

C.D.T.I. E-NEWSLETTER

CENTRAL DETECTIVE TRAINING INSTITUTION, CHANDIGARH

Only for private circulation

Vol.1, No.8, Jan to March, 2022



From the Editor's Desk



Dear Readers, I hope you all are in your best of Health and Spirits. I am happy to bring the first edition of the E-Issue of CDTI Chandigarh Newsletter for the year 2022.

The COVID-19 situation in the country from the last two years has brought us all in an unprecedented situation. Despite the challenging times, CDTI Chandigarh was able to conduct fifteen (15) online courses/webinars successfully for Police Officers, Judicial officers & Prosecutors on the topics concerning Gender Sensitization, Investigation of Economic Offences, Rape & POCSO cases, Safe use of Social Media/Online wallets, Women Safety, Cases under NDPS Act, Financial frauds, Money Laundering crimes and many more in the first quarter.

With the Covid-19 norms getting relaxed we have also started offline Training programs along with some online training courses from April 2022.

This e-Newsletter is bringing you the highlights of the various activities related to Training programs, Cultural programs and other developments at CDTI Chandigarh.

The Editorial board would like to thank all contributors and would like to express our gratitude to Director CDTI Chandigarh for her continuous guidance and support. We look forward to receive constructive suggestions from readers to improve the E-Issue contents.

JAI HIND

**SONAL, Dy.SP
CDTI CHANDIGARH**

DETAILS OF COURSES/WEBINAR CONDUCTED AT CDTI, CHANDIGARH
W.E.F. JAN TO MARCH, 2022 FOR POLICE OFFICERS

S/No.	Name of Course	Duration	Nos. of Participants
01	Investigators Training course on "Women Safety"	03.01.22 to 07.01.22	34
02	Investigation of Economic Crime Cases	11.01.22 to 13.01.22	46
03	Cyber Security for LEO-Combodia Police officers	25,27.01.22 & 01.02.22	13
04	Webinar on appreciation of Digital Evidence in Vigilance enquiries"	28.01.22	41
05	Investigation of Cyber crime cases	01.02.22 to 03.02.22	39
06	Gender Sensitization	07.02.22 to 11.02.22	37
07	Investigation of organized crime cases	22.02.22 to 24.02.22	46
08	Webinar on Awareness about Cyber Space, safe use of social media/online wallets & appreciation of digital data in office working	25.02.22	37
09	Webinar on Work life balance and capacity building for women police officers (As part of Azaadi ka Amrit Mahotsav)	28.02.22	46
10	Investigation of Rape cases (For Judicial Officers/Prosecutors/DSP/Insp/SI)	01.03.22 TO 03.03.22	26
11	Investigators Training course on "Women Safety"	07.03.22 to 11.03.22	40
12	Webinar on Mandatory provisions of NDPS Act and their compliance for Police Officers. (As part of Azaadi ka Amrit Mahotsav)	09.03.22	51
13	Investigation of Financial frauds & Money Laundering crimes.	14.03.22 to 16.03.22	43
14	Cyber surveillance for handling cross border crimes for CPOs'	22.03.22 to 24.03.22	19
15	Cyber crime awareness Programme	28.03.22 to 30.03.22	34
		Total Trainees	552

COURSE/WEBINAR CONDUCTED AT CDTI, CHANDIGARH FROM JAN TO MARCH, 2022 FOR
JUDICIAL/PROSECUTORS OFFICERS

S/No.	Name of Course	Duration	Nos. of Participants
01	5 days online training course for prosecutors on "women safety"	14.02.22 to 18.02.22	Prosecutors-24
02	Investigation of Rape cases (For Judicial Officers/Prosecutors/DSP/Insp/SI)	01.03.22 to 03.03.22	Judicial officers -24 Prosecutors-21
03	Webinar on Safe use of social media platform & payment gateways and wallets for Judicial officer & Prosecutors.	25.03.22	Judicial officers -27 Prosecutors-18
		Total Trainees	114

