash and in advance, which is then taken fraudulently from individuals and later on the fraudsters disappear with all the investment. Sometimes victims are asked to provide brand new vehicles and high monthly rents are promised. Fraudsters disappear with the vehicles and victim is only left with fake stamp papers and fake agreements.

PROPERTY SALE/PURCHASE FRAUD



Land investment based on alleged attractive deals of investment are also becoming common, in which land is offered on unusually low prices with the condition that whole payment is to be made in cash immediately. After that land / property is not transferred on different excuses. Eventually fraudsters disappear with whole payment and the victim comes to know that all property documents given to him were fake.

IMPORT/EXPORT FRAUD



This fraud is perpetrated by the lure of making lucrative profits on the offer of investment in the export / import business, such as on export of goods i.e. rice or pulses etc, or the import of silk or gadgets etc. Initially, the victim invests for the purchase of goods, excuses are made about the delay of goods at different ports and more money is taken on account of duties, clearing fees, taxes etc. Eventually the fraudsters disappear with all the money and the victim is only left with fake documentation and LC's.

MOBILE PHONE TOWER INSTALLATION FRAUD



Land investment based on alleged attractive deals of investment are also becoming common, in which land is offered on unusually low prices with the condition that whole payment is to be made in cash immediately. After that land / property is not transferred on different excuses. Eventually fraudsters disappear with whole payment and the victim comes to know that all property documents given to him were fake

PRECAUTIONS

1. Do not blindly trust social media or newspaper advertisements.
2. Never give money to anyone for security or other purposes.
3. Avoid offers that seem too good to be true for e.g. a really good salary with low qualification and experience requirements, or a low-investment promising very high returns.





بینک فراڈ سے رہیں ہوشیار

الرٹ!

بینک فراڈ سے رہیں ہوشیار!

سائبر کرائم ونگ۔ ایف آئی اے، کو موصول ہونیوالی شکایات اور ڈیٹا کے مطابق کچھ جرائم پیشہ گروہ سرگرم عمل ہیں جو لوگوں کے بینک اکاؤنٹس سے مندرجہ ذیل طریقہ کار سے پیسے لوٹ رہے ہیں!



کئی دفعہ کر منلڑ ایسے کمپیوٹر سافٹ ویئر استعمال کر کے کال کرتے ہیں جس سے آپ کی اسکرین پر بینک کا نمبر یا اس سے ملتا جلتا نمبر آتا ہے، اس طرح آپ سے تمام تر معلومات لے لی جاتی ہیں، کال کیونکہ انتہائی پیشہ وارانہ انداز میں کی جاتی ہے اور بات کرنے والا اپنے آپ کو اسٹیٹ بینک کا نمائندہ یا انٹیلی جنس ایجنسی، آرمی، ایف بی آر کا افسر ظاہر کرتا ہے اس لیے بھی لوگ اپنی حساس معلومات فراہم کر دیتے ہیں دوران گفتگو آپ کو یہ بھی کہتا ہے کہ ”ہمارا سسٹم ڈاؤن ہے اگر یہ کال منقطع ہو گئی تو میں آپ کو اپنے نمبر سے کال کر کے باقی اکاؤنٹ سیکیورٹی پر اسس مکمل کر لوں گا“

آپ کے نمبر پر بینک کی ہیلپ لائن سے ملتے جلتے نمبر سے ایک کال آئے گی جس میں کہا جائے گا۔

”میں آپ کے بینک کا نمائندہ بات کر رہا ہوں بعض اوقات وہ سٹیٹ بینک یا کسی انٹیلی جنس ایجنسی کا نمائندہ یا فوجی افسر بن کر بات کر رہے ہوتے ہیں (بڑھتے ہوئے فراڈ کے پیش نظر بینک نے تمام کسٹمرز سے ری-ویریفیکیشن کا سلسلہ شروع کیا ہے۔ یہ سہولت تمام کسٹمرز کے بینک اکاؤنٹ کی سیکیورٹی بہتر بنانے کے لیے فراہم کی جارہی ہے اس کے لیے آپ سے کچھ معلومات درکار ہوگی۔



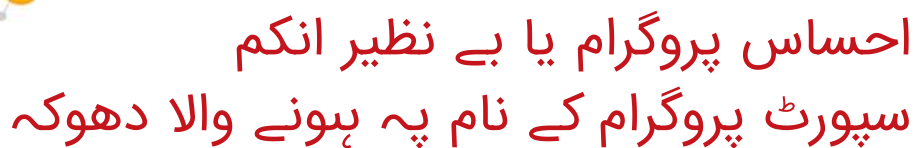
یہ سب باتیں وہ اتنے اعتماد سے کرتے ہیں کہ ہمیں پتہ ہی نہیں چلتا کہ کوئی فراڈ ہونے والا ہے۔ تمام انفارمیشن حاصل کر لینے کے بعد یقین دہانی کروائی جاتی ہے کہ ”اب آپ کا اکاؤنٹ مکمل طور پر سیکیور ہے!“

