

Performance Bulletin Jan - Dec, 2020

CYBER CRIME WING FIA

- **Mandate of Cyber Crime Wing**
- **Overview and Performance**
- **Major Initiatives**
 - Administrative
 - Operational
- **Awareness Campaign**

02

Note of Thanks

03

Mandate of CCW, FIA

04

**Zones and CCRC's
of CCW**

05

**Overview and
Performance**

06

**Major Initiatives
Administrative**

15

**Major Initiatives
Operational**

19

Public Awareness

CONTENTS

NOTE OF THANKS



Mr. Shaikh Rasheed
Interior Minister of
Pakistan



Mr. Imran Khan
Prime Minister of
Pakistan



Mr. Wajid Zia
Director General (DG)
Federal Investigation
Agency

“Upholding the vision of Government of Pakistan, Cybercrime Wing (CCW), FIA took numerous administrative and operational measures to resolve huge number of complaints following Prevention of Electronic Crime Act (PECA) 2016.

Progressing with the aim of curbing cybercrimes and providing maximum relief to victims, CCW received 84764 complaints in year 2020. This upsurge of complains shows rapid increase in digital crimes, nevertheless it reflects the trust and reliance of public on CCW, FIA

In year 2020 a special focus was placed on administrative and structural reforms as well as capacity building which resulted in operational excellence and improved public perception.

In this regard we owe special thanks to Mr. Wajid Zia DG FIA and Mr. Ehsan Sadiq ADG CCW for their continuous guidance and support, which led to strict internal accountability and close monitoring.

”

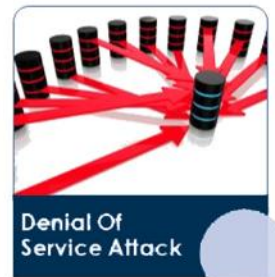
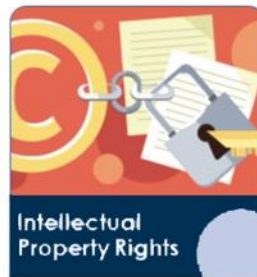
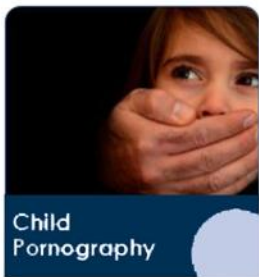
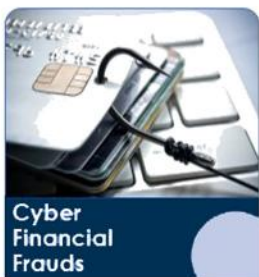
Mr. Muhammad Jafer
(PSP)
Director CCW

Mandate of Cyber Crime Wing, FIA

Cyber Crime Wing of Federal Investigation Agency, is guided by laws under Prevention of Electronic Crimes ACT (PECA) 2016, which deals with the growing threat of cybercrimes. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society. It is the only unit of its kind in Pakistan which directly receives complaints and take legal measures against cyber criminals.

CCW has expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and Trainings. The unit since its inception has been involved in capacity building of the officers of Police, Intelligence, Judiciary, Prosecutors and other Govt. organizations.

With the aim to achieve excellence by promoting culture of merit, enforcing technology based law, and extending continuous professional services, following are some of the major Cyber Crimes catered by CCW:



