



केन्द्रीय विद्यालय क्र.-1, वायु सेना स्थल , सिरसा

KENDRIYA VIDYALAYA NO.1, AIR FORCE STATION, SIRSA

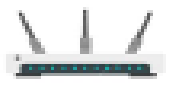
75
आज़ादी का
अमृत महोत्सव

CYBER JAAGROOKTA DIWAS ACTIVITIES E-BOOK



**DESIGNED & DEVELOPED BY:
MS SUMAN, PGT CS , KV NO 1 AFS SIRSA**

**UNDER THE GUIDANCE OF :
MR VIRENDER SINGH, PRINCIPAL
KV NO 1 AFS SIRSA**



From the desk of Principal



It gives me immense pleasure to announce that KV No 1 AFS Sirsa is going to publish e-book of the activities conducted under Cyber Jaagrookta Programme observed on first Wednesday of every month commenced from 6th October 2021.

The program was mainly focused to sensitise the students, teachers and other stakeholders of the Vidyalaya about Cyber Crimes, forgery from mobile devices, safe usage of Digital platforms, browser security, debit / Credit Card frauds etc.

This e-book witnesses the sincere efforts of our students and teachers to make the Cyber Jaagrookta campaign a huge success. All the activities conducted as per the calendar provided by KVS(HQ) in letter and spirit.

I would recommend that such programmes should be continued to sensitise more and more people to defend themselves against Cyber Crime.

With Best wishes!

Keep yourself and your family safe in Tech driven world.



Virender Singh
Principal
KV NO 1 AFS Sirsa

Kendriya Vidyalaya Sangathan (HQs)
Calendar of Activities
Suggestive topics to be covered in Cyber
Jaagrookta Diwas

Sr.No	Month	Topics to be covered (Classes XI & XII)
1	October 202 1	Introduction to cybercrimes. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, ransom ware, identity theft.
2	November 202 1	Forgery Devices and fraud from Mobile
3	December 202 1	Cyber risk associated with varied online activities and protection therefrom. Work on different digital platforms safely.
4	January 202 2	Online cybercrimes against women and impersonation scams
5	February 2022	Safety in Online Financial transactions.
6	March 2022	Examination
7	April 2022	Seminars on Cyber Security Awareness.
8	May 2022	Poster making/slogan writing on Cyber Security Awareness.
9	June 2022	Short stories/Essays writing on Cyber Security Awareness.
10	July 202 2	Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.
11	August 2022	Debit/Credit card fraud, email security, mobile phone security.
12	September 2022	Preparation of E-Book of the activities undertaken.

CYBER JAAGROOKTA DIWAS

Month: October

Topics Covered: Introduction to cybercrimes. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransomware

Cyber Crime

Cybercrime is a crime that involves a [computer](#) and a [network](#). The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.



Identity Theft

Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases.



Types of Cyber Crime

- Phishing
- Identity Theft
- Cyberstalking
- Cyber obscenity
- Computer vandalism
- Ransom ware

Phishing

Phishing is a cybercrime in which a **target or targets are contacted by email, telephone or text message** by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.



Cyber Stalking

Cyberstalking is a crime in which someone harasses or stalks a victim using electronic or digital means, such as social media, [email](#), instant messaging (IM), or messages posted to a [discussion group](#) or forum.





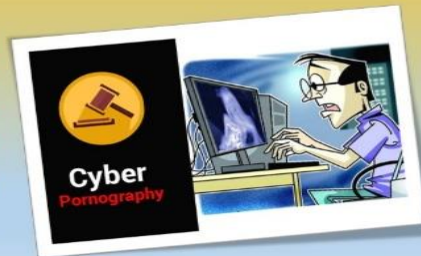
CYBER JAAGROOKTA DIWAS

Month: **October**

Topics Covered: Introduction to cybercrimes. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransomware

Cyber obscenity

Cyber obscenity is a trading of sexually expressive materials within cyber space. Legally cyber obscenity is also termed as 'pornography'.



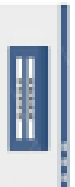
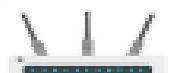
Cyber Vandalism

Computer vandalism is a process wherein there is a program that performs malicious function such as extracting a user's password or other data or erasing the hard disk. A vandal differs from a virus, which attaches itself to an existing executable program



RANSOMWARE

Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access.

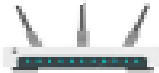




CYBER JAAGROOKTA DIWAS

Month: October

Topics Covered: Introduction to cybercrimes. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransomware



CYBER JAAGROOKTA DIWAS

Month: **October**

Topics Covered: Introduction to cybercrimes. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransomware



CERTIFICATE OF PARTICIPATION

Ms./ Mr./ Dr./ Prof. **Suman**,
has participated in the **Orientation on Cyber Jaagrookta Diwas** and completed the Post session Activity organized by CIET-NCERT on 6 October 2021.

abehera

Prof. Amarendra Prasad Behera

Joint Director
CIET - NCERT

Angel

Dr. Angel Rathnabai

Asstt. Prof. & Programme Coordinator
CIET - NCERT

Bharti

Dr. Bharti

Head, DICT & TD
CIET - NCERT




CYBER JAAGROOKTA DIWAS

Month: **NOVEMBER**

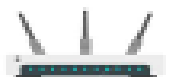
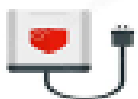

Topics Covered: **Forgery Devices and fraud from Mobile**



FRAUD VS. FORGERY



	Fraud	Forgery
Classification	Any kind of practice of dishonesty of a person or a company for financial advantage. Can be performed through the use of objects obtained through forgery.	A common technique in fraud schemes, which utilizes forged documents in order to gain access to information or materials they should not have access to.
Legal Classification	Class I Felony Fraud Count	Class A Misdemeanor
Fines	up to \$10,000	up to \$10,000
Sentence	up to 3.5 years	average of up to 16 months
Digital Protection	With Machine Learning software	With Machine Learning software





