***CyberJagrooktaDiwa*, a monthly awareness program on first Wednesday of each month to safeguard against cyber frauds and cyber crimes organised by *ElderRecreationActivities* Trust started w.e.f. 1.5.2024**

01.05.2024

ସାଇବରଠକେଇଓଅପରାଧରୁରକ୍ଷାପାଇବାପାଇଁଇଣ୍ଟରନଟେ୍ବ୍ୟବହାରକାରୀଙ୍କୁସଚତେନକରିବାଉଦ୍ଦଶ୍ୟରପ୍ରତ୍ୟକେମାସରପ୍ରଥମବୁଧବାରସାଇବ ରଜାଗୃତଦିବସ (***CyberJagrooktaD***

)ପାଳନଅବସରରନିେକଟରଭୁେବନଶ୍ରେଡିସିପିଙ୍କଦ୍ୱାରାସାମ୍ନାକୁଆସିଥିବାସାଇବରଠକେଇସମ୍ପର୍କରଉେକ୍ତଭିଡିଓବାର୍ତ୍ତାକୁଅବଗତରହିବାରଗୁରୁତ୍କୁଦର୍ଶାଉଛୁ।ସାଇବରଠକେଇପ୍ରତିସତର୍କରୁହନ୍ତୁ !

ଦସ୍ୱାକରିଆପଣଅଜାଣତରସେମ୍ମୁଖୀନହଉେଥିବାକୈାଣସିସାଇବରସଙ୍କଟପାଇଁନିମ୍ନଲିଖିତସମ୍ପର୍କଗୁଡିକପ୍ରତିଧ୍ୟାନଦିଅନ୍ତୁଯହେତୁଆମକୁସାଇବରଠକ ଇେମୁକ୍ତଜୀବନଯାପନକରିବାକୁପଡ଼ିବ।***Pleasetakenoteofthefollowingcontactsforanycybercrisesyoumayencounterinadvertently*** .

* National helpline (cyber fraud) 155260, and 1930

*Cyber police help desk - 7440006709

*Cyber fraud in Odisha region - 0674-2913100

*Mail id cybercrime.gov.in/webform/cyber_suspect.aspx

*Help line in Odisha police for senior citizen-1090

* PhonePe Customer Care 080-6872 7374 or 022-6872 7374

* PayTm Customer Service:+91 120 445 6456 (for Bank, Wallet and Payments)

* Google Pay Customer Care- 1800-419-0157

05.06.2024 -Today is the first Wednesday of the month, which means it's ***CyberJagrooktaDiwas*** . Celebrated on the first Wednesday of every month, this day is dedicated to creating awareness and sensitizing internet users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.This month's issue focuses on "***Howtohandlecookiestoavoidcyberfraud***," ***includingtipsoncheckingandblocking browsercookies***."

Keypointsyouneedtoknow : ***BrowserCookiesandTheirPurpose***:

• Browser cookies are small data files stored by your internet browser when you visit websites.

• They help websites remember your preferences, login status, and customize suggestions for your next visit.

• However, cookies can also be exploited by cybercriminals.

CookieTheftandRisks:

• Cookie theft occurs when cybercriminals steal these cookies to gain unauthorized access to your accounts.

• Malware is often used to copy cookie data and send it to attackers.

• Valuable accounts (e.g., banking, social media) are targeted for financial gain or identity theft.

ProtectingYourself:

• Safe Browsing Habits:

• Practice safe browsing to keep cookies out of criminals' hands.

• Clear your browser cache periodically to manage stored cookies.

• Use multifactor authentication (MFA) for added security.

• Close Sessions and Clear Cookies:

• Log out of websites when not in use to let cookies expire.

• Regularly delete cookies from your browser.

Remember, staying vigilant and informed helps safeguard your online privacy!

Howtocheckmybrowser'scookies?

Instructions for checking cookies in popular web browsers:

• ***GoogleChrome***:

• Open Google Chrome.

• Click the three vertical dots (⋮) in the top-right corner.

• Select “Settings.”

• In the left panel, click “Privacy and security.”

• Click “Cookies and other site data.”

• Choose “See all site data and permissions” to view your cookies. You can sort by most visited, data stored, or name. Adjust permissions or delete cookies as needed.

• ***MicrosoftEdge*** :

• Open Microsoft Edge.

• Click “Settings and more” (three horizontal dots) in the upper right corner.

• Select “Settings” > “Cookies and site permissions.”

• Click “Manage and delete cookies and site data.”

• Choose “See all cookies and site data” to view all cookies2.

Remember to manage your cookies regularly to enhance your online privacy and security!

Howtoblockthird-partycookies?

Blocking third-party cookies can enhance your privacy by preventing advertisers and other third-party services from tracking your browsing activities. Here’s how you can block third-party cookies in some of the most commonly used web browsers:

• ***GoogleChrome***:

• Open Chrome and click the three vertical dots (⋮) in the top-right corner.

• Select “Settings.”

• Click “Privacy and security,” then “Cookies and other site data.”

• Choose "Block third-party cookies."1

• ***MicrosoftEdge*** :

• Open Edge and click the three horizontal dots (…) in the top-right corner.

• Select “Settings” > “Cookies and site permissions.”

• Click on “Manage and delete cookies and site data.”

• Toggle on "Block third-party cookies.

Remember, while blocking third-party cookies can help protect your privacy, it may also affect the functionality of some websites. If you encounter issues with websites after blocking third-party cookies, consider adding exceptions for sites you trust.

03.07.2024 Today is the first Wednesday of the month- July which means it's ***CyberJagrooktaDiwas*** . It is elebrated on the first Wednesday of every month, to creating awareness and sensitizing internet users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.This month's issue focuses on

"***Howtoidentifyfakecallsorfakemessages***? ***Knowtheveryeasyprocess***"

There has been a huge increase in digital transactions in the country. This has led to an increase in online fraud in India. If you are a little lax, you may get cheated heavily. So it has become very important to be cautious while making online transactions and taking online services .

The most popular way to carry out online fraud is through messages by sending fake messages on SMS, e-mail, WhatsApp or any other electronic media. Therefore, it has become very important to identify messages related to fraud or scam.If you receive any bank related message, then you must investigate it. If you show a little caution, you can immediately identify a fraud call or message and avoid becoming a victim of fraud. Here we are giving some such tips. Which can be easily identified.

Howtoidentifyfraudmessages :

You can identify fake messages by paying attention to the name and number. If you receive a message or call from a personal number, it may be a fraudulent message. The messages sent by the bank come with names like VM-ICICI Bank, JD-ICICIBK. No bank ever sends messages from a personal number.There is no threat of termination of service :

Whenever you receive a call that your service will be terminated or any such threat, you should be cautious. Whenever your service is about to end, a reminder comes from the bank before that. Banks never call and threaten you.