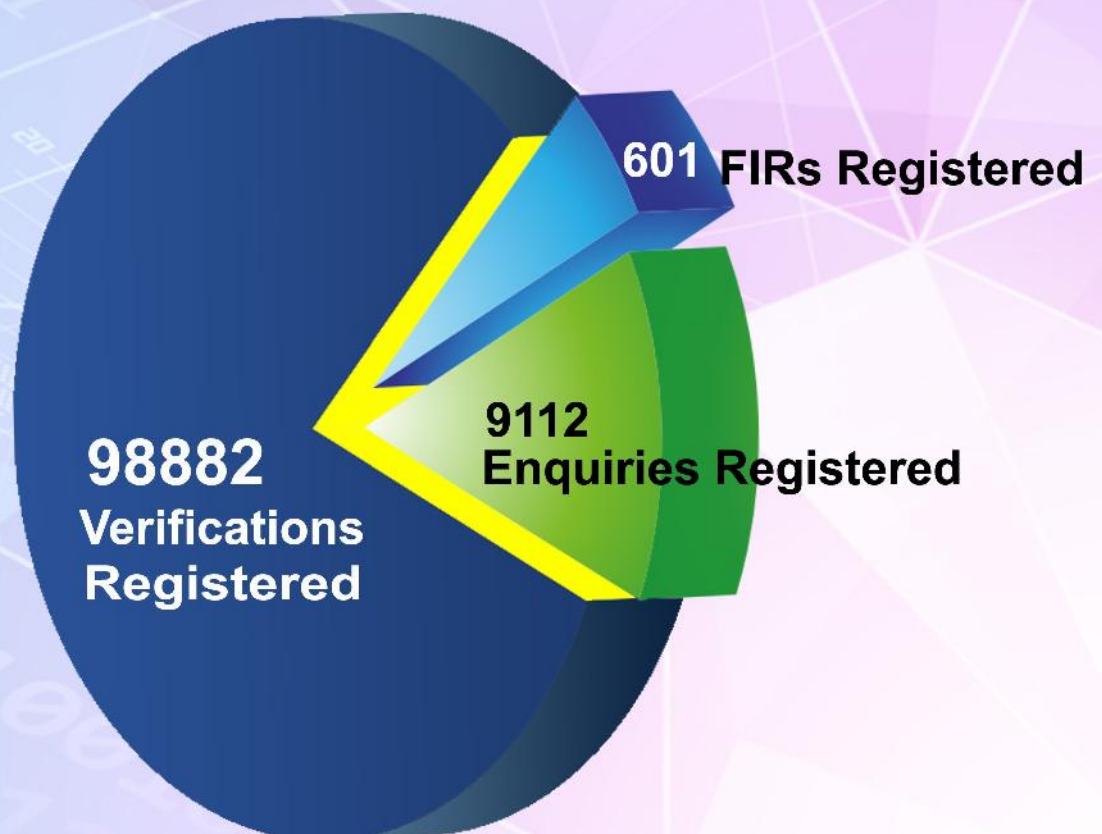
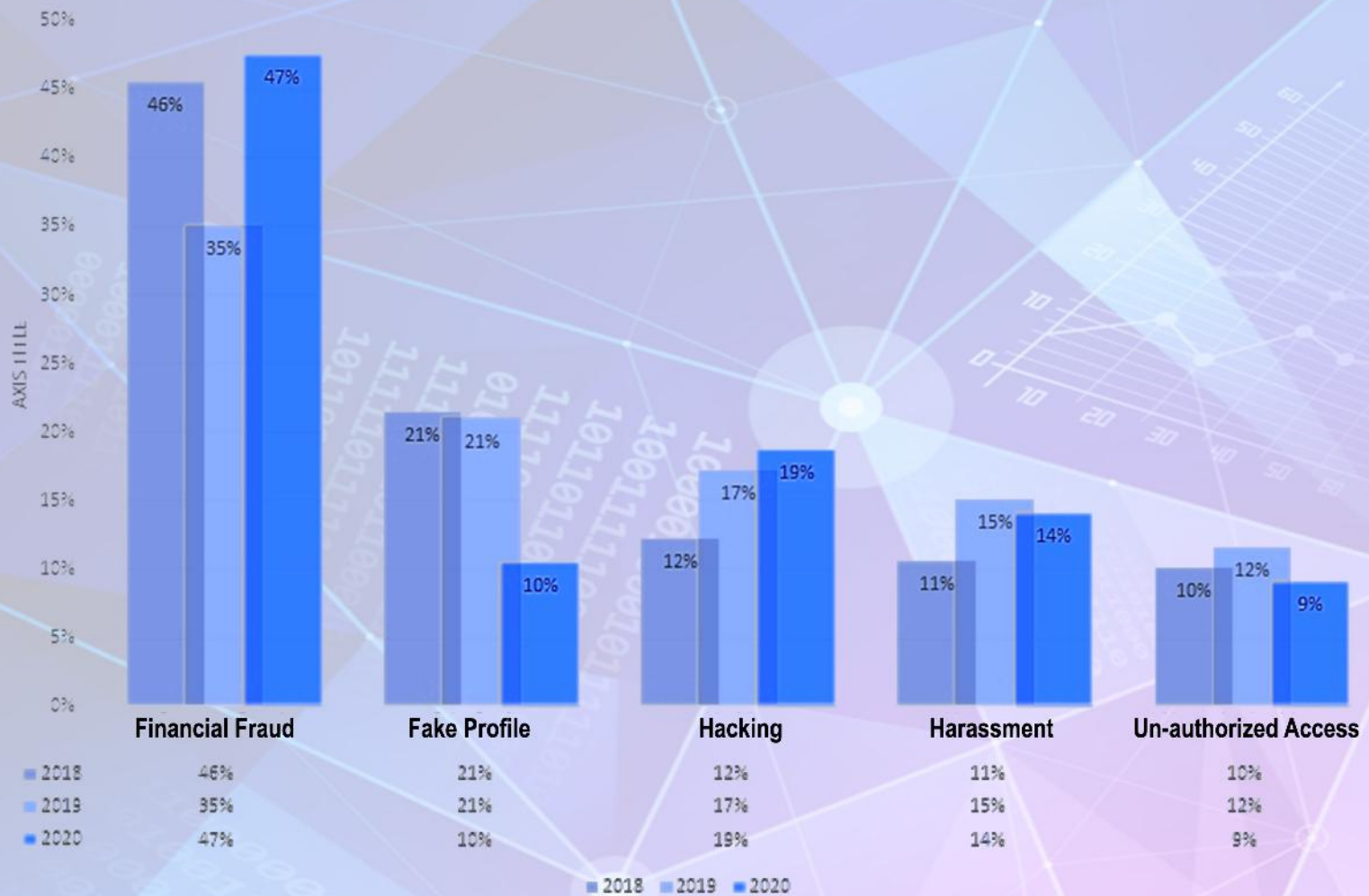
ZONES AND CCRC's OF CCW

As per survey record there are 76.3 million Internet users in Pakistan which are increasing on daily basis. This increased the risk of Cybercrimes as well. In this context, to combat cybercrimes efficiently Cyber Crime Wing, FIA extended its services in 6 zones through 15 Cyber Crime Reporting Centers (CCRC's).

Each circle is operating with competent staff, under supervision of Circle Incharge and Zonal Additional Director.



OVERVIEW AND PERFORMANCE



MAJOR INITIATIVES: Administrative

01

NEW RECRUITMENT

As a major leap towards strengthening of Cybercrime Wing, FIA, 363 personnel (including the Investigators and Technical experts) have been recruited against various posts of NR3C Project (Phase-III) in January – February 2020.



MAJOR INITIATIVES: Administrative

02

COMMON AND SPECIALIZED TRAININGS

Common Training Program

Common Training Program for the newly recruited 363 personnel of NR3C Phase III was carried out in January, 2020.

During the CTP, the most senior and experienced officers of FIA were involved who imparted excellent knowledge and skills to the trainee officers.



Specialized Training Program

As a result of special efforts of Additional Director General and Director CCW, Specialized Training Program for the newly recruited employees was organized from the most prestigious training institutions of the country. The institutions involved for STP were:

- i. National Police Academy for Investigators (BPS 17 and above)
- ii. Police Training College Sihala as well as Police Training College Choung for Inspectors, SIs, and ASIs
- iii. FIA Training Academy for HCs and Constables.
- iv. CCW- HQ for Forensics and Technical experts



MAJOR INITIATIVES: Administrative

03

Restructuring of HQ, Zones & CCRCs

Restructuring of CCW-HQ, Zonal offices and CCRCs, has been done with a view to improve the overall efficiency of Cybercrime Wing-FIA. Some major sections have been established at CCW HQ

CRIME CELL

MEDIA CELL

**ANTI WOMEN HARASSMENT
CELL**

ANTI CHILD PORNOGRAPHY CELL

**INTERNAL ACCOUNTABILITY
UNIT**

**INTERNATIONAL COOPERATION
SECTION**

New Building for CCRC



MAJOR INITIATIVES: Administrative

04

First Ever National Seminar on Digital Forensics

Cybercrime Wing of FIA took lead in organizing the first National Seminar on Digital Forensics in February, 2020.

The event was attended by the academicians, leading researchers, eminent scholars, industry experts, members of law enforcement agencies and representatives from NAB, NFSA, PFSA and NUST.

This national level platform provided a great opportunity for the fertile brains to group together to analyse the existing capacity in digital forensics and to devise a comprehensive strategy for enhancing the indigenous capacity in digital forensics in order to combat cybercrime in an efficient manner.

As a result of this collaboration and continued follow-up, Air University has recently developed valueable software tools for Cyber Crime Wing FIA.