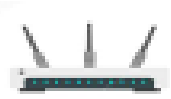
CYBER JAAGROOKTA DIWAS

Month: **NOVEMBER**

Topics Covered: **Forgery Devices and fraud from Mobile**

THE MOST COMMON TYPES OF MOBILE AD FRAUD

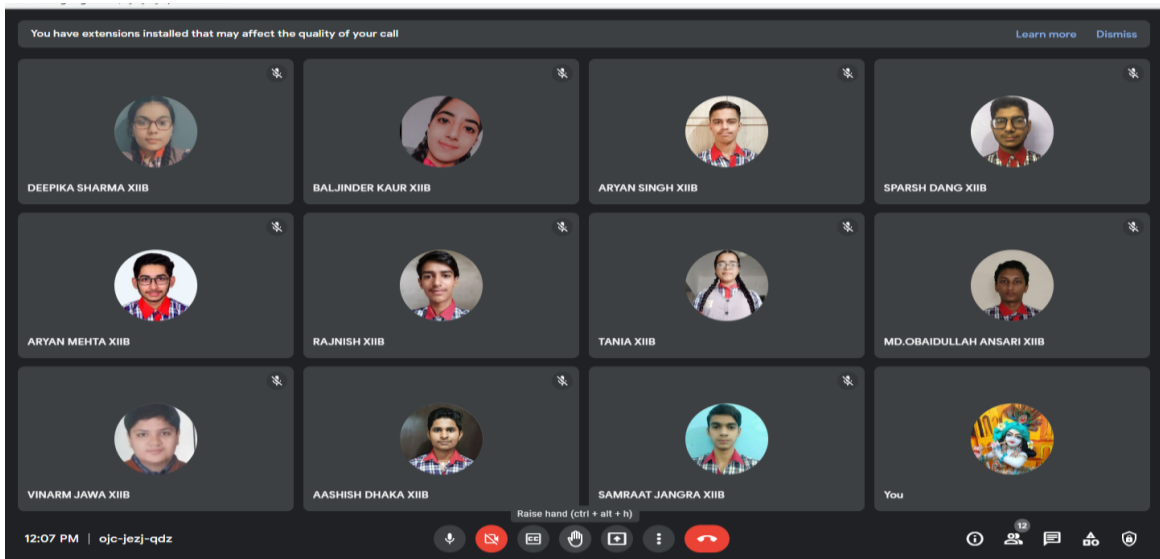
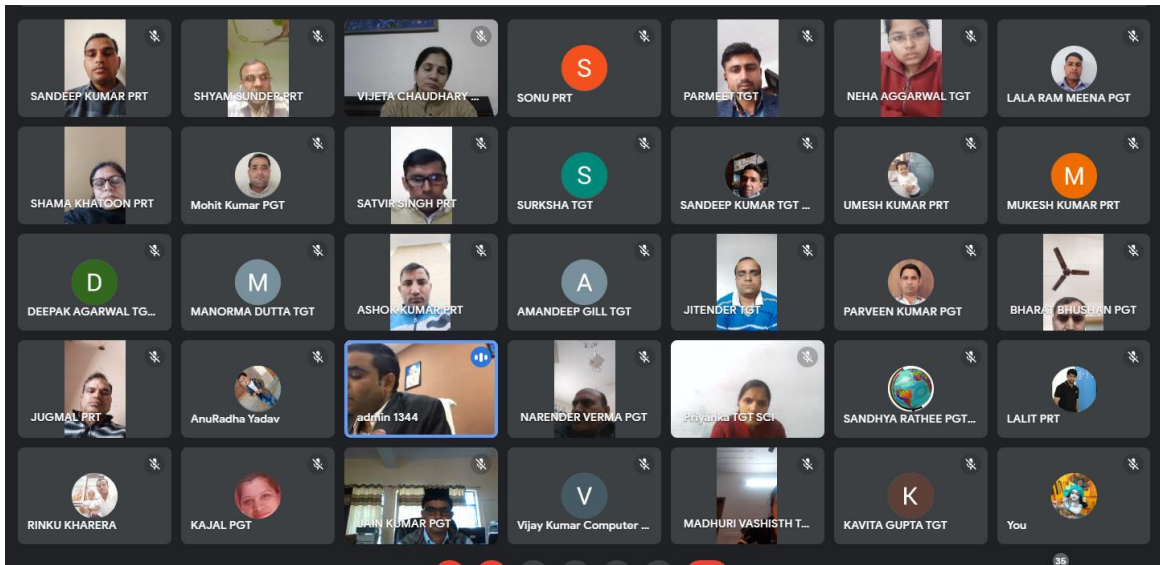
1. **IVT: Invalid Traffic** : Webcrawlers , spiders , bots
2. **Check Injection** : Check Spamming when other apps are downloaded and trigger clicks before an install completes. (android devices).
3. **Ad Stacking**: multiple ads are displayed all at once, one on top of the other. This allows an unscrupulous publisher or other involved partner to say that they technically served an ad and should receive payment for serving said ad, even though the ad was never technically visible.
4. **App Spoofing**: (spoofing example **when an email is sent from a false sender address, that asks the recipient to provide sensitive data.**)
Mobile app spoofing occurs **when the app on which the ad impressions is generated is misrepresented.** But instead of sending a fake URL as is the case with domain spoofing, the app sends a fake bundled ID, which is the identifier of the app.
5. **Background Ad Activity**:
instead of showing a video ad to a real person, the ad is played purely in the background and not seen by anyone. This way, the fraudster can still charge per view, even though no one actually saw the ad.



CYBER JAAGROOKTA DIWAS

Month: **NOVEMBER**

Topics Covered: **Forgery Devices and fraud from Mobile**



Other activities Conducted: students participate in National Cyber security awareness quiz available on mymgov.in

CYBER JAAAGROOKTA DIWAS

Month: DECEMBER

Topics Covered: Cyber risk associated with varied online activities and protection therefrom. Work on different digital platforms safely.

The Risks Behind the Apps

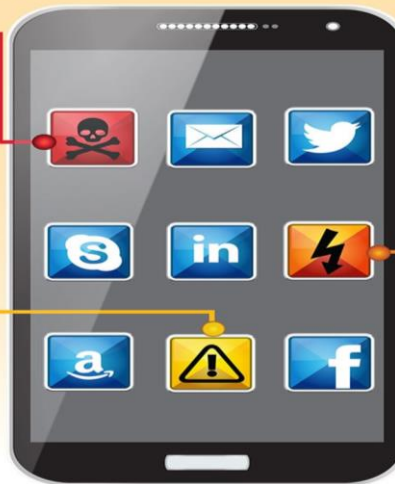
Malicious Behaviors

- Accesses device management and restricted security APIs unnecessarily
- Accesses or requests Super User permissions
- Exploits operating system or zero-day vulnerabilities
- Roots or jailbreaks device
- Steals login credentials
- Communicates with known malicious IP addresses and domains

Moderate Risk Behaviors

May be a risk if performed by apps from unknown or untrusted sources

- Reads and Sends emails
- Reads and Sends SMS messages
- Reads and sends GPS information



Dangerous Behaviors

- Uploads user information without permission or without notifying user
 - Upload address book without notifying user
 - Reads SMS messages and sends them off the device
 - Reads emails and sends them off the device
 - Reads browser history and sends it off the device
- Includes SSL vulnerabilities that enable communications to be intercepted
- No privacy policy or refers to an invalid privacy policy
- Installs boot-time startup item

MOBILE DEVICES



WHAT!?

Mobile devices are becoming a much bigger target for Cybercriminals.



HOW?

Cybercriminals will use software hidden within links to hack a mobile device. They also use Apps that contain viruses. As well as this, connecting to an unsafe WIFI on your mobile device can also exploit sensitive data.