Avoidfakelinks :

Many times such messages also come in which messages are sent with links for updating the account and other information by clicking on the link. These links are sent to you by hackers. By clicking on them, people become victims of fraud.Many times such a link can take you to a phishing site. Which may contain malware. Through this, hackers get all the bank information. Using which hackers withdraw all the money from your account.

Ifaccidentallyyougaveyournumberandfullnametoascammer. WhatdoIdo?

In India, Telecom Regulatory Authority of India (TRAI) has created a NDNC Filter i.e. National Do Not Call Registry which is fully run by Indian Govt. The main purpose for creation of NDNC is to prevent unwanted Marketing SMS and calls from Telemarketers.If you do not want to receive any promotional sms or calls from any company, you can add your number in NDNC registry.

To StartDND (***DonotDisturb***) ***Servicesfollowbelowprocess*** –To add your number in NDNC list you need to send a SMS to 01909.You will instantly receive a sms for registration in NDNC list; it may take upto 2-3 days to activate DND on your number. Check whether your number is added in NDNC list from here.If you do not get confirmation call from TRAI, try calling 1909 and then follow Instructions.

ToStartDND (***DoNotDisturb***) ***Servicesfromanyparticularcategoryfollowbelowsteps***-

TRAI has also given an option to opt out for promotional sms from particular category; they have divided it into 7 categories.

1 .Banking/Financial Products/ Insurance/Credit cards
2 .Real Estate
3 .Education
4 .Health
5 .Consumer Goods and Automobiles
6 .Entertainment/Broadcasting/Communication/IT

7 .Tourism and Leisure
If you want to stop SMS sms from only Real Estate thensend an SMS as “STOP 2” and send it to 1909.After registering your number into NDNC list you will able to avoid all unnecessary SMS and Calls.Remember, staying informed and practicing good cybersecurity habits can go a long way in protecting yourself online!

07.08.2024*CyberJagrooktaDiwas* Today is the first Wednesday of the month- August which means it's ***CyberJa*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

This month's issue focuses on ***howtofileacomplaintforscamcallsormessagesthroughtheChakshuserviceontheSancharSaathiPortal***.
The internet is a double-edged sword for seniors. It offers countless conveniences and opportunities for various connection while posing significant risks for older adults. They are particularly vulnerable to fraud and cyberattacks due to various factors, including a lack of familiarity with technology and the increasingly sophisticated tactics used by cybercriminals. So any user faced a cyber fraud, then ***here'sastep-by-stepguideonhowtofileacomplaintthroughtheChakshu*** an initiative by Govt.of India.
To avail this service, click on https://www.sancharsaathi.gov.in
• Navigate to Chakshu:
• On the homepage, find the section for "Chakshu" or "Fraud Reporting". This might be under a menu or prominently displayed on the homepage.
• Access the Complaint Form:
• Click on the option to report a scam or fraud. This should take you to a complaint form.
• Enter Your Details:
• Fill in your personal details such as your name, contact number, and email address.
• Provide information about the scam call/message, including the phone number from which you received the call/message.
• Describe the Incident:
• Write a detailed description of the scam incident. Include any relevant information such as the nature of the scam, what was said or written in the message, and any other pertinent details.
• Upload Evidence (if applicable):
• If you have any evidence, such as screenshots of the message or call logs, upload them using the provided option.
• Submit the Complaint:
• Review the information you have entered to ensure it is accurate.
• Click on the "Submit" button to file your complaint.
• Receive Acknowledgment:
• After submitting, you should receive an acknowledgment with a reference number. This reference number can be used to track the status of your complaint.
• Follow Up (if needed):
• If you need to follow up on your complaint, use the reference number to check the status on the portal or contact the relevant authorities through the provided contact details on the portal.
If you encounter any issues during the process, the portal typically has a help or FAQ section that can provide additional assistance.
N.B.***Pleasetakenoteofthefollowingcontactsforanycybercrisesyoumayencount*** .
* National helpline (cyber fraud) 155260, and 1930
*Cyber police help desk - 7440006709
*Cyber fraud in Odisha region - 0674-2913100
*Mail id cybercrime.gov.in/webform/cyber_suspect.aspx
*Help line in Odisha police for senior citizen-1090
* PhonePe Customer Care080-6872 7374 or 022-6872 7374

* PayTm Customer Service:+91 120 445 6456 (for Bank, Wallet and Payments)
* Google Pay Customer Care- 1800-419-0157

N.B. $\mathit{UpcomingCyberJagrooktaDiwasscheduledon}$ $4\mathit{th}.\mathit{Sept}$.'24 ($1\mathit{st}.\ \mathit{Wednesday}$) $\mathit{willexplorehowtodetectbysearchingunsafesiteswithhelpofGoogle's SafeBrowsingtechnology}$.

04.09.2024 $\mathit{CyberJagrooktaDiwas}$ –Today is the first Wednesday of the month- September which means it's CyberJ . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, $\mathit{ElderRecreationActivities-era}$ is conducting monthly awareness programs as part of its $\mathbb{D}\mathbb{i}\mathbb{g}\mathbb{i}\mathbb{t}\mathbb{a}\mathbb{l}$ $\mathbb{P}\mathbb{a}\mathbb{t}\mathbb{h}\mathbb{a}\mathbb{s}\mathbb{a}\mathbb{l}\mathbb{a}$ - $\mathit{EmpoweringElders}$.

This month's issue focuses on $\mathit{howtodetectbysearchingunsafesiteswithhelpofGoogle's SafeBrowsingtechnology}$.

According to a survey, cyber attack occurs every 39 seconds. This is where safe browsing comes into play.

Google's Safe Browsing technology detects unsafe sites and warns users when they attempt to navigate to dangerous sites or download dangerous files.

$\mathit{EnablingGoogle'sSafeBrowsingonasmartphonehelpsprotectyoufrompotentiallyharmfulwebsitesandonlinethreats}$. $\mathit{Here's astep-by-stepguidetoenableit}$:

$\mathit{ForAndroid}$ ($\mathit{GoogleChrome}$)

• Open Google Chrome: Launch the Chrome browser on your Android device.

• Access Settings:

• Tap the three vertical dots (menu) in the top right corner.

• Select "Settings" from the dropdown menu.

• Navigate to Privacy and Security:

• Scroll down and tap on "Privacy and security".

• Enable Safe Browsing:

• Tap on "Safe Browsing".

• You will see options like:

• Standard protection: Enables basic protection against dangerous sites and downloads.

• Enhanced protection: Provides stronger protection with proactive measures.

• Choose either "Standard protection" or "Enhanced protection" according to your preference.

• Confirm Your Selection:

• After selecting the desired level of protection, Chrome will automatically save your preferences.