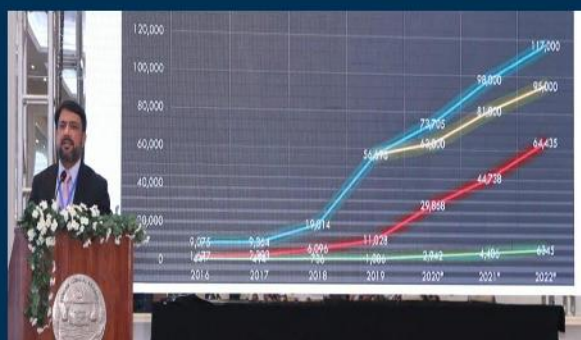
MAJOR INITIATIVES: Administrative

05

Seminar on Cyber Laws by Punjab Academy Lahore

Director CCW delivered a much appreciated lecture in a seminar on Cyber Law, organized by Punjab Judicial Academy with the collaboration of UK High Commission, in Lahore with Honorable Chief Justice of Pakistan as the chief guest.

Role of Cyber Crime Wing, FIA was highlighted by Director CCW. Recent reforms and initiatives were also discussed in this seminar.



06

First National Seminar on Cyber Financial Crimes



Cyber Crime Wing FIA organized first National Seminar on Cyber Enabled Financial Crimes in FIA (Headquarters) Islamabad.

Representatives from Banks, Mobile Financial Institutions, State Bank of Pakistan, PTA, FMU, and Cellular Companies participated and discussed the various aspects of cyber enabled financial Crimes in Pakistan.

MAJOR INITIATIVES: Administrative

07

Effective Liaison of CCW-FIA with Facebook

Cyber Crime Wing FIA has made an important breakthrough towards eradicating cybercrimes on social media as with continuous efforts of Director CCW Mr. Amir Farooqi, Facebook management agreed to share data with FIA Cyber Crime Wing and inked an agreement.

According to agreement Facebook will share user's platform data with CCW officials to investigate and eliminate the increased cybercrimes from the country.

This initiative will help CCW in protecting the digital world and restrict the freedom of cyber criminals.

To expedite the cybercrime investigation, Facebook technical expert's team also synchronized with Pakistan's ambition.

Before the access, there were many cases which could not be processed or were disposed off due to lack of sufficient evidences.



But with the latest development, the FIA cybercrime wing can have access to millions of databases, which can be used to conclude the case early.

After signing of the data sharing agreement, on Facebook requested from the authorities in the cybercrime wing to place representatives who would contact Facebook and forward data sharing requests directly.

The CCW's focal person would request information from Facebook in cases of cyber crimes against children and women. Furthermore, Facebook also extended its cooperation by offering data sharing agreement regarding WhatsApp and Instagram.

08

Webinar on Cyber Harassment Under the Shadow of Corona: Incidence, Control and Punishment

Additional Director General Cyber-crime Wing (CCW) FIA, Dr. Ehsan Sadiq spoke as the Guest of Honour at the “Cyber Harassment under the Shadow of Corona: Incidence, Control and Punishment” webinar.

Conducted by the “National Initiative Against Organized Crime”, the webinar was the first-ever initiative in Pakistan launched by a group of committed professionals and experts with law enforcement, media and other public service backgrounds.

Highlighting the progressively important role of Cybercrime Wing FIA, Dr. Ehsan Sadiq shared the different initiatives taken by CCW to counter the growing menace of cybercrime.

 National Initiative against Organized Crime Pakistan
Roundtable on
**Cyber Harassment under the shadow of Corona:
Incidence, Control and Punishment**
Online Webinar
June 18, 2020 | 5:00 pm

Guest of Honour


Ehsan Sadiq
Additional Director General
Cyber Crime Wing FIA

Panelists


Farieha Aziz
Journalist & Co-founder of Bolo Bhi


Ammar Jaffri
Director General
Center of Information Technology (CIT)


Nighat Dad
Executive Director, Digital Rights Foundation


Fasi Zaka
(Moderator)
Public policy communications expert

MAJOR INITIATIVES: Administrative

09

Collaboration with Multiple National and International Organizations

Liaison with different NGOs is developed to mitigate Cyber Harassment collaboratively.

Multiple meetings were arranged with Nighat Dad CEO Digital Rights Foundation to discuss Legal complexities related to cybercrime.

Webinars in context of Awareness campaign of Cybercrime Wing – FIA were also organized with Fozia Tariq CEO of Law is My Protector in regard of Cybercrime Unit Challenges and Prospects.

Online Seminar with Qaisera Sheikh Vice President of Cyber Arm and Karachi Women's chamber also took place. It was organized to facilitate and aware women to discuss harassment issues they face on social media etc.

Team CCW, suggested to refer cybercrime related complaints to CCW and assured that complaints related to female harassment and blackmailing are and shall remain one of the top priorities of Cybercrime Wing FIA.

FIA CYBER CRIME UNIT CHALLENGE AND PROSPECTS



Host
Fozia Tariq

Saturday 19 Sep 2020

9 PM



Exclusive Interview

Law Is My Protector

Guests



Ms. Zooni Ashfaq
Assistant Director
CCW- FIA



Mr. Najeeb Ul Hassan
Cyber Crime Analyst
CCW – FIA

MAJOR INITIATIVES: Administrative

10

Initiative by Cybercrime Wing to Incorporate Cybercrime awareness in the Curriculum

With a vision of Single National Curriculum, Cyber Crime Wing FIA stood up to add cyber security related knowledge in curriculum to make Pakistani nation cyber-wise.

Cybercrime Wing- FIA, took the innovative initiative of adding cyber security related guidelines in narrative form in reference to make the content child sensitive and age related.

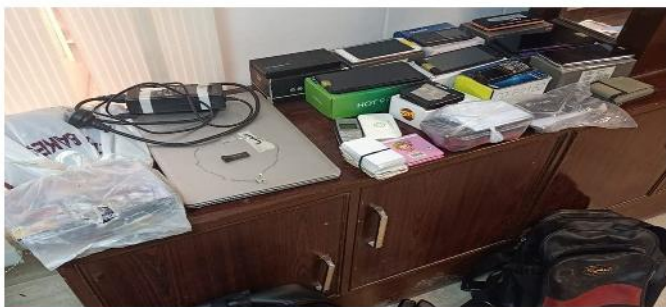
In this regard, meetings were arranged with the Curriculum team of National Curriculum Council. This proposed curriculum was presented in four committees of National Curriculum Council namely English, Urdu, Social Studies and Computer.

First Phase of single national curriculum for Primary School is prepared to be functional from academic year 2021. However team CCW is on way to inculcate cyber knowledge in second phase of curriculum preparation for secondary classes.