WHY?

Our mobiles know everything about us these days as we store lots of sensitive data on there. It is an easy way for cyber criminals to find a way into a company. Users are often ignorant about the dangers...

TOP TIPS:

1. Keep your mobile device and apps updated.
2. Be wise when using free WIFI and connecting to Bluetooth.
3. Use two-factor authentication whenever possible.
4. Be sure to back up your data, so if you are ever hacked you still have sensitive data stored.



CYBER JAAGROOKTA DIWAS

Month: DECEMBER

Topics Covered: Cyber risk associated with varied online activities and protection therefrom. Work on different digital platforms safely.

Decision Path for Building Privacy into Apps



CYBER JAAGROOKTA DIWAS

Month: DECEMBER

Topics Covered: Cyber risk associated with varied online activities and protection therefrom. Work on different digital platforms safely.

You have extensions installed that may affect the quality of your call [Learn more](#) [Dismiss](#)

You're presenting to everyone [Stop presenting](#)

The Risks Behind the Apps

Malicious Behaviors

- Accesses device management and restricted security APIs unnecessarily
- Accesses or requests Super User permissions
- Exploits operating system or zero-day vulnerabilities
- Roots or jailbreaks device
- Steals login credentials
- Communicates with known malicious IP addresses and domains

Moderate Risk Behaviors

May be a risk if performed by apps from unknown or untrusted sources

- Reads and Sends SMS messages
- Reads and sends GPS information

Dangerous Behaviors

- Uploads user information without permission or without notifying user
- Upload address book without notifying user
- Reads SMS messages and sends them off the device
- Reads emails and sends them off the device
- Reads browser history and sends it off the device
- Includes SSL vulnerabilities that enable communications to be intercepted
- No privacy policy or refers to an invalid privacy policy
- Installs boot-time startup item

proofpoint.

To avoid an infinity mirror, don't share your entire screen or browser window. Share just a tab or a different window instead. [Stop presenting](#) [Ignore](#)

12:30 PM | nbq-pjvn-htc

your entire screen or others browser window

People

Save attendance

All muted Add people Host controls

Search for people

In call

- Suman PGT COMP ... (You) Meeting host
- Suman PGT COMP SCI Your presentation
- ABHJJEET KAUR XI B
- AKASH PAL XI B
- AMAN YADAV XI B
- ANKITA YADAV XI B

You're presenting to everyone [Click here to return to the video call when you're ready to stop presenting](#)

Google Chrome • meet.google.com

Other activities Conducted: students participate in Cyber security awareness quiz

CYBER JAAGROOKTA DIWAS

Month: JANUARY

Topics Covered: **Online cybercrimes against women and impersonation scams**

Cyber Crimes

- ▶ CYBER STALKING & BULLYING
- ▶ DEBIT CARD CLONING
- ▶ KEYLOGGER
- ▶ SMS & CALL SPOOFING
- ▶ RANSOMWARE
- ▶ ONLINE GAMES
- ▶ DEEPFAKES
- ▶ CAMERA HACKING
- ▶ SOCIAL TROLLING



CYBER STALKING & BULLYING

- ▶ Cyberstalking is the use of the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites
- ▶ Sending tormenting post, harassing messages, threatening contents to a minor to cause mental harassment and depressive to the recipient of such messages.



DEBIT CARD CLONING

- ▶ Debit Card skimming happens when the PIN is revealed to another person.
- ▶ A scamster who knows the PIN and has possession of the card even for a short while can replicate the card with a skimming /schimming device and withdraw cash.



CYBER JAAGROOKTA DIWAS

Month: JANUARY

Topics Covered: **Online cybercrimes against women and impersonation scams**

ONLINE GAMES

- ▶ Girls who are vulnerable to loneliness, low self esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them.
- ▶ For ex. blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.



CAMERA HACKING

- ▶ Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment. Phones with no camera guard can be exploited for such criminal activities



shutterstock.com · 1857744442

DEEPFAKES

- ▶ Deepfake is a technique that is used to combine and superimpose new images and videos onto source images or videos. It is used to create videos where the voice or face of another is superimposed on the original in such a way that the viewer or listener cannot distinguish or doubt the veracity of it



CYBER JAAAGROOKTA DIWAS

Month: JANUARY

Topics Covered: **Online cybercrimes against women and impersonation scams**

SOCIAL TROLLING

- ▶ Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the express purpose of causing humiliation or nuisance to the object of trolling



KEYLOGGER

- ▶ It is a malicious program that may be installed in the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information.
- ▶ With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated email address