$\mathit{ForiPhone}$ ($\mathit{GoogleChrome}$)

• Open Google Chrome: Launch the Chrome browser on your iPhone.

• Access Settings:

• Tap the three dots (menu) in the bottom right corner.

• Select "Settings" from the dropdown menu.

• Navigate to Privacy:

• Scroll down and tap on "Privacy".

• Enable Safe Browsing:

• Tap on "Safe Browsing".

• You will see options for Standard protection and Enhanced protection.

• Select your preferred protection level.

• Save Your Preferences:

• Once selected, Chrome will save the Safe Browsing settings automatically.

AdditionalTips:

• Update Chrome Regularly: Ensure your browser is updated to the latest version for the best security features.

• Review Safe Browsing Settings Periodically: As your browsing habits change, revisit the settings to ensure you're getting the level of protection you need.

This will help keep your smartphone safer while browsing the web.

N.B. $UpcomingCyberJagrooktaDiwasscheduledon$ 2nd.Oct.'24 (1st.)$willexploreanewUPIPaymentbylookingatfacewhichismoresecureddduringonlinetransactionse speciallyamongseniorcitizenswhomayoftenchallenge toremembermultiplePINsorPasswords$.

2.10.2024 -Today is the first Wednesday of the month- September which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its $\mathbb{D}igital\ \mathbb{P}athasala$ - ***EmpoweringElders***.

This month's issue focuses on $howtodetectbysearchingunsafesiteswithhelpofGoogle's SafeBrowsingtechnology$.
According to a survey, cyber attack occurs every 39 seconds. This is where safe browsing comes into play.
Google's Safe Browsing technology detects unsafe sites and warns users when they attempt to navigate to dangerous sites or download dangerous files.
$EnablingGoogle'sSafeBrowsingonasmartphonehelpsprotectyoufrompotentiallyharmf ulwebsitesandonlinethreats. Here'sastep-by-stepguidetoenableit$:
ForAndroid (***GoogleChrome***)
• Open Google Chrome: Launch the Chrome browser on your Android device.
• Access Settings:
• Tap the three vertical dots (menu) in the top right corner.
• Select "Settings" from the dropdown menu.
• Navigate to Privacy and Security:
• Scroll down and tap on "Privacy and security".
• Enable Safe Browsing:
• Tap on "Safe Browsing".
• You will see options like:
• Standard protection: Enables basic protection against dangerous sites and downloads.
• Enhanced protection: Provides stronger protection with proactive measures.
• Choose either "Standard protection" or "Enhanced protection" according to your preference.
• Confirm Your Selection:
• After selecting the desired level of protection, Chrome will automatically save your preferences.
ForiPhone (***GoogleChrome***)
• Open Google Chrome: Launch the Chrome browser on your iPhone.
• Access Settings:

• Tap the three dots (menu) in the bottom right corner.
• Select "Settings" from the dropdown menu.
• Navigate to Privacy:
• Scroll down and tap on "Privacy".
• Enable Safe Browsing:
• Tap on "Safe Browsing".
• You will see options for Standard protection and Enhanced protection.
• Select your preferred protection level.
• Save Your Preferences:
• Once selected, Chrome will save the Safe Browsing settings automatically.
AdditionalTips:
• Update Chrome Regularly: Ensure your browser is updated to the latest version for the best security features.
• Review Safe Browsing Settings Periodically: As your browsing habits change, revisit the settings to ensure you're getting the level of protection you need.
This will help keep your smartphone safer while browsing the web.

N.B. $UpcomingCyberJagrooktaDiwasscheduledon$ 2nd.Oct.'24 (1st.)$willexploreanewUPIPaymentbylookingatfacewhichismoresecureddduringonlinetransactionsespeciallyamongseniorcitizenswhomayoftenchallenge toremembermultiplePINsorPasswords$.

6.11.2024 --***CyberJagrooktaDiwas*** -- Today is the first Wednesday of the month- November which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its $\mathbb{D}igital\ \mathbb{P}athasala$ - ***EmpoweringElders***.

This month's issue $willexploreSpoofingAttackbycybercriminals$.

Before going to topic , let's know $whatisaSpoofingAttack$?

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source for the purpose of gaining access to personal information & acquiring money.

Howitworks?Cybercriminals are using various forms of communication methods to make themselves look legitimate to further convince the victim to reveal sensitive information. When the victim gives up this information, they compromise their security and the cybercriminals can use the information for their own malicious benefits.

$Herearefewofthemostcommontypesofspoofingattacks$.

* ***Websitespoofing*** - Generally, a cybercriminal creates a website that looks legitimate. The URL will resemble the site they're spoofing, but after closely examining the URL, you'll notice that there is something off. For example, instead of Google.com, the URL may look something like G0ogle.com. Another example of a fake message from RTO - For online payment of challan visit:https://echallanparivahan.in/you can also contact RTO office for disposal of challan.

Here the ORIGINALLINK https://echallan.parivahan.gov.in

FAKE LINKhttps://echallanparivahan.in

Their goal to steal sensitive information such as credit card numbers, login credentials, social security numbers and more by infecting your device with malware.

* ***Spoofedemails*** - The cybercriminal will send an email that seems to be coming from someone you know or a company you have an account with. You can check the actual email address by hovering sender's details. Upon further inspection, you'll notice the email address looks odd. For example, instead of support@[companyname].com, one character of the company name will be replaced with a different letter,

symbol or number.You may notice that the email is urging you to click on a link or attachment that can send you to a spoofed site or infect your device with malware.

* Spoofed calls - When we receive a phone call, our phones display a caller ID – revealing who's calling us. Typically, when our phones display that the call is a “Spam Risk” we tend to not answer because it's likely the call is a scammer or telemarketer. The cybercriminal easily gets you to pick up the phone and continues to pretend to be someone they're not. This can be dangerous because if you believe them, you may be tempted to share sensitive information they ask for – especially if it seems urgent.

* IP spoofing - Internet Protocol (IP) spoofing is used by cybercriminals to hide the real source of IP packets so it's difficult to know where an attack came from. Here the IP address is different from the actual source. It is commonly used to carry out DDoS and man-in-the middle (MITM) attacks – preventing the cybercriminals from getting caught by authorities and enabling them to bypass IP address blacklists. IP blacklisting is meant to filter out malicious IP addresses from accessing networks and is often used by organizations to prevent cyber attacks.

HowtoDetectSpoofingAttacks :

Spoofing can be hard to spot if you don't pay close attention. Here are a few warning signs to look out for.

* ***Useofurgentlanguage*** -

Urgent language through emails, phone calls or text messages can all be indications of spoofing. Such language could be prompting you to click on a link, attachment or urging you to reveal sensitive information.

* ***Poorspellingandgrammar*** -

When you receive emails or text messages with spelling and grammar issues, you should not trust them. Remember, legitimate companies will communicate with you in a formal manner – meaning their grammar should be correct and nothing should be spelled wrong.