MAJOR INITIATIVES: Operational

GANG INVOLVED IN SELLING CALL RECORD DETAILS AND HACKING EMAIL ACCOUNTS OF POLICE OFFICERS BUSTED.



Cyber Crime Reporting Center Peshawar took strict actions against the gang by conducting immediate enquiry. This gang was facilitating criminals to lure people by Hacking, selling of CDR, family tree and other information. During initial examination of the mobile phones seized from the alleged revealed that CDR, ownerships and NADRA records are being sold on WhatsApp. Culprits admitted during interrogation that they have hacked email accounts of officers of Punjab Police to gain access to data from mobile companies.

GANG INVOLVED IN ACTIVATION OF ILLEGAL SIMS BY USING SILICON THUMBS BUSTED

In Gujranwala Circle of Cybercrime, A secret piece of information was received that illegal SIMs are being activated using fake silicon thumbs in Hafizabad based UFone Franchise. The requisite on ground evidences were collected and matter was taken up with Directorate of Enforcement, PTA and mandatory complaint under the law was obtained.

During the search operation 2000 fake silicon thumbs, 3000 activated illegal SIMS, 04 cell phones, 50 BVS machines, 03 Desktop Computers containing database of thumbs of innocent citizens with other allied equipment was confiscated. FIR against four persons were registered after their arrest.



MAJOR INITIATIVES: Operational

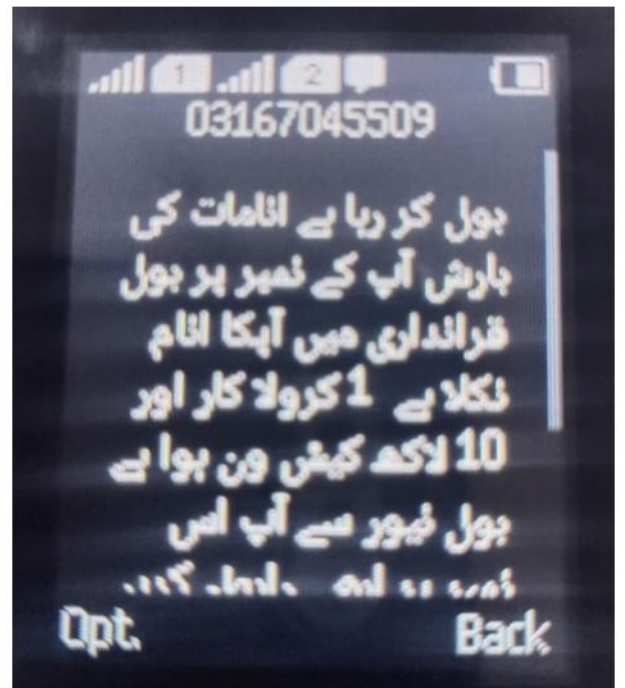
بچوں کی نازیبا اور غیر اخلاقی تصاویر بنانے اور نشر کرنے والے ملزمان ویڈیوز سمیت گرفتار



سائبر کرائم رپورٹنگ سنٹر، اسلام آباد، کراچی اور راولپنڈی میں مقدمات درج۔ ملک میں بڑھتے ہوئے بچوں پر جنسی تشدد کے واقعات کے تناظر میں ایف آئی اے سائبر کرائم ونگ نے اٹھارہ (18) سائبر ٹپ لائن رپورٹس کا تکنیکی تجزیہ کرتے ہوئے ملزمان کو گرفتار کیا۔ ملزمان نے غیر قانونی اور غیر اخلاقی فیس بک اور واٹس ایپ اکاؤنٹس / گروپس بنائے ہوئے تھے جن کا مقصد سوشل میڈیا پلیٹ فارمز پر سرعام نابالغ اور کمسن بچوں کی فحش اور غیر اخلاقی ویڈیوز اور تصاویر وغیرہ حاصل کرنا، بنانا، انہیں پھیلانا اور بیچنا تھا۔ پاکستان میں موجود چائلڈ پورنوگرافی میں ملوث تمام گروہوں اور چینل کے خلاف سائبر کرائم ونگ ایف آئی اے کی سخت کارروائی اور کڑی نگرانی جاری ہے۔

بول نیوز اور دیگر انعامی سکیمز کے نام پر لوگوں سے لاکھوں روپے لوٹنے والا ملزمان سرگودھا سے گرفتار

ملزمان کا یہ گروہ دھوکہ دہی سے بول نیوز کا نمائندہ بن کر لائٹری فراڈ کے ذریعے لوگوں سے رقم بٹورنے کے جرم میں ملوث پایا گیا۔ بروقت کارروائی کے نتیجے میں ملزمان سے کئی موبائل فونز برآمد ہوئے۔ یہ گروہ مختلف لوگوں کو جعلی نمائندہ بن کر کال کرتا اور ان کو مختلف ریکارڈنگ اور تصاویر بھیجتا اور دھوکہ دہی سے انعام کا لالچ دے کر پروسیسنگ فیس کی مد میں رقم بٹورتا تھا۔ سائبر کرائم ایف آئی اے نے ناصرف ملزمان کو گرفتار کیا بلکہ ان کے اس طریقہ واردات کے حوالے سے سے آگاہی مہم کا بھی آغاز کیا۔



MAJOR INITIATIVES: Operational

سوشل میڈیا کے ذریعے خاتون کی تصویریں، ویڈیوز شیئر کر کے بلیک میل کرنے والے ملزم کو 7 سال کی سزا



راولپنڈی زون کی مسلسل کاوشوں کے نتیجے میں مجرم کو گرفتار کیا گیا اور اسکے قبضے سے نازیبا ویڈیوز اور تصاویر برآمد کر لی گئیں۔ مجرم کیخلاف سائبر کرائم ایکٹ کے تحت جون 2020 میں مقدمہ درج کیا گیا تھا۔ لیگل اور انوسٹی گیشن ٹیم کی مستقل نگرانی اور کورٹ کے تمام معاملات کی پیروی کے نتیجے میں مجرم کی درخواست ضمانت ہائیکورٹ سے مسترد ہوئی اور راولپنڈی کی ٹرائل کورٹ نے مجرم کو سات قید کی سزا سنائی۔

خاتون جو کہ بہت ذہنی افیت کا شکار تھیں، کو سائبر کرائم ونگ ایف آئی اے کی جانب سے انصاف فراہم کیا گیا۔

فیس بک کے ذریعے آن لائن موبائل فروخت کرنے کے فراڈ میں ملوث ملزمان گرفتار

سائبر کرائم سرکل فیصل آباد نے ملزمان کے خلاف فوری ایکشن لیتے ہوئے مقدمہ درج کیا۔ مبینہ ملزمان فیس بک پر موبائل فروخت کرنے کا جعلی اشتہار پوسٹ کر کے لوگوں سے رقم بٹورتے اور بعد میں انہیں ناقص اور ناکارہ موبائل بھجواتے دیتے۔