PREVENTIVE MEASURE

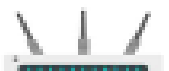
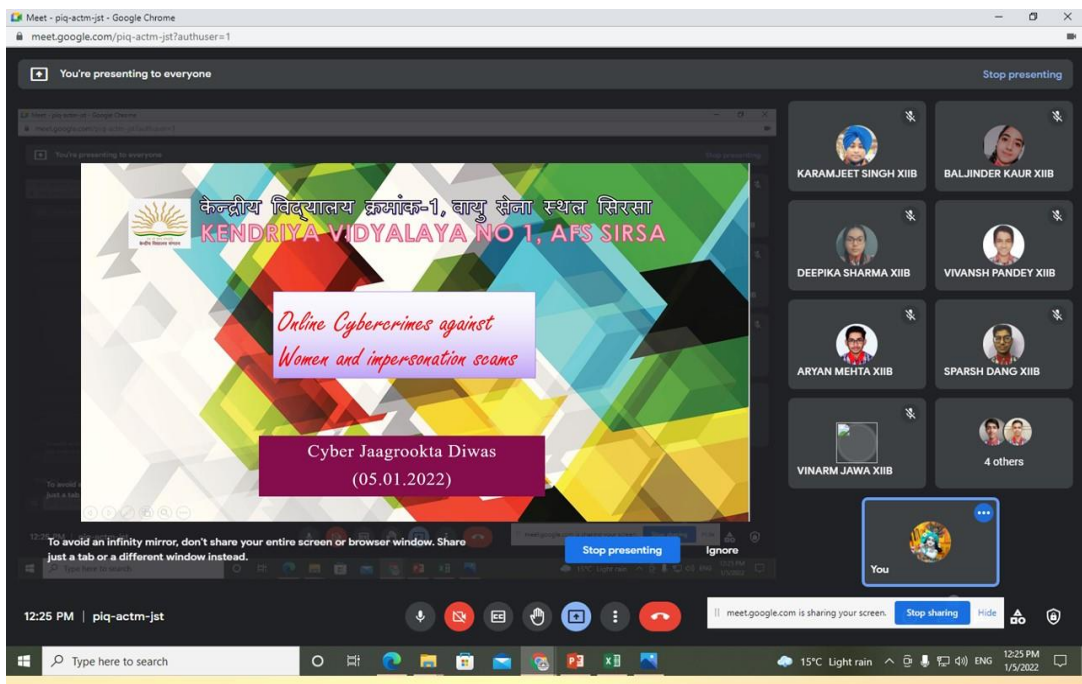
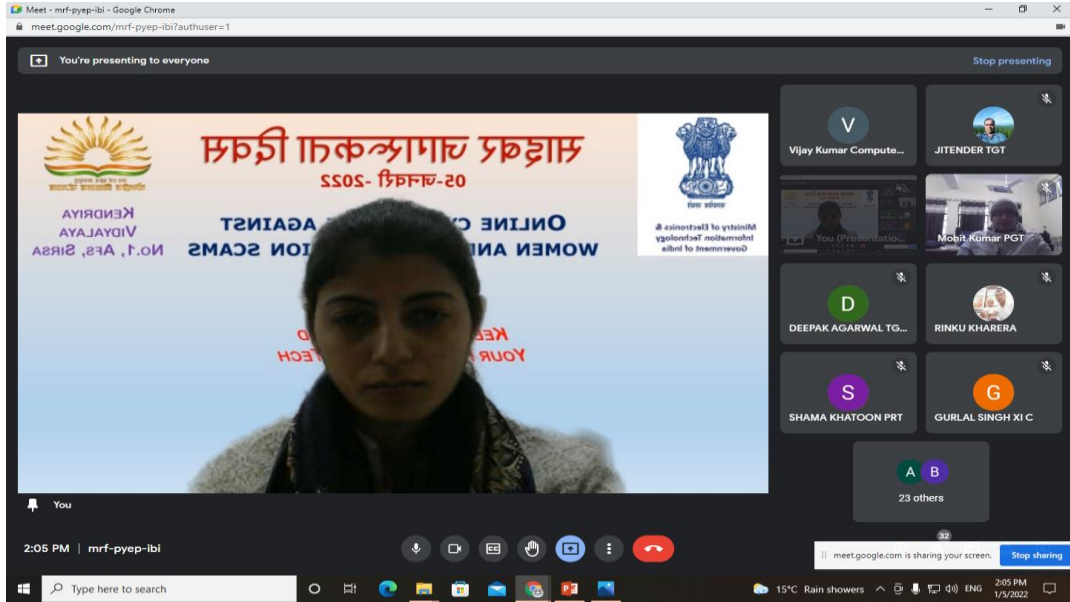
Cybercrime of any nature and gravity should be reported at the police station or Cyber Cell. It is always advisable to place it on records with the authorities concerned.

This will not only help the police to investigate the crime that you have faced but will also help them to understand and analyse the modus operandi of the criminals and take corrective actions for preventions and detections.

CYBER JAAGROOKTA DIWAS

Month: JANUARY

Topics Covered: **Online cybercrimes against women and impersonation scams**



CYBER JAAGROOKTA DIWAS

Month: FEBRUARY

Topics Covered: **Safety in Online Financial transactions.**

Safety in Online Financial Transactions



Cyber Jaagrookta Diwas (02.02.2022)

INTRODUCTION

- ▶ Online transaction covers both computer and mobile transaction.
- ▶ Allows to view recent transactions, print out statements, transfer funds between account and to make payments.
- ▶ Provides 24 hours access to bank account.
- ▶ Also known as online banking or internet banking.

STEPS IN ONLINE TRANSACTION

How it works???

1. The customer opens an account.
2. The customer receives a certificate.
3. The merchant receives a certificate.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment detail sent to the merchant along with customer digital certificate.
7. The merchant request payment authorization.

FEATURES OF ONLINE TRANSACTION

- ▶ Can log on from almost anywhere
- ▶ Makes all payment electronically
- ▶ Transaction speed
- ▶ Saves time
- ▶ Convenient
- ▶ Flexible



CYBER JAAGROOKTA DIWAS

Month: **FEBRUARY**

Topics Covered: **Safety in Online Financial transactions.**

SECURITY TIPS FOR TRANSACTION

Do not:

- ▶ Disclosure of personal information such as credit card no.
- ▶ Having other browser open.
- ▶ Download or open files from strangers.
- ▶ Telling id and password in e-mail.



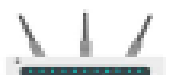
STEPS IN ONLINE TRANSACTION

8. The payment gateway authorizes the payment.
9. The merchant confirms the order.
10. The merchant provides goods or services as per order.

So by using digital certificate payment details are kept secret from merchant. he can't read it!!

E-MONEY

- ▶ E-money is another way of making payments on internet.
- ▶ Its nothing but money represented in computer files(binary form).
- ▶ Also known as electronic cash or digital cash.





CYBER JAAGROOKTA DIWAS

Month: FEBRUARY

Topics Covered: **Safety in Online Financial transactions.**



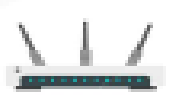
DISADVANTAGES

- ▶ Transaction can be impacted if the database is unavailable.
- ▶ System failure or network availability.
- ▶ Also requires offline maintenance.
- ▶ Can be complex for beginners.
- ▶ Online transaction can be complete success or complete failure.

SECURITY TIPS FOR TRANSACTION

Do not:

- ▶ Disclosure of personal information such as credit card no.
- ▶ Having other browser open.
- ▶ Download or open files from strangers.
- ▶ Telling id and password in e-mail.



CYBER JAAAGROOKTA DIWAS

Month: FEBRUARY

Topics Covered: **Safety in Online Financial transactions.**

SAFETY TIPS FOR TRANSACTION

Do not:

- ▶ Disclosure of personal information such as credit card no.
- ▶ Having other browser open.
- ▶ Download or open files from strangers.
- ▶ Telling id and password in e-mail.