* ***Weird-looking - URL*** - In order to check if a site is spoofed, it requires you to take a close look at the website address or URL. When a site is spoofed, the URL will look odd because one or more characters will be off. An example of a spoofed URL would be Amazonn.com instead of Amazon.com. If you notice this, it's a sign that the site you're on is spoofed.

Conclusion: So please stay protected from Spoofing Attacks . The best way to protect yourself from spoofing attacks is by knowing what they are and what they do. Only then can you know how to spot them and prevent yourself from becoming a victim of these types of attacks. If by mistake, you've been a victim of this type of attack , please report at cyber crime helpline number 1930 or website https://www.cybercrime.gov.in.

N.B. ***UpcomingCyberJagrooktaDiwasscheduledon*** 4th.Dec.'24 (1***st***.) will explore on ***HowtoStayProtectedFromSpoofingAttacks*** " ***byusingaURLcheckersuchasGoogle'sTransparencyReport***.

4.12.2024 -.***CyberJagrooktaDiwas*** Today is the first Wednesday of the month- December which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

Last month we discussed about different types of spoofing attacks. This month's issue ***willexploreHowtoStayProtectedFromSpoofingAttacks*** " ***byusingaURLcheckersuchasGoogle'sTransparencyReport***.

As we increasingly rely on the internet for daily activities, we discover thousands of new unsafe sites .When you detect unsafe sites, you show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.If you’re not feeling confident that a website is safe,

the easiest thing to do is enter it into a website checker like the Google Transparency Report. It'll tell you whether the website is safe or not .

Let's get started !

VisittheGoogleTransparencyReportwebsitebyclickingfollowinglink

https://transparencyreport.google.com/safe-browsing/search

Check site status by entering the URL for which doubt arises and see the results. . If the website is marked as "not safe," avoid visiting it.

Conclusion:

By following these steps you can significantly reduce your risk of falling victim to spoofing attacks and other cybercrimes. If by mistake you encounter suspicious activity, report it to the appropriate authorities or cyber crime helpline number 1930 or website https://www.cybercrime.gov.in.

Remember, your online safety is in your hands. Stay vigilant and protect yourself!

N.B. ***UpcomingCyberJagrooktaDiwasscheduledon*** 1***st. January***'25(1***st.Wednes***sday)***willexploreonarecentcybercrimei.e. Cyberarrestandhowtoavoidbecomingavictimofdigitalarrestscam***?

8.1.2025 --Today is the first Wednesday of the month- January '25 which means it's ***CyberJa*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

This month's issue is focusing on a newest form of cyber scam i.e. "Digital arrest" that has affected more than 92,000 Indians in 2024 in which money is extracted through online transfers under the guise of resolving tax or legal dues. So we will explore ***how avoidbecomingavictimofdigitalarrestscam***?

Here the scammers intimidate the victims and falsely accuse them of illegal activities. They later demand money and puts them under pressure for making the payment. So the most important way to protect yourself from getting scammed is to be aware. Always stay vigilant against such crimes.
Herearesometipstosaveyoufromdigitalarrestscam:

Be suspicious of calls from fake officials claiming that you are in trouble. It is always important to remember that real law enforcement agency officials will never ask for payment or banking details.

Do not give in to the "pressure tactics" deployed by cyber criminals, who seek quick action by creating "a sense of urgency".

If you are suspicious about the call, verify their identity by directly contacting the relevant agency they are referring to. Try to be calm and do not panic.

Avoid sharing personal information and never disclose sensitive personal or financial details over the phone or video calls, especially to unknown numbers.

Remember, government agencies do not use platforms like WhatsApp or Skype for official communication.

If you think you are being scammed, never forget to report the incident to the local police or cyber crimeauthorities .

What to do if you are a victim of digital arrest scam and lost money?

If you are a victim of digital arrest scam, the first step is to immediately report your bank and freeze your account. You may contact the financial helpline1930 within 15-20 minutes to freeze any transfer.

File a complaint with the National Cyber Crime Reporting Portal (cybercrime.gov.in).

Always keep whatever evidence you have — call details, transaction details, messages, screen shot etc.

Seek help from a lawyer if needed. Stay safe online!

Conclusion: By following these steps you can significantly reduce your risk of falling victim to digital arrest scam.

N.B. ***UpcomingCyberJagrooktaDiwasscheduledon*** 5th. February '25 ***will*** be on the topic- How to check if somebody has used your Aadhaar card without your knowledge and how do you lock your Aadhaar card ?

HappyNewYear! ***Wishingyouayearofjoy***, ***happiness***, ***andfulfillment***.

5.2.2025 ---Today is the first Wednesday of the month-5th. February '25 which means it's ***CyberJa*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***. This month's issue is "***HowtoCheckifYourAadhaarCardHasBeenMisusedandStepstoLockIt*** ".

With the rise in online fraud individuals must be aware of their Aadhaar since it holds all your vital identification documents as a result it is becoming a target for scammers.

Fortunately, Unique Identification Authority of India (UIDAI) provides tools to check if your Aadhaar card has been misused and to secure it by locking or unlocking it. Here's a step-by-step guide:

1. ***CheckifYourAadhaarCardHas*** : You can monitor the usage of your Aadhaar card by checking its authentication history. Follow these steps:

Step 1: Visit the UIDAI website https://uidai.gov.in

Step 2: Click on "Aadhaar Authentication History" under the Aadhaar Services section.

Step 3: Enter your 12-digit Aadhaar number and the security code displayed.

Step 4: Click on "Generate OTP." An OTP will be sent to your registered mobile number.

Step 5: Enter the OTP and specify the date range for which you want to check the authentication history.

Step 6: Review the list of Aadhaar authentications. If you notice any unauthorized usage, report it to UIDAI immediately by calling their toll-free helpline (1947).

2. ***HowtoLockYourAadhaarCard***

Locking your Aadhaar card prevents unauthorized access to your biometric data and limits its usage. Here's how you can do it:

Step 1: Go to the UIDAI Resident website https://uidai.gov.in

Step 2: Select the "Lock/Unlock Aadhaar" option under Aadhaar Services.

Step 3: Enter your Aadhaar number and solve the security CAPTCHA.

Step 4: Click on "Send OTP" to receive a one-time password on your registered mobile number.

Step 5: Enter the OTP and proceed to lock your Aadhaar.

Note: After locking, you cannot use your Aadhaar number for authentication unless it is unlocked.

3. ***HowtoUnlockYourAadhaarCard***

If you need to use your Aadhaar for authentication, you can unlock it temporarily. Follow these steps:

Step 1: Go back to the UIDAI website.

Step 2: Click on "Unlock Aadhaar."