Course Calendar w.e.f. April to June, 2022 in r/o CDTI, Chandigarh

S/No.	Name of Course	Duration
01	Investigation of crimes using social media platform	05.04.22 to 07.04.22
02	Online course on Investigation of Bank fraud cases & plastic card fraud cases	11.04.22 to 15.04.22
03	Webinar on Registration of Zero FIR. Its legal aspects and procedure for Police officer (As part of Azaadi ka Amrit Mahotsav)	12.04.22
04	DSI Investigation of Murder/Homicide cases	18.04.22 to 22.04.22
05	eITEC (online) course on Cyber crime investigation for Guyana Police	19.04.22 to 21.04.22
06	Investigation of Organized Financial Crimes & Money Laundering crimes	25.04.22 to 29.04.22
07	Webinar on use of Dark web and crypto currency for criminal activities for Police officer (As part of Azaadi ka Amrit Mahotsav)	26.04.22
08	Investigation of Organized Cyber crime cases	02.05.22 to 06.05.22
09	Investigation of Rape cases	09.05.22 to 11.05.22
10	Webinar on Mandatory Provisions of NDPS Act – reasons for failure in courts for Police officers (As part of Azaadi ka Amrit Mahotsav)	13.05.22
11	Online course on Cyber crime & Cyber law awareness for Public Prosecutors & Judicial officers	18.05.22 to 20.05.22
12	Investigation of Organized crime	23.05.22 to 27.05.22
13	Webinar on Importance of Emotional & Mental Health and ways to promote well-being for Police officer (As part of Azaadi ka Amrit Mahotsav)	25.05.22
14	Investigation of Organized cyber crime cases	30.05.22 to 03.06.22
15	Investigation of NDPS cases	06.06.22 to 10.06.22
16	Online Course on Cyber crime awareness programme for police officers	07.06.22 to 09.06.22
17	Investigation of Sexual assault cases against women & children	13.06.22 to 17.06.22
18	Webinar on use of technology in effective policing for Police officer (As part of Azaadi ka Amrit Mahotsav)	15.06.22
19	Awareness about Mobile Forensic & its utility in Investigation	20.06.22 to 24.06.22
20	Webinar of Wild life crimes & trade across the borders for CPOs (As part of Azaadi ka Amrit Mahotsav)	23.06.22
21	DSI Course on Advanced technology in Forensic science	27.06.22 to 08.07.22

CDTI AT A GLANCE



Mess & Gymnasium



Recreation Hall & Hostel



Cyber Lab & Class Room

Sh. Gurcharan Singh, Cyber Faculty, CDTI Chandigarh, while delivering a session on Cyber security in Chandigarh University



साइबर अपराध से बचना है जरूरी: गुरचरण सिंह

चंडीगढ़। दयानंद/शिवम

पंजाब यूनिवर्सिटी, चंडीगढ़ में चल रहे एन.एस.एस के सात दिवसीय विशेष शिविर में छठे दिन मुख्य वक्ता के तौर पर सेंट्रल डिटेक्टिव ट्रेनिंग इंस्टीट्यूट चंडीगढ़ से गुरचरण सिंह रहे। उन्होंने सभी स्वयंसेवकों को संबोधित करते हुए कहा कि आज हम इंटरनेट के युग के अंदर स्मार्टफोन का काफी ज्यादा इस्तेमाल कर रहे हैं। परंतु आज इस जिस तरह से दिन प्रतिदिन हमारा लगाव स्मार्टफोन की तरफ हो रहा है और हम अपने सारे महत्वपूर्ण कार्य ऑनलाइन माध्यम से कर रहे हैं। इससे हमारा डाटा किसी द्वारा हैक कर लिए जाने की ज्यादा संभावना बन चुकी है। क्योंकि साग डाटा ऑनलाइन होने के कारण आज हमारी निजी जानकारी शरारती तत्वों के हाथ में जाने की संभावना बहुत ज्यादा बढ़ गई है। इससे हमें बचना होगा। क्योंकि आज यदि हम साइबर सुरक्षा के प्रति सजग नहीं हुए तो आने वाले समय के अंदर हम साइबर अपराध का शिकार हो सकते हैं। उन्होंने कहा कि हमें अपने बैंक खाते



की जानकारी किसी भी व्यक्ति को नहीं देनी चाहिए। यदि हम ऐसा करते हैं तो किसी भी व्यक्ति के द्वारा हमारे बैंक खाते से पैसे निकाले जा सकते हैं और हमारा बैंक खाता पूर्ण रूप से खाली हो सकता है। इसलिए इस तरह के ऑनलाइन अपराधों से बचने के लिए आज हमें साइबर सुरक्षा के बारे में जनता को जागरूक करना होगा तभी आने वाले समय के अंदर भारत पूर्ण रूप से साइबर सुरक्षित राष्ट्र बन पाएगा और विश्व में