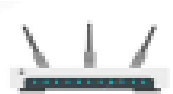
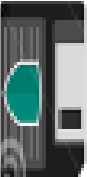
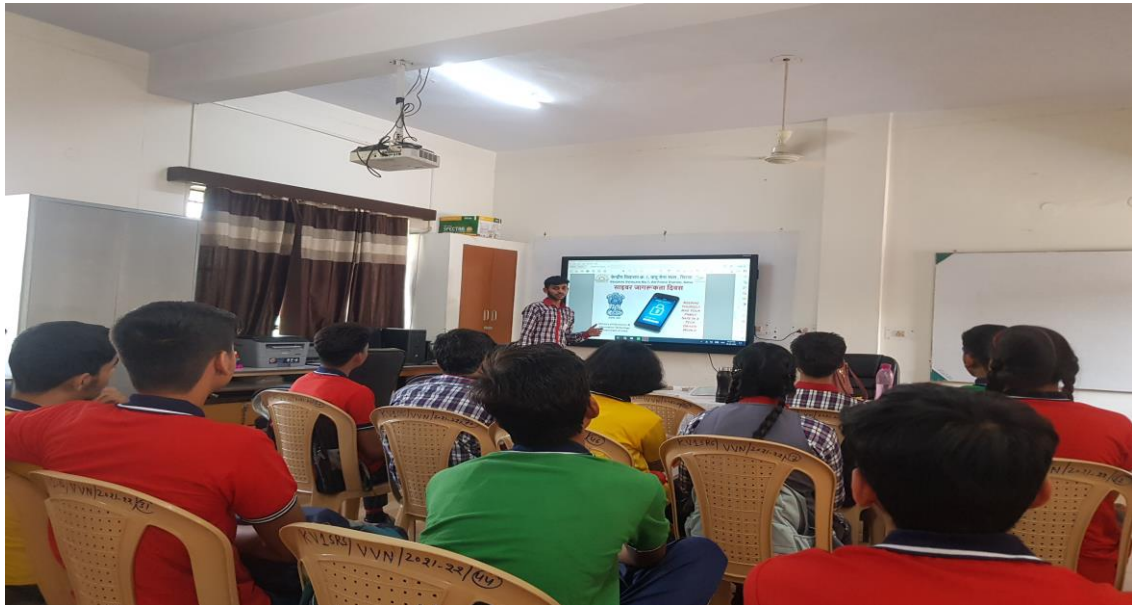




CYBER JAAGROOKTA DIWAS

Month: **APRIL**

Topics Covered: **Seminars on Cyber Security Awareness**

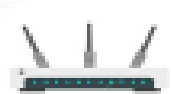
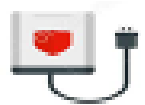
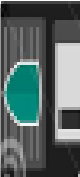




CYBER JAAGROOKTA DIWAS

Month: **APRIL**

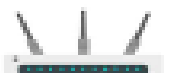
Topics Covered: **Seminars on Cyber Security Awareness**



CYBER JAAAGROOKTA DIWAS

Month: MAY

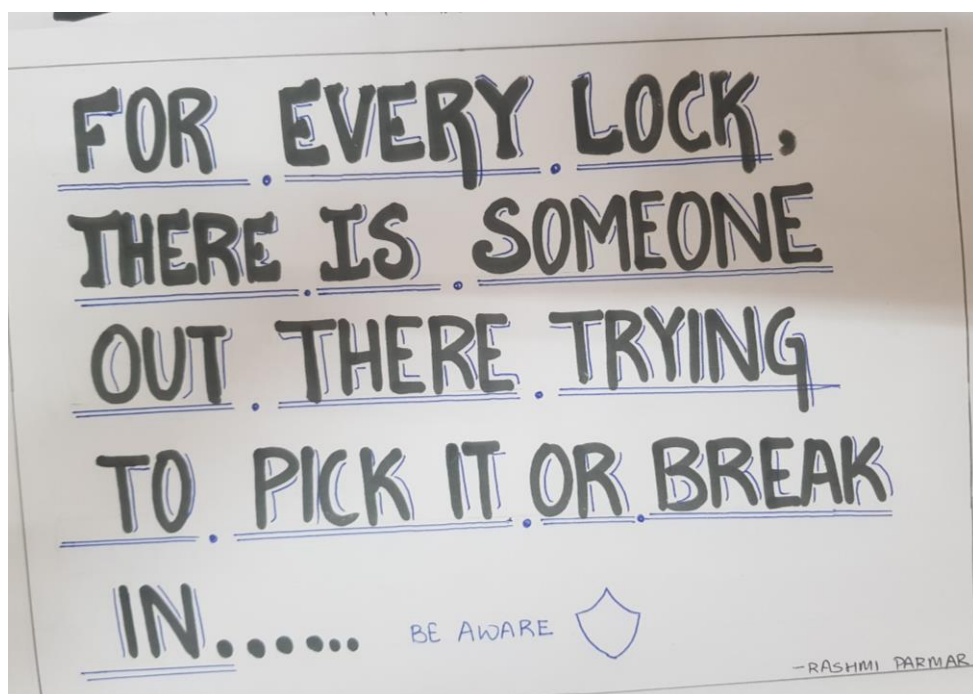
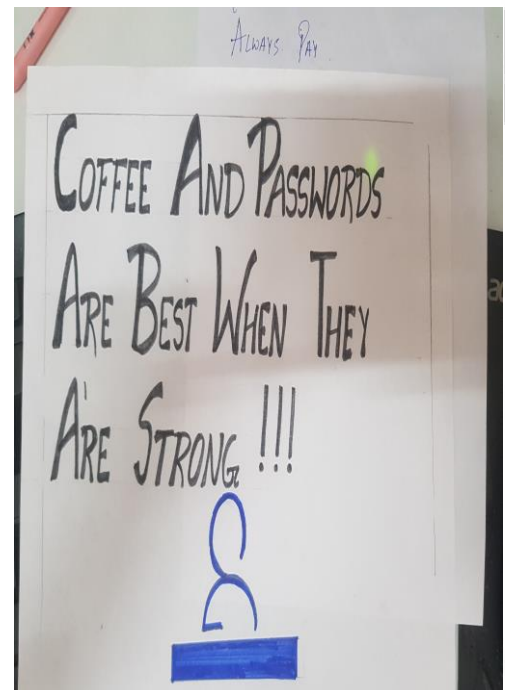
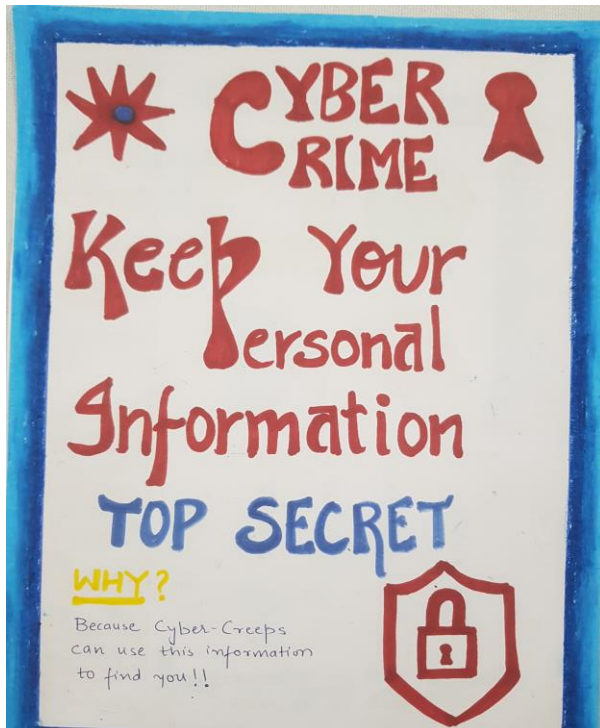
Topics Covered: **Poster making/ Slogan writing on Cyber Security Awareness.**