Step 3: Enter your Aadhaar number and CAPTCHA.

Step 4: Generate an OTP and authenticate yourself.

Step 5: Once unlocked, you can use your Aadhaar temporarily for the required service.

Conclusion: By taking these steps, you can safeguard your Aadhaar card from unauthorized access and ensure your personal information remains protected.

Please join the global celebration of ***SaferInternetDayonthecomingssecondTuesdayofFebruary*** (11.02.2025) !

This annual event raises awareness about online safety and promotes responsible digital citizenship.

Thisyear'stheme, "***Toogoodtobetrue? Keepingyourselfandotherssafefromscamsonline***," highlights the importance of being cautious and vigilant in the digital world. With the rapid digitization of financial services, online scams are becoming increasingly common and sophisticated.

On Safer Internet Day, let's start a conversation about how to:

- Develop awareness programs on Digital Financial literacy (DFL) giving importance to use safely digitally delivered financial products and services .

- A quick search can help spot fake news

- Respond to suspicious activity

- Report scams to the authorities Stay vigilant and secure!

N.B. ***UpcomingCyberJagrooktaDiwasscheduledon*** 5th.March '25 will highlight some Additional Tips Securing Your Aadhaar Card Safe .

5.3.2025 --Today is the first Wednesday of the month-5th.March '25 which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***. In its twelfth edition of The***CyberJagrooktaDiwas*** our topic is focusing on ***TipstoSecuringYourAadhaarCardSafewithstepbystepguide***. Protecting your Aadhaar card from cyber fraud is essential to safeguard your personal and financial information. Here are several steps you can take to enhance its security:

1. ***Lock/UnlockYourAadhaarNumber***:To prevent unauthorized use of your Aadhaar number, you can lock & unlock it . Detail procedure for locking &Unlocking described on last month's awareness program.

2 .***Lock/UnlockYourBiometrics***: Securing your biometric data (fingerprints and iris scans) ensures that no one can misuse them for authentication.

Steps to Lock/Unlock Biometrics:Visit the UIDAI Resident Portal https://resident.uidai.gov.in

Click on "Lock/Unlock Biometrics."Enter your Aadhaar number and the displayed Captcha code.

Click "Send OTP" and enter the OTP received on your registered mobile number. Toggle the biometric lock status as desired.

3. ***UseMaskedAadhaar***: A masked Aadhaar displays only the last four digits of your Aadhaar number, reducing the risk of misuse.

Steps to Download Masked Aadhaar:

Visit the UIDAI e-Aadhaar download page.https://myaadhaar.uidai.gov.in/genricDownloadAadhaar

Enter your Aadhaar number and the Captcha code.Select the option "Do you want a masked Aadhaar?"

Click "Send OTP" and enter the OTP received.Download the masked Aadhaar.

4. $\boldsymbol{RegularlyMonitorAadhaarAuthenticationHistory}$: Keeping an eye on your Aadhaar authentication history helps detect any unauthorized use.

Steps to Check Authentication History:Visit the UIDAI Resident Portal as above. Navigate to "Aadhaar Authentication History."Enter your Aadhaar number and the Captcha code.Click "Generate OTP" and enter the OTP received.View the list of authentication attempts.

5. $\boldsymbol{BeCautiouswithSharingAadhaarDetails}$: Avoid sharing your Aadhaar number, OTPs, or personal details with unverified entities.When providing a photocopy of your Aadhaar, write the purpose and date on it to prevent misuse.

6. $\boldsymbol{DownloadAadhaarOnlyfromOfficialSources}$: Always download your Aadhaar from the official UIDAI website to ensure its authenticity.

7. $\boldsymbol{UpdateYourMobileNumberandEmail}$: Ensure that your current mobile number and email are linked to your Aadhaar to receive timely notifications.

8. $\boldsymbol{ReportSuspiciousActivities}$: If you suspect any misuse of your Aadhaar, immediately contact UIDAI through their official website or helpline as discussed earlier .

Conclusion: By following these steps, you can significantly enhance the security of your Aadhaar and protect yourself from potential cyber frauds. However, you should know the places where there is a necessity to give your Aadhaar details. You shouldn't produce your Aadhaar details to anyone and everyone. It is utmost important to know the reason why you have been asked to give your Aadhaar details. There are high chances of your Aadhaar number been misused.

N.B. $\boldsymbol{UpcomingCyberJagrooktaDiwasscheduledon}$ 2nd.April '25 will explore on $\boldsymbol{AadhaarFaceAuthenticationunderwhichyourfacewillbeyourAadhaarcard}$. You will not have to show Aadhaar Card everywhere. This means that now the paperwork will end, which will make the services faster and safer. Detail step-by-step guide also will be given to install and to use it on your mobile phone.

2.4.2025 Today is the first Wednesday of the month-2nd April '25 which means it's ***CyberJag*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its $\mathbb{D}\mathrm{igital}\ \mathbb{P}\mathrm{athasala}$ - ***EmpoweringElders***.

In its thirteenth edition of The***CyberJagrooktaDiwas*** our topic is on $\boldsymbol{AadhaarFaceAuthenticationunderwhichyourfacewillbeyourAadhaarcard}$ as a result there is no need to show Aadhaar Card everywhere. Thus the paperwork will end which will make the services faster and safer.

Imagine walking into some cyber café to download an Aadhaar card or update your PAN details, some time

you have fallen prey to a sophisticated cybercrime network that fuels identity theft and financial fraud. A survey indicates that 87% of India's citizens believe one or more of their personal data elements are already in public domain or in databases and 50% worried about their Aadhaar security.

To face this acute problem , Ministry of Electronics & Information Technology (MeitY) has launched a new Aadhaar authentication portal , swik.meity.gov.in Aadhaar Face Authentication under which your face will be your Aadhaar card. Anyone can

installAadhaar Face Authentication on their mobile phone .

Here'sastep-by-stepguide :

Step 1: Check Device CompatibilityEnsure your smartphone has: A front-facing camera Android 9.0 or above (for Android users) A stable internet connection.

Step 2: Open Google Play Store on your mobile phone. Search for "AadhaarFaceRD" (byUIDAI).Download UIDAI AadhaarFaceRD .Click "Install" and wait for the app to download and install.

(Note: This app may not be available on iOS devices yet.)

Step 3: Open the AadhaarFaceRDAppLocate the AadhaarFaceRD app on your phone and open it.

Grant the necessary camera and storage permissions for the app to function.

Step 4: Perform Aadhaar Face AuthenticationEnter your Aadhaar Number or the required details.

Align your face within the frame and follow on-screen instructions for live facial scanning.

The system will verify the image with the Aadhaar database.

Step 5: Successful Authentication If successful, you will see a confirmation message. If unsuccessful, try again with proper lighting and a stable face position.