भारत की एक अलग पहचान बन पाएगी। कैप के छठे दिन सभी स्वयंसेवकों के लिए खेलकूद प्रतियोगिता का आयोजन किया गया। जिसमें सभी स्वयंसेवकों के द्वारा बड़ चढ़कर भाग लिया गया। कैप में शाम के समय सांस्कृतिक गतिविधियों का आयोजन भी किया गया। इस अवसर पर सभी कार्यक्रम अधिकारी डॉ. रोहित कुमार शर्मा, डॉ. लोकेश कुमार, डॉ. विवेक कपूर, डॉ. रिचा शर्मा आदि मौजूद रहे।

DIRECTOR CDTI CHANDIGARH PARTICIPATED IN INTERNATIONAL WOMEN'S DAY FUNCTION AT BPR&D HEADQUARTER, NEW DELHI



ONLINE TRAINING COURSES @ CDTI

e-ITEC Programme on Cyber Crime Investigation
and Digital Forensic Science, for Cambodian LEO/Successive Police
Instructors held in January

The screenshot displays a Cisco Webex meeting interface. At the top, the title bar shows 'Cisco Webex Meetings' and 'Meeting Info'. Below this, a grid of 16 video feeds shows participants, including Dr. Nishakant Ojha. To the right, a 'Participants (19)' list shows names like CDTI CHD, BPR&D, Col Lim Leang, Dr. Nishakant Ojha, Eour Sophos, Leng Kimhai, Nob Sophanit, Seng SokAnn, SokAnn, Sokchea Heng, sriengsophy, SUY CHHIM, and tith tina. Below the grid, a presentation slide titled 'WHY DO BREACHES OCCUR?' is visible. The slide shows a bar chart with categories: Mis-configured system or application (42%), Vulnerable code (6%), End-user error (31%), Targeted attack, exploited (6%), and Undetermined (15%). The slide also lists various factors contributing to breaches, such as Configuration Errors, Weak defaults, Easy passwords, Bugs, Input validation, Installing suspect applications, Clicking malicious links, Phishing Emails, and Watering Hole attacks. The bottom of the screen shows the Windows taskbar with the search bar and various application icons.

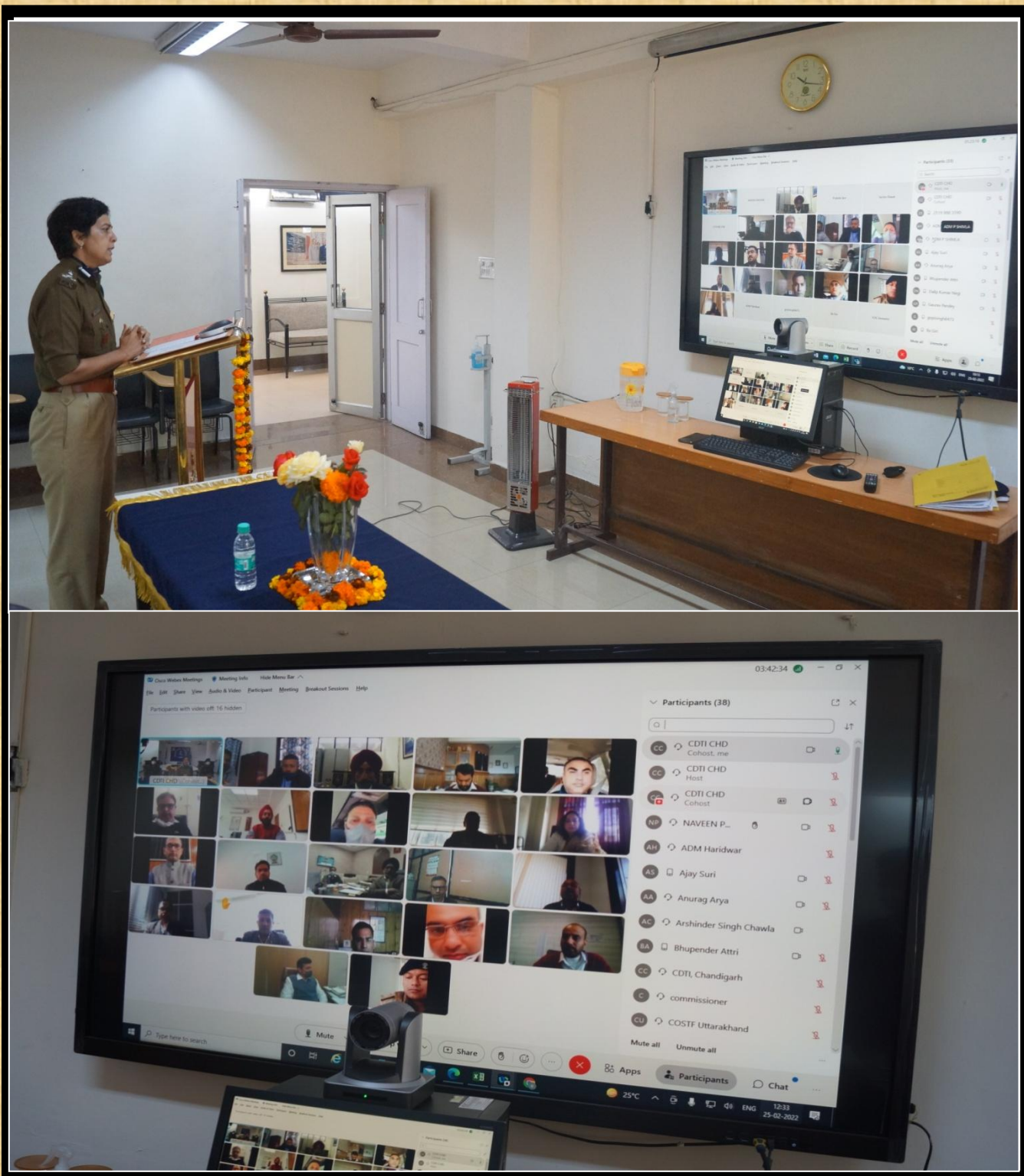
WHY DO BREACHES OCCUR?