سائبر کرائم سرکل فیصل آباد نے کامیاب ریڈ کے دوران ملزمان کو گرفتار کر لیا ہے۔ ملزمان کے قبضے سے کئی موبائل فون برآمد ہوئے جن سے مشکوک ٹرانزیکشن کے شواہد حاصل ہوئے ہیں۔ ملزمان نے مختلف بینکوں میں 9 لاکھ روپے کھول رکھے تھے۔ ملزمان کے خلاف پریوینشن آف الیکٹرانک ٹرانزیکٹ ایکٹ اور تعزیرات پاکستان کی دفعات کے تحت مقدمہ درج کیا گیا۔



STRESS COUNSELLING SERVICES

Stress Counselling Sessions are arranged in Cybercrime Wing FIA, for females and children to help them fight the battle against cyber bullying, harassment, defamation, and child pornography. Here the victims are guided with complete procedure of case processing and they are motivated to stay consistent in case pursuance against cyber criminals. This special initiative is also taken for females to maintain their confidentiality and data secrecy. It was appreciated by female complainants who got compassionate accommodating and responsive behaviour due to female investigation officers in handling their case.



PUBLIC AWARENESS

Official Social Media Accounts of CCW

Official social media accounts have been created on Facebook, Twitter and Instagram with regular updates including awareness posts as well as posts related to the activities and achievements of CCW-FIA on daily basis. Number of followers on these social media platforms has increased by **200%** as compared to the beginning of year 2016.



CyberCrimeFIA



cybercrimewingofficial



cybercrimefia

Close Liaison with PTA for Awareness

A close liaison with PTA at the level of director CCW is being ensured for dissemination of text messages related to awareness about cybercrimes and tactics of cybercriminals.



Awareness through PSL Team

During PSL, members of the Pakistan Cricket Team were involved in the awareness campaign and their video messages were shot for dissemination on electronic media.

https://m.facebook.com/story.php?story_fbid=3240435236024681&id=150991004969135



Awareness Through PEMRA

With the motive to reach maximum public in order to make them aware about Cyber-crime Wing FIA that is specifically functional to deal cyber crimes. Social Media Team of CCW prepared awareness videos under guidance of Director Cybercrime Wing, FIA and disseminated through PEMRA.

https://m.facebook.com/story.php?story_fbid=3212969278771277&id=150991004969135&sfnsn=mo&extid=O6NjYcoA34tem26K

PUBLIC AWARENESS

Advisories

Advisories for the general public have been devised and circulated with a view to impart awareness about the modus operandi of the cybercriminals and the ways for the general public to combat the same:

- 1) Advisory for general public on cyber crime during corona emergency .
- 2) Advisory for parents and children during corona emergency .
- 3) Advisory for social media users against possible hacking of personal accounts by cyber criminals .
- 4) Advisory for female social media users regarding tactics of cyber criminals.
- 5) Advisory for recently retired army men concerning common financial frauds.
- 6) Advisory for general public regarding different types of financial frauds.
- 7) Advisory for the general public regarding "Hacking".
- 8) Advisory on World Health Organization job scam and laptop scheme scam.
- 9) Advisory on online plasma donating scam during Covid-19 .
- 10) Advisory on safe use of Social Media Platforms .

50 Real-Life Case Studies

Around 50 real-life case studies have been prepared to promote awareness and guidance among the general public about Cybercrime, Cyber security measures, Cyber risks and Cyber ethics. These real life case studies are in process of publication for the awareness of general public.

Awareness Through Leaflets

A Variety of Leaflets on cyber financial frauds, Awareness Standees regarding online banking scams and multiple cyber security based awareness banners are designed and placed at different public places.

PUBLIC AWARENESS

Ways to Secure Smartphone

Always secure your smartphone with a strong password

Ensure that your device locks itself automatically













Install security software & only download apps from approved sources

Check your apps permissions plus Don't miss operating system updates

Careful of links you receive via email or text message & turn off automatic Wi-Fi connection

When browsing or shopping on your phone (or computer), always look for "HTTPS" in the URL instead of "HTTP"



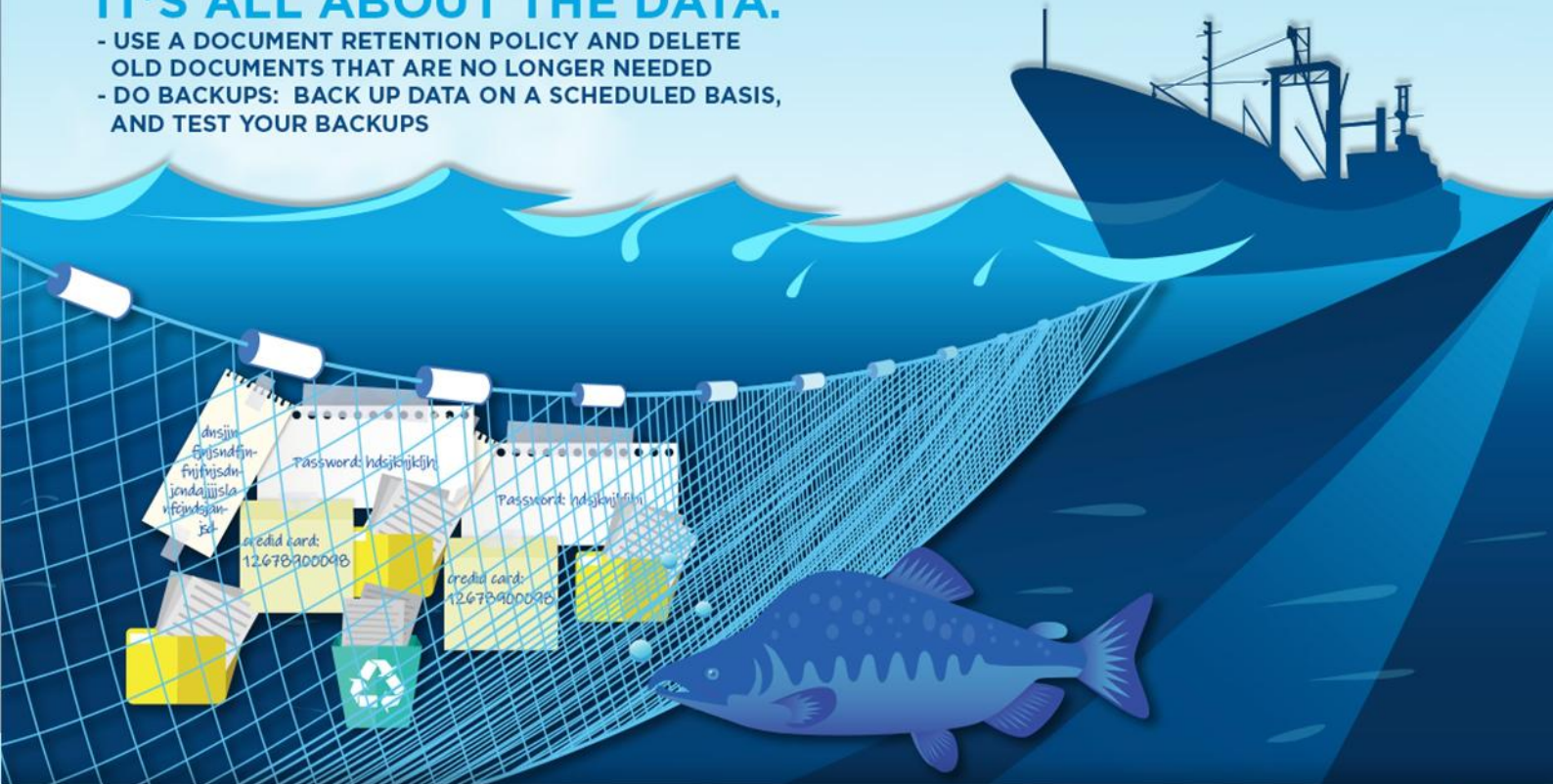
Do... 	Don't... 
use a mixture of lower and upper case letters, numbers and symbols 	use personal names or dates, repeated characters or sequences e.g. yours or your pet/ child's name 
choose a password that is at least 8 characters long 	save passwords on shared devices 
use different passwords for different sites and devices 	write your password down 
change your password immediately if you suspect it has been compromised 	use the same password for multiple accounts 
change your password regularly 	let anyone watch you type in your password 