It works in collaboration with the Aadhaar Authentication User Agency (AUA), the KYC User Agency (KUA), and other entities.

Conclusions: It can significantly enhance the security of your Aadhaar and protect yourself from potential cyber frauds due to following advantages :

1 . Contactless (no fingerprint scanning required).

2 . Remote Access (can be used from a smartphone or laptop).

3. Quick & Secure authentication method.

4 .Useful for Elderly & Disabled Individuals who may have difficulty with fingerprints or OTP-based verification[8]

N.B. TheupcomingCyberJagruktaDiwason 7***thMay*** 2025 ***willfocusonarisingcyberthreatfakeIVRcalls***, a new scam designed to steal your money. This will cover:

What fake IVR calls are and how they operate

How to identify and avoid such fraudulent calls

Effective measures to protect yourself from IVR scams

Steps to take if you become a victim Stay informed, stay secure!

7.5.2025 Today is the first Wednesday of the month- 7th May '25 which means it's ***CyberJag*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

In its 14th episode of The***CyberJagrooktaDiwas*** we aim to raise awareness about a new cyber threat exploiting the recent Pahalgam attack to spread malware.

SobewareofMalwareHiddeninPahalgamAttackMedia !

TheThreat: ***MalwareDisguisedasEmotionalContent*** :

Cybercriminals are circulating images and videos related to the Pahalgam attack, urging users to "set this as your Display Picture - DP "or "watch this tourist's final message." These emotionally charged messages are designed to prompt users to download and share malicious content. Once engaged, the malware initiates a tactic known as 'push bombing' or 'MFA fatigue,' sending repeated login prompts to the victim's device in hopes of gaining unauthorized access.

(MFA is Multi-Factor Authentication. It is a security process that requires a user to provide two or more authentication factors to access a system, network, or application. This adds an additional layer of security to prevent unauthorized access.)

WhyEldersAre : Elderly individuals, often less familiar with digital security practices, may be more susceptible to these emotionally manipulative tactics. The use of heartfelt messages and familiar platforms increases the likelihood of engagement with malicious content.

HowtoProtect : Be Skeptical of Emotional Appeals: Avoid downloading or sharing content that plays heavily on emotions, especially if it urges immediate action.

● Verify Before Sharing: Confirm the authenticity of messages and media before forwarding them to others.

● Strengthen MFA Settings: Use biometric verification and set short expiration times for authentication prompts to reduce vulnerability.

● Educate and Inform: Share this information with peers and family members to spread awareness about such cyber threats.

Real-Lif : A Bengaluru resident received a message with a video titled "Final Moments of Pahalgam Tourist." After downloading, they were bombarded with login prompts and eventually lost access to their email and banking accounts. This incident highlights the real danger of such malware attacks.

Stayvigilantandprioritizedigitalsafety

For more information and resources, visit Cybersecurity Resources (Computer Emergency Response Team) website https://www.cert-in.org.in

N.B. TheupcomingCyberJagruktaDiwason 4***thJune*** 2025 ***willfocusonarisingcyberthreatfakeIVRcalls***, a new scam designed to steal your money. This will cover:

What fake IVR calls are and how they operate , How to identify and avoid such fraudulent calls

Effective measures to protect yourself from IVR scams , Steps to take if you become a victim Stay informed, stay secure!

4.6.2025 Today is the first Wednesday of the month- 4th June'25 which means it's ***CyberJag*** . It is celebrated globally on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.In its 15th episode of The ***CyberJagrooktaDiwas*** our topic is on ***WhatsappBlurryImageScam*** , a new type of scam that has emerged on WhatsApp these days. This is a very clever way to scam people using new technique i.e. ***Steganography*** , an art of hiding information ***.Oneclicktodownloadanyphotosharedbyscammersmightgivehackersaccesstopersonaldata, bankingapps, andevenyourentirephone, leadingtomassivefinanciallosses.***

In today's digital era , cybercriminals are targeting WhatsApp , one of the most widely used messaging platforms, that has become a hotspot for hackers.

Unlike conventional scams that depend on phishing links or OTP fraud, this scheme employs a more deceptive tactic by embedding malicious software within seemingly harmless image files, making it harder to detect and more dangerous for users.

Once the infected image is opened, the malware silently installs itself on the device. From there, it can steal sensitive information such as saved passwords, one-time passwords, and banking credentials, and even carry out unauthorised financial transactions—all without the user's knowledge.

Howdoesthisphotoscamwork ?

In the present scenarios , you received a funny image from a friend who in turn got it from someone unknown to him . So, you decide to forward this funny image to your family WhatsApp group. Now some members of your family or WhatsApp group may share this funny meme to their friends and this is how the

cycle goes on. In reality this image has embedded spyware or malware or a QR code which redirects you to a phishing website which once opened can download a keystroke logger or ransomware in your phone.

Howtoprotectyourselffromsuchscams, ***followthesesafetyguidelines***:

■ Never download photos or video, or link files from an unknown sender.Check for authentication of messages forwarded even from known contacts. Ignore and block calls and messages that seem suspicious.

■ Enabling two-factor authentication, keeping device software up to date, and using a reputable antivirus app.

■ Disable auto-download of media under WhatsApp settings.

■ Regularly update your phone's antivirus software.

■ Use caller ID apps like Truecaller to verify unknown numbers.

■ Report suspicious messages to WhatsApp and block the sender instantly.

■ Educate others about such scams to help them stay alert.

■ Report any incidents to the official Cybercrime portal: https://cybercrime.gov.in

N.B. TheupcomingCyberJagruktaDiwason 2nd. July 2025 ***willfocusonarisingcyberthreat - fakeIVRcalls***, a new cyber threat designed to steal your money.

2.7.2025 Today is the first Wednesday of the month- 2nd July'25 which means it's ***CyberJag*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

In its 16th episode of The***CyberJagrookta Diwas*** our topic is on***fakeIVRcalls***, a new cyber threat designed to steal your money.

In today's digital age, fraudsters have found new ways to deceive people—one of the most common being fake IVR (Inteĺractive Voice Response) calls. These calls can sound official and convincing, but they often aim to steal your personal or financial information. Here's how you can protect yourself and what to do if you fall victim. Before going to topic, let us know ***WhatAreFakeIVRCa***ll ?

Fake IVR calls use automated voice systems pretending to be from banks, government agencies, or well-known companies. You might hear a message like, "Your ATM card is blocked. Press 1 to fix this issue." These calls are designed to create urgency and trick you into sharing sensitive details like your bank account number, ATM PIN, or OTP.

HowtoIdentifyandAvoidFraudulentCalls

Unknown Numbers: Be cautious if the call comes from an unknown or suspicious number.

Pressure Tactics: Scammers often use fear or urgency. Real organizations won't threaten or rush you.