جیسے ہی کام منقطع ہوتی ہے آپ بہت بڑے فراڈ کا شکار ہو چکے ہوتے ہیں کیونکہ آپ کو بینک اکاؤنٹ سے مختلف انجانے اکاؤنٹس میں پیسے ٹرانسفر ہونے کے میسج وصول ہوتے ہیں، نہ صرف بزرگ و کم تعلیم یافتہ فرد بلکہ باشعور اور پڑھے لکھے خواتین و حضرات بھی اس فراڈ کا شکار ہو رہے ہیں۔

احتیاطی تدابیر: اپنے اکاؤنٹ کی تفصیل فراہم کرنے سے پہلے کال منقطع کر کے خود اپنے بینک کال کریں اور تصدیق کر لیں کیا واقعی آپ کے بینک نے کوئی ”ری۔ویرفیکیشن“ کا سلسلہ شروع کیا ہے یا نہیں! یاد رکھیں اگر بینک نے ویرفیکیشن کا سلسلہ شروع کیا بھی ہے تب بھی کوئی بینک بذریعہ کال آپ سے مندرجہ ذیل تفصیلات حاصل نہیں کرتا اور نہ ہی آپ کو یہ معلومات کسی بھی حالت میں کسی بھی مجاز یا غیر مجاز شخص کو دینی چاہیے۔

1۔ پن کوڈ 2۔ اے ٹی ایم ATM کارڈ کے آخری 4 نمبر

3۔ او ٹی پی OTP 4۔ تین ہندسوں والا کوڈ



یہ پیغامات کچھ اس طرح ہوتے ہیں کہ ”مبارک ہو! احساس پروگرام کے تحت آپ 12000 یا مختلف رقم کے حقدار ہیں اپنی رقم حاصل کرنے کے لیے ☆☆☆☆☆☆☆033 پر رابطہ کریں“

یاد رکھیں!

اس طرح کے پیغامات سراسر جعلی اور جھوٹ پر مبنی ہیں۔

محتاط رہیں! محفوظ رہیں!

شکر

محتاط رہیں۔ موبائل کیش اکاؤنٹ فراڈ

جرائم پیشہ افراد کے فراڈ کے مختلف طریقہ کار

طریقہ نمبر ۱

آپ کو ۸۵۵۸ یا ایسے ہی کسی نمبر سے ایس ایم ایس آئے گا جس میں رقم کی ترسیلات لکھی ہوگی اور ساتھ ہی ایک نمبر سے کال آئے گی جس میں ایک شخص آپ سے مخاطب ہو کر کہے گا کہ

آپ کے اکاؤنٹ میں غلطی سے پیسے ٹرانسفر ہو گئے ہیں، برائے مہربانی مدد کریں جس پر وہ آپ کی بات دکاندار سے کروائے گا، جو آپ کو یقین دہانی کروا کر کہے گا کہ آپ کو کچھ دیر میں اس موبائل بینک سے ایسی ایم ایس آئے گا آپ اس میسج میں آنے والے ۴ ہندسوں کے کوڈ کو ہمیں بتادیں تاکہ ہم اس کا نمبر دوبارہ درس کر سکیں اس طرح آپ کے اکاؤنٹ سے رقم آسانی منتقل کر لی جائے گی۔



طریقہ نمبر ۲

اس فراڈ میں آپ کو ایک انجان شخص کال یا ایس ایم ایس کے ذریعے رابطہ کر کے بتائے گا کہ

، وہ ایزی پیسہ کمپنی / جیز کیش کا نمائندہ ہے اور آپ کا کیش اکاؤنٹ بلاک کر دیا گیا ہے، اگر آپ اپنا اکاؤنٹ دوبارہ استعمال میں لانا چاہتے ہیں، تو دی گئی ہدایت پر عمل کریں۔ آپ کا اکاؤنٹ بحال کر دیا جائے گا

آپ کے اکاؤنٹ تک رسائی حاصل کرنے کے لیے یہ جعلی نمائندہ آپ سے آپ کے اکاؤنٹ کی حساس معلومات جیسے پین کوڈ وغیرہ پوچھے گا۔ اس کوڈ کو حاصل کرنے کے بعد یہ جلساں آپ کے اکاؤنٹ سے رقم آسانی منتقل کر سکتا ہے۔