PUBLIC AWARENESS

CLEAN UP!

IT'S ALL ABOUT THE DATA.

- USE A DOCUMENT RETENTION POLICY AND DELETE OLD DOCUMENTS THAT ARE NO LONGER NEEDED
- DO BACKUPS: BACK UP DATA ON A SCHEDULED BASIS, AND TEST YOUR BACKUPS



Ways to Secure Laptop/PC

Use different and strong passwords for different accounts.

Use Updated antivirus software and never deactivate it.

Always use updated Operating System and regularly install system updates.

Scan the USB devices before opening it.

Lock Your Computer every time you leave.

Avoid installing software from unknown sources

Ignore spam email and don't give unnecessary details in reply.

Scan your laptop Regularly for Malwares.

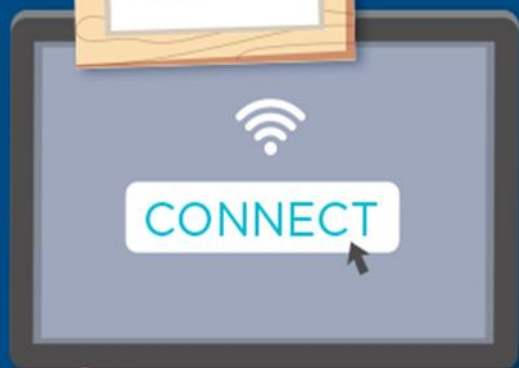
Frequently Back Up Your Data

Use Data encryption software

PUBLIC AWARENESS



QUICK TIPS



SECURITY DANGERS OF PUBLIC WI-FI

- **USE A VPN:** A VIRTUAL PRIVATE NETWORK (VPN) CONNECTION IS RECOMMENDED WHEN CONNECTING TO THE INTERNET THROUGH AN UNSECURED CONNECTION, LIKE A WI-FI HOTSPOT.
- **TURN OFF SHARING:** TURN OFF SHARING IN SYSTEM PREFERENCES OR IN THE CONTROL PANEL OF YOUR MOBILE DEVICE. OR DO IT AUTOMATICALLY BY CHOOSING "PUBLIC" THE FIRST TIME YOU CONNECT TO A NEW, UNSECURED NETWORK.
- **KEEP WI-FI OFF WHEN YOU DON'T NEED IT:** WHEN ON, THE WI-FI HARDWARE IN YOUR COMPUTER IS STILL TRANSMITTING DATA BETWEEN ANY NETWORK WITHIN RANGE. THERE ARE SECURITY MEASURES IN PLACE TO PREVENT THIS MINOR COMMUNICATION FROM COMPROMISING YOU, BUT NOT ALL WIRELESS ROUTERS ARE THE SAME, AND HACKERS CAN BE A PRETTY SMART BUNCH.

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

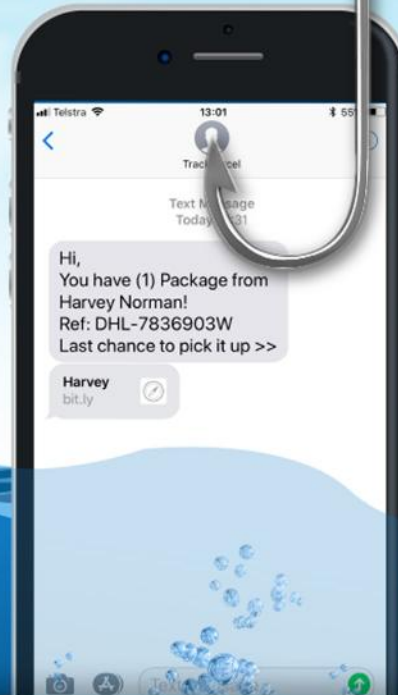
CONNECT WITH CARE



PUBLIC AWARENESS

“AVOID PHISHING ATTACKS”

VALIDATE THE URL
FOR THE WEBSITES YOU ACCESS BEFORE
PROVIDING YOUR **PERSONAL DATA**



“SMISHING” SMS-PHISHING

DELETE TEXT MESSAGES THAT ASK YOU TO CONFIRM OR PROVIDE PERSONAL INFORMATION:
LEGITIMATE COMPANIES DON'T ASK FOR INFORMATION LIKE YOUR ACCOUNT NUMBERS OR PASSWORDS BY EMAIL OR TEXT.

DON'T REPLY, AND DON'T CLICK ON LINKS PROVIDED IN THE MESSAGE: LINKS CAN INSTALL MALWARE ON YOUR COMPUTER AND TAKE YOU TO SPOOF SITES THAT LOOK REAL BUT WHOSE PURPOSE IS TO STEAL YOUR INFORMATION.