CYBER JAAGROOKTA DIWAS

Month: MAY

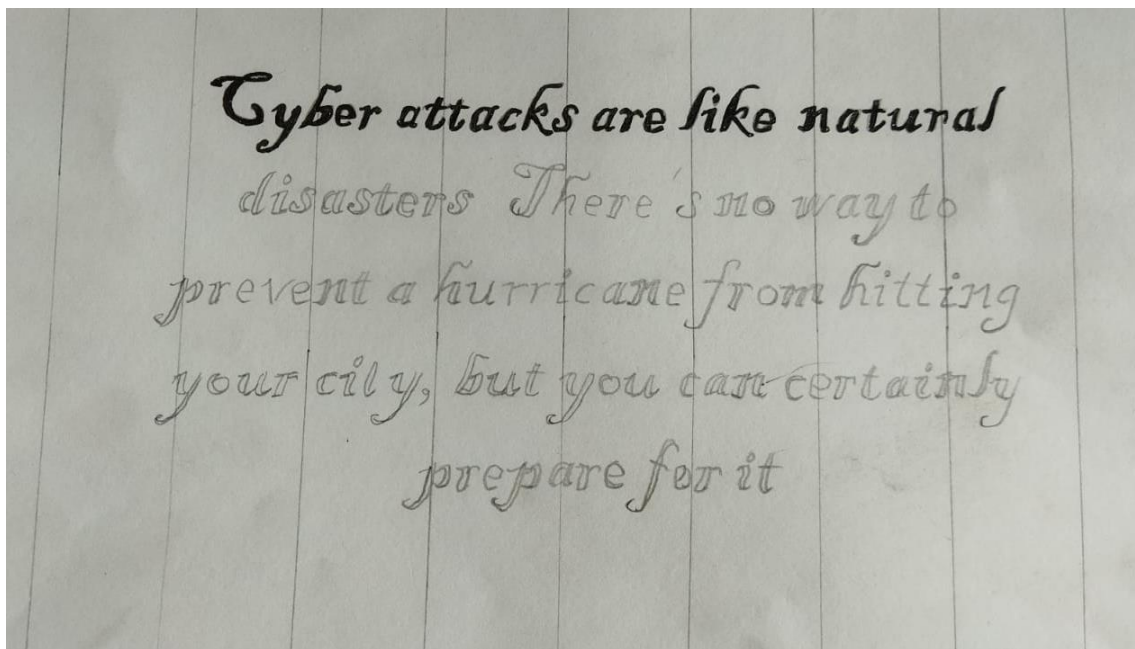
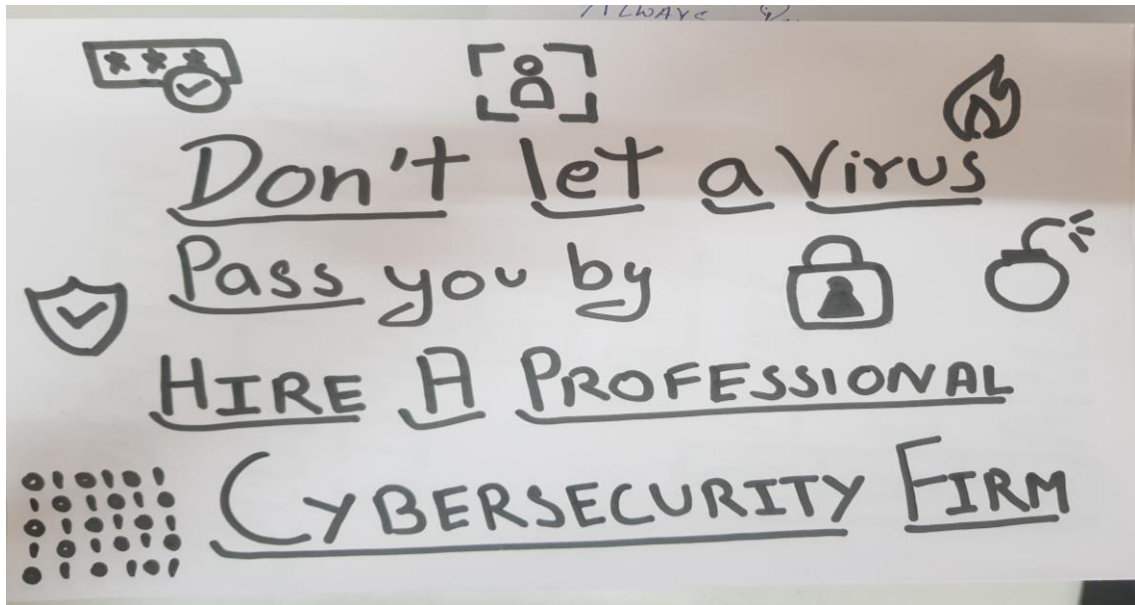
Topics Covered: **Poster making/ Slogan writing on Cyber Security Awareness.**



CYBER JAAGROOKTA DIWAS

Month: MAY

Topics Covered: **Poster making/ Slogan writing on Cyber Security Awareness.**



CYBER JAAAGROOKTA DIWAS

Month: JUNE

Topics Covered: **Short stories/ Essays writing on Cyber Security Awareness.**

Short Story on Cyber Security Awareness

1st June, 2022

A Couple of days ago, internet banking was blocked due to three unsuccessful attempt of accessing using a wrong or forgetted password of SBI internet banking account. But it was urgent to do the transactions, so I start looking for other alternative like google pay, Paytm etc. But huge amount needed to be transacted that was not feasible using these alternatives.

Further, I tried to contact SBI helpdesk to restore banking services by searching contact number on google. I found a mobile number as well as a landline number. But it was late evening so I dialed mobile number thinking office hours are closed now. No one picked the call but after a few moments, I got a call pretending calling from SBI helpdesk. I narrated the whole story that I am unable to utilize internet banking services.

After listening the whole story, fake SBI caller asked me to click on the link shared by him to restore back the banking services. Before clicking on link, I thought twice and lied to the caller that I am out of internet connectivity.

CYBER JAAGROOKTA DIWAS

Month: JUNE

Topics Covered: **Short stories/ Essays writing on Cyber Security Awareness.**

By listening that I won't click anyhow and assuming that I am aware of his trick, He started behaving rudely on the phone call that clearly reflecting that he was trying to trick me to get all the amount from my account and disconnected the call.