طریقہ نمبر ۳

اس قسم کے فراڈ میں آپ کو ایک جعلی میسج موصول ہوگا جس میں لکھا ہوگا کہ معزز صارف موبائل کیش اکاؤنٹ کی جانب سے ایک انعامی سکیم کی قرعہ اندازی میں آپ کا نام نکلا ہے اور آپ انعام کے حقدار ٹھہرے ہیں۔ انعام کی تفصیل کے لیے دیے گئے نمبر پر رابطہ کریں یا لنک کو کلک کریں



جس کے ذریعے آپ سے آپ کی تمام حساس معلومات بذریعہ کال یا لنک حاصل کر لی جائیں گی اور آپ کے موبائل اکاؤنٹ سے رقم لوٹ لی جائے گی۔

گزارش ہے کہ ایسی فراڈ فون کال سے ہوشیار رہیں، اپنے آپ کو محفوظ رکھیں اور اپنی حساس معلومات فراہم نہ کریں۔

گزارش ہے کہ ایسی فراڈ فون کال سے ہوشیار رہیں، اپنے آپ کو محفوظ رکھیں اور اپنی حساس معلومات فراہم نہ کریں۔



CYBER CRIME WING TEAM

DIRECTORS



Mr. Muhammad Jafer (PSP)
Director (Administration)
Cybercrime - FIA



Mr. Babur Bakht Qureshi (PSP)
Director (Operations),
Cybercrime - FIA

ADDL. DIRECTORS CYBERCRIME - FIA



Ms. Sumera Azam (PSP)
Addl. Director
(Administration)
Cybercrime - FIA



M. Abdul Qadir Qamar (PSP)
Addl. Director
(Operations)
Cybercrime - FIA



Imran Riaz (PSP)
Additional Director
FIA Cyber Crime Zone
Sindh



Syed Shahid Hassan
Additional Director
FIA Cyber Crime Zone
Lahore



CONTACT US

For any help related to Cybercrime, dial cyber helpline 1991.

Online complaint may be lodged through email at: helpdesk@nr3c.gov.pk

Complaint may also be lodged by visiting any of the following Cyber Crime Reporting Centers.

| No | Name | Address | Contact |
|----|-----------------------|--|---------------|
| 1 | Cyber Crime Wing HQ | 2nd Floor, National Police Foundation Building, Mauve Area, Sector G10/4, Islamabad, Pakistan | 051 9106384 |
| 2 | CCRC Islamabad | Street 169, Building 5/C, G13/3, Islamabad | 051 92621068 |
| 3 | CCRC Rawalpindi | The Professionals Plaza, 7A West Service Road New Gulzar E Quaid, Rawalpindi | 051 9330719 |
| 4 | CCRC Abbottabad | House No 3, Street No 1 Mosazai Colony, Mirpur Mansehra Road (K.K.H), Abbottabad | 0992384148 |
| 5 | CCRC Peshawar | Opposite RMI Hospital Hayatabad, PhaseV, Peshawar | 0919219565 |
| 6 | CCRC Dera Ismail Khan | Sohna Khan Street (3rd House on the left from Indus View Road) Near Dera Board, Dera Ismail Khan | 096 6852945 |
| 7 | CCRC Gilgit | Mehboob Manzil No06, Near CM Secretariat Chinar Bagh, River Road, Gilgit | 05811 960707 |
| 8 | CCRC Lahore | 8 B, G Block, GulbergII, Lahore | 042-99268527 |
| 9 | CCRC Faisalabad | Zia Town, Street No 2, East Canal Road, Near Kashmir Pul (Opposite Gohar Textile), Faisalabad | 041 9330865 |
| 10 | CCRC Gujranwala | Ghaus Plaza, Commercial Area, City Housing Society Lahore Road, Gujranwala | 0559330015-16 |
| 11 | CCRC Multan | H.06, Street3 Shalimar Town Bosan Town, Multan | 061-9330999 |
| 12 | CCRC Sukkur | House No A-126, Sindh Housing Society, Near NADRA Office, Airport RoadSukkur | 071 9310849 |
| 13 | CCRC Hyderabad | Plot A-100, Site Area near Custom House Hyderabad | 022 9250010 |
| 14 | CCRC Karachi | Near Darul Sehat Hospital Gulistan-e-Johar Karachi | 021-99333950 |
| 15 | CCRC Quetta | FIA Office Bungalow 105 , Shabo Road Quetta | 081 2870057 |
| 16 | CCRC Gwadar | Near Fish Harbor Rest House Gwadar | 03322400190 |



CYBER CRIME WING

FEDERAL INVESTIGATION AGENCY

Ministry of Interior, Government of Pakistan

2nd Floor, National Police Foundation Building, Mauve Area,
G-10/4, Islamabad. Ph: +92 51 9106384 Email: helpdesk@nr3c.gov.pk

www.nr3c.gov.pk