TREAT YOUR PERSONAL INFORMATION LIKE CASH: YOUR SOCIAL SECURITY NUMBER, CREDIT CARD NUMBERS, AND BANK AND UTILITY ACCOUNT NUMBERS CAN BE USED TO STEAL YOUR MONEY OR OPEN NEW ACCOUNTS IN YOUR NAME. DON'T GIVE THEM OUT IN RESPONSE TO A TEXT.

JUST A CLICK CAN SINK A SHIP

TRUST NO ONE ON SOCIAL MEDIA. DON'T ACCEPT INVITES FROM PEOPLE YOU DON'T KNOW. THEY MAY BE TRYING TO HARVEST YOUR PERSONAL INFORMATION.



PUBLIC AWARENESS



QUICK TIPS

ONLINE SHOPPING

IF A DEAL IS TOO GOOD TO BE TRUE IT PROBABLY IS

- SOME SCAMMERS USE STOLEN CREDIT CARDS TO PURCHASE PRODUCTS AND THEN RESELL THEM ON THE INTERNET.
- VERIFY E-COMMERCE SITES. LOOK AT REVIEWS, AND OTHER VERIFICATIONS.
- DON'T SET UP ACCOUNTS WITH SITES YOU RARELY USE.
- USE ESCROW SERVICES LIKE PAYPAL.
- READ SHIPPING INVOICES CAREFULLY.

90% OFF

SUPER SALE

SHOPPING SECURELY?

Use SSL security websites that begin with



https://www.|



PUBLIC AWARENESS

OPT FOR SECURE ONLINE BANKING



- 01 Never use same PIN CODE for multiple bank accounts
- 02 Never use unprotected PCs for internet banking
- 03 Never leave the PC unattended when using internet banking in a public place
- 04 Register for Mobile SMS, Email Transaction Alerts
- 05 Never reply to emails asking for your password or pin code
- 06 Log off and close your browser when you are done using internet banking
- 07 Before using ATM, make sure that there is no extra device installed in the surroundings

الرٹ! بینک فراڈ سے رہیں ہوشیار!

سائبر کرائم ونگ-ایف ائی 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!

آپ کے نمبر پر بینک کی ہیلپ لائن سے ملنے جلتے نمبر سے ایک کال آئے گی جس میں کہا جائے گا کہ "میں آپ کے بینک کا نمائندہ بات کر رہا ہوں (بعض اوقات وہ سٹیٹ بینک یا کسی انشیلجنس 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 لئے فراہم کی جا رہی ہے! اس کے لئے آپ سے کچھ معلومات درکار ہوں گی"

کئی دفعہ کر منزل ایسے کمپیوٹر سوفٹ ویئر استعمال کر کے کال کرتے ہیں جس سے آپ کی سکرین پر بینک کا نمبر یا اس سے ملتا جلتا نمبر آتا ہے۔ اس طرح آپ سے تمام معلومات لے لی جاتی ہیں، کال کیونکہ انتہائی پیشہ ورانہ انداز میں کی جاتی ہے، اور بات کرنے والا اپنے آپ کو سٹیٹ بینک کا نمائندہ یا انشیلجنس ایجنسی / آرمی ایف ائی اے کا افسر ظاہر کرتا ہے اس لیے بھی لوگ اپنی حساس معلومات فراہم کر دیتے ہیں دوران گفتگو آپ کو یہ بھی کہا جاتا ہے کہ "ہمارا سسٹم ڈاؤن ہے تو اگر یہ کال منقطع ہو گئی تو میں آپ کو اپنے نمبر سے کال کر کے باقی اکاؤنٹ سیکیورٹی پراسیس مکمل کر لوں گا"

یہ سب باتیں وہ اتنے اعتماد سے کرتے ہیں کہ ہمیں پتا ہی نہیں چلتا کوئی فراڈ ہونے والا ہے۔ تاہم تمام انفارمیشن حاصل کر لینے کے بعد یقین دہانی کروائی جاتی ہے کہ "اب آپ کا اکاؤنٹ مکمل طور پر سیکیور ہے!" جیسے ہی کال منقطع ہوتی ہے آپ بہت بڑے فراڈ کا شکار ہو چکے ہوتے ہیں۔



CCW, FIA

✉ Helpdesk@Nr3c.gov.pk ☎ +92 51 9106 384



Stay Alert
Stay Safe
1991

Cyber Crime Helpline



cybercrimewingofficial



Cybercrimefia



Cybercrimefia

احساس پروگرام یا بے نظیر انکم سپورٹ پروگرام کے نام پر ہونے والا دھوکہ

احساس پروگرام کے تحت مالی معاونت
سائبر کرائم ونگ-ایف ای اے، آپکو باور کروانا چاہتا ہے کہ احساس پروگرام
کے نام سے فراڈ پر مبنی کچھ میسج گردش کر رہے ہیں!

یہ پیغامات کچھ اس طرح ہوتے ہیں کہ "مبارک ہو! احساس پروگرام کے تحت آپ 12000 یا مختلف
رقوم کے حقدار ہیں اپنی رقم حاصل کرنے کے لیے ☆☆☆☆☆☆033 پر رابطہ کریں"
ایسی کسی بھی سکیم کا احساس پروگرام سے کوئی تعلق نہیں۔ اس فراڈ سے بے خبر افراد رقم کے حصول
کے لیے دیے گئے نمبر پر رابطہ کرتے ہیں جہاں ان سے شناختی کارڈ اور بینک اکاؤنٹ سے متعلق حساس
معلومات حاصل کر لی جاتی ہے یا انھیں رقم حاصل کرنے کے لیے رجسٹریشن فیس جمع کروانے کا کہا جاتا ہے!
اور مختلف بہانوں سے معصوم افراد کو لوٹ لیا جاتا ہے۔

یاد رکھیں!