Category	Percentage
Mis-configured system or application	42%
Vulnerable code	6%
End-user error	31%
Targeted attack, exploited	6%
Undetermined	15%

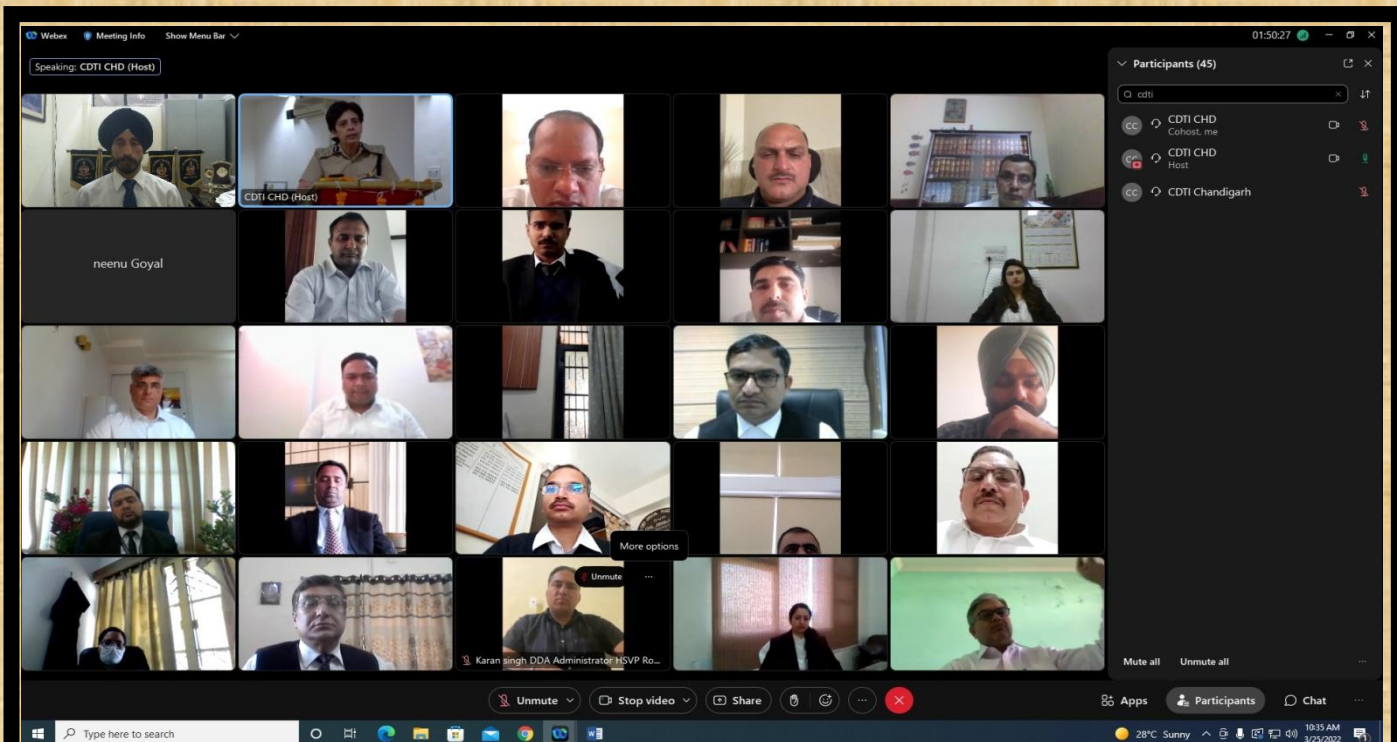
Factors contributing to breaches:

- Configuration Errors
- "Weak" defaults
- Easy passwords
- "Bugs"
- Input validation
- Installing suspect applications
- Clicking malicious links
- Phishing Emails
- Watering Hole attacks

NEW INITIATIVE TAKEN BY HOLDING WEBINAR ON AWARENESS
ABOUT CYBER SPACE & SAFE USE OF SOCIAL MEDIA.
(Exclusively for Administrative officers of client States on
25.02.22)



WEBINARS AS PART OF (AZAADI KA AMRIT MAHOTSAV) ON “WORK LIFE BALANCE AND SAFE USE OF INTERNET”



Webinar on safe use of internet



Webinar on work life balance

AWARENESS PROGRAMME ON SAFE USE OF SOCIAL MEDIA PLATFORMs
EXCLUSIVELY FOR JUDICIAL OFFICERS & PROSECUTORS ON 25.03.2022



Dr. Balram K. Gupta, Director, Judicial Academy, Chandigarh, being presented with memento on his visit as Chief Guest for the valedictory session of webinar on 25.03.2022

SOME GLIMPSES OF THE CULTURAL DAY CELEBRATED ON 21.03.2022



SAFE USE OF E-WALLETS AND DIGITAL PAYMENT



An Electronic-wallet(e-wallet) is an application that allows us to do e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc, by using smart phones or computers. Large number of e-wallets is available online to be downloaded on our smart phones to support both point-of-sale transactions and peer-to-peer transactions between individuals. A number of Banks, Telecoms firms, online e-commerce portal, taxi-services, supermarket chains etc. provide e-wallets and personally identifiable information (PII's) of the customer like his name, mobile phone number including his protected personal information like Customer card numbers, secret PIN, net banking credentials etc is permanently stored in e-wallets, requiring just final authorization from the user through means like biometrics authentication, one-time passwords (OTP) etc.

The COVID-19 pandemic has impacted the world in an unprecedented manner. It had forced most of the consumers to opt for digital payments. With social distancing becoming the new normal in times of COVID-19, consumers had no option other than going for contactless and digital modes of payments. But with this rapid increase in the use of digital payments comes the fear of digital payment frauds too especially when fraudsters and hackers have become more active.

In this article, we will discuss about the types of digital payment frauds and the measures that can prevent these online payment frauds.

Types of E-wallets/Digital Payment Frauds

i) **Impersonation by SIM swapping** – In this type of fraud, the fraudsters first collect the user's information, and use it to get his mobile phone SIM card blocked and obtain a duplicate one by visiting the mobile operator's retail

outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudster who then generates one-time passwords using stolen information.

ii) **Man-in-the-middle attack and Phishing** - Sophisticated threats like Man-in-the-Browser or Man-in-the-Middle attacks intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details. Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.

iii) **KYC fraud** - Usually, the victim gets a text message stating his e-wallet needs to be KYC compliant; he is asked to call the telephone number provided in the message. To update the KYC, he is asked to download an app, usually TeamViewer Quick Support or AnyDesk -- these are remote access control mobile apps. The phishers ask the victim to transfer Rs 1 to check the status of the e-wallet. While the customer is entering a password or PIN for his e-wallet, the scammers are collecting details being entered alongside. They now have access to his mobile wallet ID and password and can empty his wallet.

iv) **QR Code Scan** – Such types of incidents are happening on the OLX website for buying and selling of goods. Fraudster poses as a customer to buy the good and then send QR Code to the victim mobile to scan for accepting the payment, which incidentally is meant for sending the payment.

v) **Malware Attack** - An attacker can inject a malware (a malicious application) to attack the app and collect details from his phone to misuse it.

Preventive Measures to Remain Safe while using e-wallets/Digital Payments:

Enable Passwords on Devices: Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used. Users should try to apply additional layers of security like biometric, retina, facial authentication etc.

SIM Swap Attack prevention - Some Mobile network operators send an SMS to alert their customers of a SIM swap, the affected customer can act and stop this fraud in its tracks by contacting the mobile operator immediately. Further in case the subscriber's network going off suddenly, then he should contact his operator immediately to inquire the reason.