Requests for Sensitive Information: No legitimate bank or agency will ask for your card number, PIN, or OTP over a call.

Too Good to Be True: Offers like lottery wins or cash prizes are almost always scams.

HowtoProtectYourself

Do Not Share Personal Information: Never share your bank details, OTP, or passwords over the phone.

Use Call Blocking Apps: Install call-blocking apps that can help identify and block spam numbers.

Register for Do Not Disturb (DND): Reduce telemarketing calls by registering your number on the DND list.

Talk to a Trusted Person: If you're unsure about a call, consult a family member or friend before taking action.

WhattoDoIfYouBecomeaVictim

Call Your Bank Immediately: Report the incident and request to block your card or account to prevent further loss.

File a Complaint: Call the national cybercrime helpline at 1930 or visit www.cybercrime.gov.in.

Keep a Record: Note down the details of the call and any transactions for investigation.

Stay Informed: Attend community awareness programs or ask your bank about scam prevention tips.

Conclusions:

Scammers are getting smarter, but so can you. By staying aware and cautious, you can protect yourself and your loved ones from falling prey to fake IVR scams. Remember—when in doubt, hang up and verify with the official source.

Beware of Fake IVR Calls:Stay Alert, Stay Safe !

N.B. TheupcomingCyberJagruktaDiwason 6th August 2025 ***willfocuson*** a most common cyber frauds - ***Phishing***attack .

6.8.2025 Today is the first Wednesday of the month- 6th August'25 which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

In its 17th episode of The ***CyberJagrooktaDiwas*** our topic is on a most common cyber fraud - ***Phishing*** attack. In previous episode it was explored " Spoofing Attack " in which someone pretends to be a trusted entity (like a website, email, or phone number) to trick you into doing something or revealing sensitive information. Think of it like someone wearing a disguise to look like someone you trust. But incase phishing attack, it is a type of scam where attackers try to trick you into revealing sensitive information (like passwords, credit card numbers, or personal data) by sending fake emails, messages, or creating fake websites that look legitimate. The goal is to "fish" for your valuable information. So the key difference is Spoofing is more about pretending to be someone you're not, while phishing is specifically about trying to steal sensitive information by tricking you into revealing it. Think of it like this:
- Spoofing is the disguise, and phishing is the specific tactic used to steal your info while wearing that disguise !
ExampleofaPhishingAttack:
The phishing attacks have been seen to be triggered through SMSes containing links that end with ngrok.io/xxxbank. (Sample SMS.-"Dear customer your xxx bank account will be suspended! Please Re KYC Verification Update click here link http://446bdf227fc4.ngrok.io/xxxbank".) Once a victim clicks on this URL (universal resource locator) and log in to the phishing website using internet banking credentials, the attacker generates OTP for 2FA or two factor authentication which is delivered to the victim's phone number."The victim then enters this OTP in the phishing site & the attacker gains access to the victim's account using the OTP and performs fraudulent transactions..
The best practices to nip these attacks is to "Look for suspicious numbers that don't look like real mobile phone numbers as scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number." "Genuine SMSes received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field." So "only click on URLs that clearly indicate the website domain."

When in doubt, users can search for the organisation's website directly using search engines to ensure that the websites they visited are legitimate. A specific check against such attacks is "exercising caution towards shortened URLs, such as those involving bit.ly and tinyurl."

Howtoprotectyourselffromphishingattempts.

☆ Be mindful of URL structure– when clicking on any link–make sure it uses https:// protocols - the 's' means the URL is secure.

Never click on links from pop-ups. In order to avoid being 'pharmed', you should never click links from pop ups, always manually type the official domain of a website into your browser.

Never connect to a public Wi- Fi hotspot without VPN.

☆ Email Filtering - Most popular email service providers, such as gmail, yahoo, AOL and hotmail offer ways to set up filters to block emails coming from specific domains. Verizon offers ways to add spam blocks via its My Verizon portal.

FollowtheseinstructionsonhowtoAdd /RemoveSpamBlocksonMyVerizon.

Adding Spam Blocks:

1. Go to Verizon's official website https://www.verizon.com and sign in to your account.
2. Navigate to Settings . Click on "My Verizon" and select "Account" or "Settings."
3. Find Spam Block Option . Look for "Spam Block" or "Call Block" under the "Account Settings" or "Phone Settings" section.
4. Add Numbers . Enter the phone number(s) you want to block or select from your recent calls/contacts.
5. Save Changes .Click "Save" or "Apply" to add the numbers to your spam block list.

Removing Spam Blocks:

1. Follow Steps 1-3 . Visit Verizon's website, sign in, and navigate to the "Spam Block" or "Call Block" section.
2. Find the Number .Locate the phone number(s) you want to remove from the block list.
3. Remove Number . Select the number(s) and click "Remove" or "Delete."
4. Confirm Removal .Confirm that you want to remove the number(s) from the block list.
5. Save Changes .Click "Save" or " Apply " to add the numbers to your scam block list

If you come across of***Phishing*** attacks or any suspicious unusual activity in their account ,please report immediately to Computer Emergency Response Team for India through the official website https://cert-in.org.in and respective banks with the relevant details for taking further appropriate actions

Stay Alert, Stay Safe !

N.B. TheupcomingCyberJagruktaDiwason 3rd September 2025 ***willfocuson howtouseartificialintelligence&howtohelppreventfraud, andhowit'sbeingusedtoscam***.

3rd September '25 which means it's ***CyberJagrookta Di***was . It is celebrated on the first wednesdayof every month to create awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

In its 18th episode of The ***CyberJagrookta Diwas*** we will explore a new clever phishing campaign which is tricking users with a small but dangerous Japanese hiragana letter "ん" to create fake website addresses that look almost identical to real ones.

HowThisAttackWorks :

Cybercriminals are registering domain names using the hiragana character "ん" which visually resembles the Latin letter "n" in many fonts. To untrained eyes, these URLs appear completely legitimate. Most people won't notice the difference. Clicking such a link could take you to a fraudulent website where attackers steal passwords, banking details, or personal information.This attack is called homograph spoofing, where letters from different languages are mixed to fool the eye.

ForExamples:

Real : amazon.com

Fake: amazoん.com (notice the last “n” is actually the Japanese “ん”)

googleん.com (fake) vs google.com (real)

microsoftん.com (fake) vs microsoft.com (real)

Why This is Particularly Dangerous

Even security-conscious users who carefully check URLs can be fooled because:

The characters look nearly identical in most browsers

Standard security training focuses on obvious misspellings

Many antivirus programs don't flag these domains initially.

Tipstostaysafe:

● Don’t rely only on looks. Always check URLs carefully by hovering the mouse or long-pressing on mobile before clicking.

● Type it yourself. Manually enter web addresses like amazon.com instead of clicking unknown links.