From the story, it can be concluded that **no body should trust on anyone on the call seeking your personal information in order to complete KYC, convincing you to click on some link, installing apps on your android & many more such activities to fall prey you.**

It's a great initiative by govt. to celebrate **Cyber Jaagrookta Diwas** on first wednesday of every month to sensitize the people about cyber threats by delivering lectures/sessions, slogan writings, poster making, organising seminars, essay writing, short stories on cyber security awareness. **These types of programs keeps on organising to protect the people in the cyber world.**

CYBER JAAGROOKTA DIWAS

Month: JUNE

Topics Covered: **Short stories/ Essays**
writing on **Cyber Security Awareness.**

CYBER SECURITY IN INDIA

Cyber security means protecting data, networks, programs and other information from unauthorized or unintended access, destruction or alteration. The rapid development of technology and the availability of the internet to the majority of public widens the path of cyber-crime. In this era where cyber security is a major concern, the use of computers has become common-place. With the increasing penetration of internet, cyber security is paramount for India's development. Threats from people with malicious intent may be due to negligence and vulnerabilities.

Various types of attacks like virus, malware, spyware, phishing, ransomware, fraud etc.. To other computer systems, infected web pages and malicious websites allow hackers to gain illegal access. Opening email attachments carrying viruses, clicking on malicious links or websites or inadvertently downloading any dangerous programs or installing infected app on mobile.

Attackers can be crackers or recreational hackers, terrorists.

There is a great risk to an individual's personal information and financial transaction. It can be used for

CYBER JAAGROOKTA DIWAS

Month: JUNE

Topics Covered: **Short stories/ Essays**
writing on **Cyber Security Awareness.**

Date:
Page:

personal gain such as blackmailing and fraudulent transactions. It is also important for individuals, organizations and countries. India still ranks higher in cases of malware and ransomware attacks compared to global peers at 54% compared to 47% globally. Yahoo acknowledged that three billion email accounts were breached in 2013. In India - Reliance Jio, IRCTC, Yes Bank etc. McAfee Labs researcher 244 new cyber threats in India every minute. The increasing use of Internet and social media has made cyber security even more important. Now we need more advanced security system to reduce the threat. Regular updates of antivirus i.e. genuine product only. More awareness among the public, users should be vigilant about the security of the data. There is a need to implement better cyber security laws by the government like National Cyber security Policy 2013, latest SC Directives to government for data privacy.

Thank You!!

- RASHMI PARMAR
XII - SCIENCE

CYBER JAAGROOKTA DIWAS

Month: JULY

Topics Covered: **Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.**

Browser Security

Web browser is used to access the information and resources on the world wide web. It is a software application used to trace and display the web page.

- Always update your Web Browser with latest patches.
- Use privacy or security settings which are inbuilt in the browser.
- Also use content filtering software.
- Always have Safe Search "ON" Search Engine.

Desktop Security

Always update Operating System with latest patches before using them

Use strong passwords and change regularly

Never keep any of your sensitive documents on your tabletop

Never install unknown or unsolicited software on your computer

Secure Yourself Your System & Your Network

Giving access to a guest user creates a security risk. Disable it

Always maintain regular backup of your critical data

Secure your Internet Connectivity with strong password

Never open email attachments if the subject line is questionable or unexpected

UPI Security

- Beware of Mobile phishing.
- Keep strong passwords for your phone as well as for your UPI application.
- Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.
- Use biometric authentication if possible.



CYBER JAAGROOKTA DIWAS

Month: JULY



Topics Covered: **Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.**



Juice Jacking



juice jacking is a security exploit in which an infected USB charging station is used to compromise connected devices. The exploit takes advantage of the fact that a mobile device's power supply passes over the same USB cable the connected device uses to sync data.

Types of juice jacking attacks

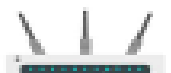
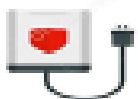


- Data theft
- **Malware installation**
- Multi-device attack
- **Disabling attack**

How to protect against juice jacking



- **Avoid public charging stations or portable wall chargers**
- Always lock your phone so it can't pair with a connected device.
- Choose a different method to charge your phone
- **Use USB pass-through devices**
- Your best defense against juice jacking is understanding the risks. Keep your device charged at all times, take a backup power bank, enable any security features on your device





CYBER JAAGROOKTA DIWAS

Month: JULY

Topics Covered: **Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.**

UPI Security



- Update your mobile OS and applications as often as possible to be secure from vulnerabilities.
- It is advisable for users to enable encryption and anti-virus software on the phone.
- Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device.
- Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

Google Map Security

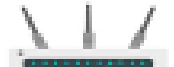


Google map application is a great technological advancement all over the world that helps millions of its users in getting quality geographical information for **finding paths, locations, places, distances, required time to travel at specific place,** and making rational decisions on the behalf of provided information.

Preventive Measures for OTP Fraud



- Not share your OTPs over the phone.
- **App pin, UPI pin, CVV number, expiry date of debit card and 16 digit debit card number is for personal use. These should never be shared with anyone in any circumstances.**
- Never reveal your account related information on Social Media.

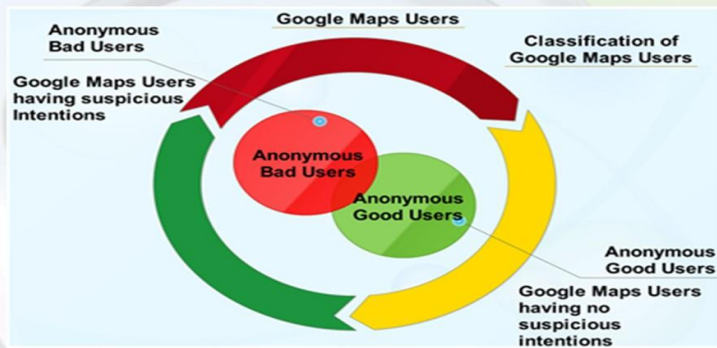


CYBER JAAAGROOKTA DIWAS

Month: JULY

Topics Covered: **Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.**

Google Map Security concerns



Google Map Security Preventive measures

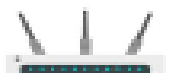
- Initiate Sign up Process
- Monitoring & Reviewing Agreement
- Session logs, browsing history and activity logs must be maintained for each user.



OTP Fraud

- OTP is an added factor of authentication and is enabled by a Bank for verifying whether the transaction is initiated by the user or not.

Dear Valued Customer, As a security measure, we recommend to have your HDFC Bank card ending with 7815 reissued. We are unable to reach you to get your confirmation for reissue, hence please contact phone banking @ 480-00-1900 for further assistance.

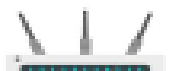
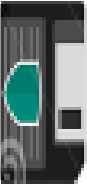




CYBER JAAGROOKTA DIWAS

Month: JULY

Topics Covered: **Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud.**



CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**

केन्द्रीय विद्यालय क्र.-1, वायु सेना स्थल, सिरसा
KENDRIYA VIDYALAYA No.1, AIR FORCE STATION, SIRSA
आज़ादी का अमृत महोत्सव
CYBER JAGROOKTA DIWAS (03-जुलाई -2022, बुधवार)
DEBIT/CARD CARD FRAUD, EMAIL SECURITY, MOBILE PHONE SECURITY

BEST PRACTICES FOR EMAIL SECURITY

- 01 Back up critical files
- 02 Educate employees
- 03 Automate email encryption
- 04 Implement multifactor authentication
- 05 Secure the email gateway

THE IMPORTANCE OF MOBILE APP SECURITY TESTING

Debit/Credit Card

A debit/ Credit card is a payment card that deducts money directly from a consumer's checking account when it is used.