Prevention from Phishing attacks - The URL of the webpage should be verified, by establishing the authenticity of the website by validating its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of the browser window. Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.

Use Secured and trusted Network Connections: Users should only connect to the trusted networks and avoid the use of public Wi-Fi networks. More secured and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.

Install Apps from Trusted Sources: User ratings and reviews provide some clues about the integrity of the e-wallet app. The user must check for the e-wallet provider to be showing strong legacy of securely, reliably, and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).

Keep the wallet software up to date: Using the latest version of software allows receiving important stability and security fixes timely to prevent malware attacks.

Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and

intrusion-detection systems, mobile security solutions should be installed and activated.

Keep Login Credentials Safe and Secured: Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid easy access of same to fraudster to misuse.

Keep a Unique Password for each Digital Wallet: Keep strong and hard-to-guess passwords, unique to each digital wallet to prevent unauthorized access by the fraudster.

Register for Alerts through SMS and emails and check unusual behaviour of cellphone devices. The user should not switch off his cellphone in the event when numerous annoying calls are received, rather answering the calls should be avoided. It's a tactics adopted by the fraudsters to irritate you to switch off the devices or put it on silent mode to prevent him from noticing that his connectivity has been tampered with. The user will then not receive any SMS notifications or alerts from the banks when the fraudsters have fraudulently gained access to his e-wallet.

Check your Bank Statement regularly – Banks are supposed to send you the bank statement regularly on your emails or physical address. Go through the bank statement thoroughly to check whether there is any unusual transaction, which you never carried out and alert the bank accordingly.

Identify Points of Contact in case of Fraudulent Issues: For any fraudulent activity occurring on the user's account in the scenarios like when phone is lost or stolen, an individual card stored in the wallet is lost or account has been hacked, appropriate points of contact for resolving the issues should be understood by the user. The Government of India has created a portal for reporting such incidents on www.cybercrime.gov.in and also through toll free number 1930.

By Gurcharan Singh,
Cyber Faculty,
CDTI, Chandigarh

THE IMPACT OF COVID-19 ON VIOLENCE AGAINST WOMEN AND GIRLS- AN OVERVIEW OF UN/WHO REPORT



There is **initial evidence of intensification of violence against women and girls across the globe**. Reports from service-use data in different countries have shown an important increase in reported cases of domestic violence to helplines, women's refuges/shelters and to the police, linked to COVID-19. Calls to helplines have increased five-fold in some countries. Other countries, however, have observed a decrease in the number of domestic violence incidents reported, highlighting accessibility and availability challenges during lockdowns and other social distancing measures. By October 2021, **52 countries had integrated violence against women and girls prevention and response into COVID-19 plans**, and 150 countries have adopted measures to strengthen services for women survivors of violence during the global crisis. Continuing efforts are needed to ensure the recovery responses fully integrate ending violence against women measures to build a post-pandemic equal world. **{Big data analysis in eight Asian countries shows that Internet searches related to violence against women and help-seeking rose significantly during COVID-19 lockdowns}**.

Reporting of violence against women

- **Less than 40 per cent of the women who experience violence seek help of any sort.** In the majority of countries with available data on this issue, among women who do seek help, most look to family and friends and very few look to formal institutions, such as police and health services. Less than 10 per cent of those seeking help appealed to the police.
- **Laws on violence against women and girls**
- **At least 158 countries have passed laws on domestic violence, and 141 have laws on sexual harassment in employment.** However, even when laws exist, this does not mean they are always compliant with international standards and recommendations or are implemented and enforced. In 2020, Kuwait and Madagascar introduced specific and comprehensive legislation on domestic violence for the first time.

Economic costs of violence against women and girls

Violence against women & girls can result in significant costs to the State, to victims/survivors, and communities. **Costs are both direct and indirect, and tangible and intangible.** For example, the costs of the salaries of individuals working at shelters are direct

tangible costs. Costs are borne by everyone, including individual victims/survivors, perpetrators, the government and society in general.