احساس پروگرام یا بے نظیر انکم سپورٹ پروگرام کے تحت مختلف رقوم کے حوالے
سے پیغامات سراسر جعلی اور جھوٹ پر مبنی ہیں۔

مخاطب رہیں! محفوظ رہیں!
شکریہ



CCW, FIA

✉ Helpdesk@Nr3c.gov.pk ☎ +92 51 9106 384



Stay Alert
Stay Safe

1991

Cyber Crime Helpline



cybercrimewingofficial



Cybercrimefia



Cybercrimefia

مخاطب رہیں! موبائل کیش اکاؤنٹ فراڈ

جرائم پیشہ افراد کے فراڈ کے مختلف طریقہ کار

طریقہ #1

آپ کو 8558 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 ایس ایم ایس آئے گا آپ اس میسج میں آنے والے 4 ہندسوں کے کوڈ کو ہمیں بتادیں تاکہ ہم اسکا نمبر دوبارہ درست کر سکیں " اس طرح آپ کے اکاؤنٹ سے رقم باآسانی منتقل کر لی جائے گی۔

طریقہ #2

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 لئے 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 باآسانی منتقل کر سکتا ہے۔

طریقہ #3

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 آپکا 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۔



CCW, FIA

Helpdesk@Nr3c.gov.pk ☎ +92 51 9106 384



cybercrimewingofficial



Cybercrimefia



Cybercrimefia

Stay Alert
Stay Safe

1991

Cyber Crime Helpline

PUBLIC AWARENESS

BE
CAREFUL
WHAT
YOU POST
ONLINE.

DON'T
BECOME
AN
**EASY
TARGET.**



Internet-based social networking sites have created a revolution in social connectivity. However, con artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes.

Preventive Measures Include:

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service.
- Do not post anything that might embarrass you later, or that you don't want strangers to know.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.

BE SOCIAL, STAY SAFE

5 GOLDEN RULES

1. Show me



Ask your child to show you the sites they use

Show an interest, take note of the sites your children visit and re-visit them later when you are alone.

Find out how to set the safety features and how to report any issues directly to the site.

46% of parents admit that their children know more about the internet and social media than they do.

2. Low profile

Ask your child to set profile settings to private

Since children use social media sites to share just about everything they do, setting their profile to private can help protect them against photos, personal information or even location in the real world ending up in the wrong hands.



3. Just ask



Ask your child about their online friends

Help your children understand that people can create fake identities online and lie about who they are. They should only give out personal information and be "friends" with people they know and trust in the real world.

35% of children have unsupervised access to the internet.

4. Photo check

Ask your child to only share photos that they wouldn't mind showing you first!

Talk to your child about the images they send, the sites and apps they use to share them and who they are sending them to.



Children aged **12-15** are spending more time online.

5. Don't worry



Ask your child to tell you if they are worried about something online

By talking to your child about the internet, their favourite sites and the risks they may encounter, they are more likely to turn to you if they get into situations online where they don't feel comfortable or see something they don't want to see.

Children aged **8-11** are more likely than they were in 2011 to watch and download user-generated content*.

If your child is facing cyber crime speak up, report at

1991



HELP LINE
1991



EMAIL
helpdesk@nr3c.gov.pk



COMPLAINT FORM
complaint.fia.gov.pk



BY POST



INPERSON VISIT



FAX
+92-51-9106383



CyberCrimeFIA



@cybercrimefia

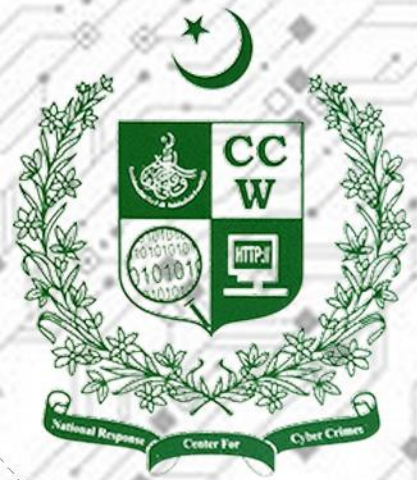


cybercrimewingofficial

What To Do in Case of Being Victimized?

- Identify and report false/misleading scams online
- You may also file an online complaint through email at:
helpdesk@nr3c.gov.pk
- You can lodge a complaint to CCW-FIA, by visiting any of the following Cyber Crime Reporting Centers

CYBER CRIME HQ	2ND FLOOR, NATIONAL POLICE FOUNDATION BUILDING, MAUVE AREA, SECTOR G-10/4, ISLAMABAD, PAKISTAN	051 9106384
CCRC ISLAMABAD	STREET 169, BUILDING 5C, G13/3 ISLAMABAD	051 9334627-28
CCRC RAWALPINDI	7A WEST SERVICE ROAD NEW GULZAR E QUAID RAWALPINDI	051 9330719
CCRC ABBOTABAD	HOUSE NO 3, STREET NO 1 MOSAZAI COLONY, MIRPUR MANSEHRA ROAD (K.K.H) ABBOTTABAD	0992 414483
CCRC PESHWAR	OPPOSITE RMI HOSPITAL HAYATABAD, PHASE V PESHAWAR	919 219565
CCRC DI KHAN	SOHNA KHAN STREET (3RD HOUSE ON THE LEFT FROM INDUS VIEW ROAD) NEAR DERA BOARD DERA ISMAIL KHAN	096 6852945
CCRC GILGIT	NEAR CM HOUSE, RIVER ROAD, CHINARBAGHGILGIT	05811 960707
CCRC LAHORE	8 B, G BLOCK, GULBERG-II, LAHORE	042 99268527
CCRC FAISALABAD	ZIA TOWN, STREET NO 2, EAST CANAL ROAD, NEAR KASHMIR PUL (OPPOSITE GOHAR TEXTILE) FAISALABAD	041 9330865
CCRC GUJRANWALA	GHAUS PLAZA, COMMERCIAL AREA, CITY HOUSING SOCIETY LAHORE ROAD GUJRANWALA	055 9330015-16
CCRC MULTAN	H.06, STREET-3 SHALIMAR TOWN BOSAN TOWN MULTAN	061 9330999
CCRC SUKKHAR	HOUSE NO A-126, SINDH HOUSING SOCITY, NEAR NADRA OFFICE, AIRPORT ROAD SUKKAR	071 9310849
CCRC HYDERABAD	PLOT A-100, SITE AREA NEAR CUSTOM HOUSE HYDERABAD	022 9250010
CCRC KARACHI	NEAR DARUL SEHAT HOSPITAL GULISTAN-E-JOHAR KARACHI	021 99333950
CCRC QUETTA	FIA OFFICE BANGLOW 105, SHABO ROAD QUETTA	081 2870057
CCRC GAWADAR	NEAR FISH HARBOR REST HOUSE GAWADAR	0332 2400190



CYBER JUSTICE

STAY CYBER AWARE

CYBER PREVENTION

CALL 1991

CYBER PROTECTION

CCW

CYBER CURE
CYBER CRIME WING

BE CYBER WISE

BE AWARE BE SAFE

CYBER RIGHTS

STAY CYBER SECURE

REPORT CYBERCRIME

CYBER WISE

KNOW CYBER LAWS

CYBER LAWS
CYBER CRIMES

FIA

FEDERAL INVESTIGATION AGENCY