Email Security

Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise.

What is Mobile Security?

Mobile security, which refers to the protection of mobile devices against cybersecurity threats, is a top-of-mind concern for today's companies due to the growing use of mobile devices for business purposes.

03-जुलाई -2022, बुधवार



CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**

What Is Debit Card Fraud?

❖ Debit card fraud is when someone gets access to your debit card number or PIN and makes unauthorized purchases or withdrawals from your account.

Here are some ways that debit card fraud might occur:

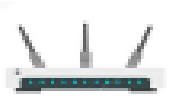
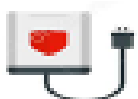
- ❖ A fraudster installs a card skimming device to a gas station fuel pump, skims your debit card information and uses it to drain your bank account.
- ❖ A service or repair person finds old statements in your home, steals your account number and racks up thousands of dollars in fraudulent charges.
- ❖ You get an email that links to a fraudulent retail store where your debit card number is collected and used to commit fraud.
- ❖ A data breach happens at your bank and hackers run off with your personal data.

Preventive measures for Debit Card Fraud

- ❖ Be careful about where you store your data. Avoid storing your debit card number or PIN on your device or sending it through email.
- ❖ Protect your debit card when shopping online. Scrutinize online stores before shopping because scammers can set up shops with bad intent.

There are several precautions to take when making online transactions

- ❖ Before entering debit card information, make sure there's an "https" (the "s" means secure) before the website name in the address bar and that there's a padlock icon next to it.
- ❖ Watch out for phishing scams, which often come in the form of fraudulent emails pretending to be from banks or retailers.
- ❖ Only give a business your debit card number if there's a valid reason and after you've determined that the company is reputable.
- ❖ Avoid making purchases on unsecured networks.





CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**

Abuses of email

- ✓ phishing attempts
- ✓ spoofing
- ✓ spam phishing
- ✓ malware delivery
- ✓ business email compromise (BEC)
- ✓ denial of service (DoS) attacks

03 जुलाई - 2022, बुधवार

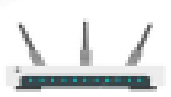
Email security Best Practices

- ❖ Train on anti-phishing: Phishing is a common email threat. It's important to train users to avoid risky behaviors and spot phishing attacks that get through to their inbox.
- ❖ Use domain authentication: The use of domain authentication protocols and techniques, including domain-based message authentication, reporting and conformance, can help to reduce the risk of domain spoofing.

Email security best practices

- ❖ Enforce encrypted connections. All connections to and from an email platform should occur over an SSL/TLS connection that encrypts the data as it transits the public internet.
- ❖ Encrypt email: While perhaps not an ideal option for every user at every organization, encrypting email messages provides an additional layer of privacy that can help to protect against unauthorized information disclosure.
- ❖ Create strong passwords: For users, it is important that any passwords are complex and not easy to guess. It's often recommended that users have passwords with a combination of letter, numbers and symbols.
- ❖ Implement 2FA or MFA. While strong passwords are helpful, they often aren't enough. Implementing two-factor authentication (2FA) or multifactor authentication (MFA) provides an additional layer of access control that can help to improve email security.

03-जुलाई - 2022, बुधवार



CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**

CYBER SECURITY AWARENESS FOR DEBIT/CARD CARD FRAUD, EMAIL SECURITY , MOBILE PHONE SECURITY

Top mobile security threats

- Malware attacks
- Phishing
- Lost or stolen devices
- Cross-app data sharing
- Unpatched OSes

03-जुलाई -2022, बुधवार

CYBER SECURITY AWARENESS FOR DEBIT/CARD CARD FRAUD, EMAIL SECURITY , MOBILE PHONE SECURITY

SMART PHONE SECURITY THREATS

- Downloadable Applications Threats:**
 - ★ Malware
 - ★ Spyware
 - ★ Privacy
 - ★ Zero Day Vulnerabilities
- Network and WiFi Security Threats:**
 - ★ Network Exploits
 - ★ WiFi Sniffing
 - ★ Cross-Platform Attacks
 - ★ BOYD
- General Cyber Security Threats:**
 - ★ Phishing
 - ★ Social Engineering
 - ★ Drive By Downloads
 - ★ Browser Flaws
 - ★ OS Flaws
 - ★ Data Storage
- Physical Threats:**
 - ★ Loss/Theft

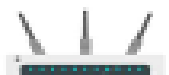
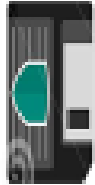
03-जुलाई -2022, बुधवार



CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**



CYBER JAAGROOKTA DIWAS

Month: **AUGUST**

Topics Covered: **Debit/Credit card fraud, email security, mobile phone security**



मोबाइल एप्लिकेशन सुरक्षा

मोबाइल ऐप्स डाउनलोड करने के लिए केवल आधिकारिक स्टोर्स का प्रयोग करें		शीर्षक या विवरण में वर्तनी की असुद्धियों की जांच करें	
लंबे समय तक उपयोग में न रहने वाले ऐप्स को अनइन्स्टॉल कर दें		खरीदारी छूट का वादा करने वाले ऐप्स से सावधान रहें	
किसी भी मालवेयर को हटाने के लिए अपने फोन के फैक्ट्री सेटिंग्स को रीसेट करें		समीक्षाओं को पढ़कर ऐप्स और उनके डेवलपर्स के बारे में अच्छा शोध करें	
आपके द्वारा डाउनलोड किए जाने वाले प्रत्येक ऐप के लिए अनुमतियों की समीक्षा सुनिश्चित करें		ईमेल, सोशल मीडिया आदि में दिए गए लिंक्स पर क्लिक करके ऐप्स इंस्टाल करने से बचें	
हमेशा एक अद्यतित एंटी वाइरस सुरक्षा समाधान का इस्तेमाल करें		प्रकाशन तिथि को देखें। एक नकली ऐप में हाल में ही प्रकाशित तिथि होगी	



स्टोरेज डिवाइसों(भंडारण उपकरणों) को रिसाइकिल करने से पहले डेटा का सुरक्षित निस्तारण सुनिश्चित करें।

Ensure secure disposal of data before recycling storage devices

CYBER JAAGROOKTA DIWAS

You are the
best defence!

Technology is only a small part of Cyber Defence

- You are the most important person – protect yourself
- For businesses/family the most important and best defence is Cyber Security
- Aware employees – train your staff/family

Always be aware!
Always be on your guard!

THANKYOU