Following are the description of types of violence which women's & girls across the globe are facing:-

1. Sexual violence against women and girls

- **Globally, 6 per cent of women report they have been subjected to sexual violence from someone other than their husband or partner.** However, the true prevalence of non-partner sexual violence is likely to be much higher, considering the particular stigma related to this form of violence.
- **15 million adolescent girls worldwide, aged 15–19 years, have experienced forced sex.** In the vast majority of countries, adolescent girls are most at risk of forced sex (forced sexual intercourse or other sexual acts) by a current or former husband, partner, or boyfriend. Based on data from 30 countries, only one per cent have ever sought professional help.
- **In the Middle East and North Africa, 40–60 per cent of women have experienced street-based sexual harassment.** In the multi-country study, women said, "the harassment was mainly sexual comments, stalking or following, or staring or ogling". Between 31 and 64 per cent of men said that they had carried out such acts. Young men, men with more education, and men who experienced violence as children were more likely to engage in street sexual harassment.

2. Trafficking in women

- **In 2020, for every 10 victims of human trafficking detected globally, about five were adult women and two were girls. Most of the detected victims of trafficking for sexual exploitation (92 per cent) are females.** Since the onset of the COVID-19 pandemic, women have been affected disproportionately and have been recruited, often locally or online, for sexual exploitation, particularly for exploitation in private apartments.

3. Violence against girls

During the past decade, the **global rate of child marriage** has declined, with the global proportion of young women aged 20–24 years who were married before the age of 18 decreasing by 15 per cent, from nearly one in four in 2010 to one in five in 2020. As a

result of this progress, the child marriages of some 25 million girls have been averted. However, the profound effects of the pandemic are threatening this progress, with up to 10 million additional girls at risk of child marriage in the next decade as a result of the pandemic.

School-related gender-based violence is a major obstacle to universal schooling and the right to education for girls. Globally, one in three students, aged 11–15, have been bullied by their peers at school at least once in the past month, with girls and boys equally likely to experience bullying.

4. Female genital mutilation

- **At least 200 million women and girls, aged 15–49 years, have undergone female genital mutilation in 31 countries where the practice is concentrated.** Half of these countries are in West Africa. There are still countries where female genital mutilation is almost universal; where at least 9 in 10 girls and women, aged 15–49 years, have been cut.

5. Cyber-harassment

- **One in 10 women in India having experienced cyber-harassment since the age of 15.** This included having received unwanted and/or offensive sexually explicit emails or SMS messages, or offensive and/or inappropriate advances on social networking sites. The risk is highest among young women aged 18–29 years. Although this is the best information available so far. That the increasing reach of the internet, the rapid spread of mobile information, and the widespread use of social media, especially since the onset of the COVID-19, and coupled with existing prevalence of violence against women and girls.
- In the U.S., two out of every ten young women, aged 18–29, have been sexually harassed online and one in two says that they were sent unwarranted explicit images. In Pakistan, 40 per cent of women had faced various forms of harassment on the internet. Women

and girls are using internet with greater frequency during the pandemic while there is a gender digital divide. And when women and girls do have access to the internet, they face online violence more often than men.

6. Violence against women in politics

Across five regions, 82 per cent of women parliamentarians reported having experienced some form of psychological violence while serving their terms. This included remarks, gestures, and images of a sexist or humiliating sexual nature, threats, and mobbing. Women cited social media as the main channel of this type of violence, and nearly half (44 per cent) reported receiving death, rape, assault, or abduction threats towards them or their families. Sixty-five per cent had been subjected to sexist remarks, primarily by male colleagues in parliament.

**Rajeev Kumar Sharma,
Dy.SP (Admin)
CDTI Chandigarh**

आज़ादी का अमृत महोत्सव



आज़ादी का अमृत महोत्सव, आत्मनिर्भरता का एहसास है।
जन-जन की भागीदारी का यह गौरवशाली इतिहास है।।

भारत माँ परतन्त्रता की बेड़ी में जकड़ी सिसक रही थी।
तब नेताजी ने हर भारतवासी को इक बात कही थी।।
'तुम मुझे खून दो मैं तुम्हें आज़ादी दूँगा', नारा था।
फिर लाखों रण में कूद पड़े, वतन जो जाँ से प्यारा था।।
गाँधी, लाल, बाल, पाल, भगत, गुरु, सुखदेव, हुए थे कुर्बा।
बिस्मिल, अफ़ाक़, आज़ाद, लुटा गए वतन पर अपनी जाँ।।
बलिदानों की वेदी से हो कर आज़ादी हम तक आई।
स्वतन्त्रता सेनानियों ने जाँ देकर इसकी कीमत चुकाई।।
उन आज़ादी के मतवाले वीरों को कोटि कोटि वन्दन।
जिन्होंने लिया हँसते-हँसते फाँसी के फ़न्दे का चुम्बन।।
यह आज़ादी लाखों के बलिदानों का अद्भुत प्रयास है।
आज़ादी का अमृत महोत्सव, आत्मनिर्भरता का एहसास है।
जन-जन की भागीदारी का यह गौरवशाली इतिहास है।।

पन्द्रह अगस्त सन् सैंतालीस नई आशा, उर्जा लाया।
आज़ादी के सूर्योदय का खूब हुआ था भव्य उजाला।।
पचहत्तरवीं वर्षगाँठ से अब पचहत्तर सप्ताह पूर्व।
बारह मार्च दो हज़ार इक्कीस को हुई एक पहल अपूर्व।।
मोदी जी ने साबरमती से पदयात्रा को झण्डी दिखाई।
आज़ादी के अमृत महोत्सव की अद्भुत शुरुआत कराई।।
इसको पचहत्तर सप्ताहांत चलाने का आह्वान किया।
पन्द्रह अगस्त दो हज़ार बाईस को समापन ठान लिया।।
स्वतन्त्रता की वेदी पर न्यौछावर वीरों की गाथा है।
यह भारत माँ के आँचल की ममतामय निर्मल छाया है।।
आज़ादी के दीवानों का यह अनुपम पावन उल्लास है।
आज़ादी का अमृत महोत्सव, आत्मनिर्भरता का एहसास है।
जन-जन की भागीदारी का यह गौरवशाली इतिहास है।।

है अलबेला महोत्सव ये तो जन-जन के आत्म-चिन्तन का।
देता है अचूक अवसर ये पग-पग पर आत्म-मंथन का।।

क्या खोया, क्या पाया हमने, क्या किया और क्या करना है।
चिन्तन कर, हासिल पर आत्मविभोर न हो, आगे बढ़ना है।।
आई. टी., अंतरिक्ष, चिकित्सा, अनुसंधानों में हम उत्तम।
योग, शोध, ज्योतिष, सांस्कृतिक अनुष्ठानों में हम सर्वोत्तम।।
गत् गौरवशाली पचहत्तर वर्षों पर करते हैं हम मान।
नव उन्नति के अन्नत आयाम छूने पर है हमारा ध्यान।।
आर्थिक उन्नति, सामाजिक समरसता, हो सांस्कृतिक उत्थान।
ध्येय हमारा एक यही द्वेष-भाव त्याग मानव हो महान।।
वैभवशाली, समृद्ध, उन्नत, हिन्दुस्तां बनने की आस है।
आज़ादी का अमृत महोत्सव, आत्मनिर्भरता का एहसास है।
जन-जन की भागीदारी का यह गौरवशाली इतिहास है।।

स्वराज ने पारदर्शी, निर्भय, औद्योगिक माहौल दिया।
कई ऐतिहासिक भूल सुधारीं, प्रोद्योगिक विस्तार हुआ।।
जन-कल्याण योजनाएँ अब, खोल रही हैं द्वार समृद्धि के।
है देश प्रगति पथ पर अग्रसर, अवसर बहुतेरे उन्नति के।
भारतीय युवाशक्ति का है यह दसों दिशाओं में गुणगान।
उन्नत भारत के पचहत्तर वर्षों का है ये अभिमान।।
आज़ादी का अमृत महोत्सव, लाया हर चेहे पर मुस्कान।
भारत के बच्चे-बच्चे के दिल में है एक यही अरमान।।
हर सू 'वसुधैव कुटुम्बकम्' की सौँधी-सौँधी खुशबू महके।
'हसरत' अम्नो-इंसानियत का हर सू गीत सुरीला चहके।।
भारत के विश्वगुरु बनने के दृढ़ संकल्प की यह आस है।।
आज़ादी का अमृत महोत्सव, आत्मनिर्भरता का एहसास है।
जन-जन की भागीदारी का यह गौरवशाली इतिहास है।।

डॉ. सुशील 'हसरत' नरेलवी
केन्द्रीय गुप्तचर प्रशिक्षण संस्थान,
चण्डीगढ़-160036

Know our Faculty



Shri Gurcharan Singh is a renowned Cyber Faculty of CDTI, Chandigarh having around 25 years of experience. He is visiting faculty with many State Police Academies/CPOs, Universities and training Police Officers, Judicial Officers, Academicians and Public Prosecutors across the country. Although, it is not in his mandate of duties but he is always proactively guiding the I.O's of various investigating agencies in their hour of need and has helped the Investigating officers in solving a number of blind and dead cases.

CDTI CHANDIGARH ON SOCIAL MEDIA



www.cdtschd.gov.in



@cdtichandigarh



Central Detective
Training Institute: Chandigarh