● Turn on browser protections and keep devices updated.

● Use two-factor authentication wherever possible.

● Use reputable security software with updated threat detection

● When in doubt, navigate directly to the official website

● Remember, one small character can open the door to a big cyber risk.

Stayvigilantandspreadawarenessabouttheseevolvingcyberthreats !

N.B. TheupcomingCyberJagruktaDiwason 1st October 2025 ***willfocuson***

howtouseartificialintelligence&howtohelppreventfraud, andhowit'sbeingusedtoscam.

howtouseartificialintelligence&howtohelppreventfraud, andhowit'sbeingusedtoscam.

5.11.2025 --Today is the first Wednesday of the month- 5th Nov. '25 which means it's ***CyberJagr*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes.

In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

In its 19th episode of The***CyberJagrooktaDiwaswewillexplorehowAIisbeingusedtoscampeople&howtoprotectfromsuch scams usingAIskills***.

AI is a double-edged sword – when used wisely, it can greatly improve life, but we must stay alert to its misuse.Thecybersecurity landscape in India is evolving rapidly, and the elderly are often prime targets due to their limited familiarity with digital security measures. Protecting elders is not just a necessity but a responsibility that can save them from financial and emotional distress. Unlike traditional scams, some of the latest AI scams include deepfakescams,voice cloning and phishing attacks etc.

Let'sexplorethekeyareasoffraudwhereAIprovidesthegreatestadvantagetocybercriminals.

1. ***Deepfakevideoscams*** -

Deepfake videos are AI-generated videos that might include completely fake people or simulated real people.

2. ***ScammersalsomightcreateAI-generatedimages*** to enhance their scams. They could use the images as part of an advertisement or post on social media and link to scam websites in the comments.

3. ***Voicecloning*** -Deepfake videos are not the only way to convincingly impersonate someone. Voice cloning schemes, where fraudsters use AI to artificially create “deepfake” voice messages, are gaining in popularity.

4. ***Syntheticidentityfraud*** -

Synthetic fraud is another AI-driven cyber threat, where fraudsters create fake AI-generated information.

5. ***Advancedfinancialmalware***

Using AI to create advanced financial malware is one of the most widely discussed threats in cybersecurity.

6. ***Moredangerousphishing***

which was discussed in last episode is now widely used in cyber scams .

HowtoProtectfromAIScams :

1. ***Howtoknowascammeris*** : Watch out for these red flags when you receive a call.

Example - Being asked to pay money in order to receive a prize or get a job. Pressure to act immediately and use of scare tactics, (Telling you a loved one is in danger, that your computer has been hacked or threatening arrest if you don't act now.)

2. ***BeforeAnsweringp*** :

• International area code that looks local

• Number doesn't match the caller ID name (e.g., says a big company but has a local number)

• Claims to be from a government agency like the Indian Revenue Service (they won't call you out of the blue)

• Caller ID shows "Scam Likely" or "Spam Risk" (your carrier has flagged it as potential spam) .
With Truecaller, you can easily identify and block spam calls or SMS and search for unknown numbers.

• You should not answer calls from area codes 268 (Antigua and Barbuda), 284 (British Virgin Islands), 473 (Grenada), 649 (Turks and Caicos), and 876 (Jamaica) due to frequent scam and fraud attempts.

• Identify unknown callers and missed calls with online reverse phone lookup tool as mentioned below which is a quick, easy, and legal way of doing it. https://www.truecaller.com/reverse-phone-number-lookup

• Using many free sites as mentioned below for "Who Called Me?"
https:// numlooker.com or https://findpeoplefast.net or https://naam.ai (Indian site) Just type in a phone number and you might get some details back about who owns.

• You can also use Chatgpt to know who call me https://chatgpt.com/g/gH5eSKDXWY-who-called-me

• You can use India’s First Fraud Prevention Solution website which is Guarding You & Your Loved Ones Against All Possible Frauds https://www.quickheal.co.in/quick-heal-antifraud

• You can use a Self Help AI Tool website where different types of easy-to use tools to protect you from fraud and other online harms. This website is a well-known and highly respected non-profit organization based in the UK. It functions as a public/private sector partnership, supported by the UK Government and law enforcement, to provide free, expert, and impartial advice on how to stay safe online.

• Check if a website is likely to be legitimate or fraudulent by clicking below mentioned website https://www.getsafeonline.org/checkawebsite/

• Check a physical location of a business or person genuine? Find out where the street and premises of a company or person are and what they look like.https://maps.google.co.uk/

• Check whether your contact details been stolen by cybercriminals? Enter emails ID you want to check & stay protected .Get immediate notifications when your data appears in breaches https://haveibeenpwned.com

• Instantly verify if an email is real, active, and deliverable by clicking on https://mailmeteor.com/email-checker

• A free Scam Checker, simply send a screenshot you want to check WhatsApp and get an instant analysis. https://www.getsafeonline.org/asksilver

• Spot the what's been generated by AI, and what hasn't? Check now clicking this fun tool. https://sightengine.com/detect-ai-generated-images

Stayvigilantandspreadawarenessabouttheseevolvingcyberthreats !

N.B. TheupcomingCyberJagruktaDiwasscheduledfor 3***rdDecember*** 2025, ***willfocusonwhatyoushoulddoifyoususpectyouhaveinadvertentlyfallenforacybercrimeattack.***

3.12.25 – Today is the first Wednesday of the month- 3rd December 2025 which means it's ***CyberJagro*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

In its 20th episode of The***CyberJagrooktaDiwaswewillexplore***

onwhatyoushoulddoifyoususpectyouhaveinadvertentlyfallenforacybercrimeattack.

ImmediateActions

1. ***StopAllCommunicationwiththeAttacker***:

• Cease all interactions immediately

• Do not make any further payments or share additional information

• Block the suspicious phone numbers, emails, or social media accounts

2. ***SecureYourBankingandFinancialAccounts***:

• Call your bank's customer care immediately (use the number on your bank card or official website)

• Request to freeze or block compromised accounts, cards, or wallets

• Enable transaction alerts if not already active

• Change your internet banking passwords, UPI PINs, and ATM PINs

3. ***EmailandSocialMedia***:

• Change passwords for all email and social media accounts

• Enable two-factor authentication (2FA) wherever possible

• Review recent login activity and log out of all devices

4. ***MobileandComputer***:

• Disconnect from the internet if you suspect malware installation

• Run a full antivirus scan

• Consider doing a factory reset if malware is confirmed

5. ***DocumentEverything***

• Take screenshots of all communications, messages, emails, and transaction details

• Note down dates, times, and amounts of suspicious transactions

• Save caller IDs, email addresses, website URLs, and any other relevant information

• Keep records of all account statements showing fraudulent transactions

6. ***NationalCybercrimeReport*** :

• Visit: www.cybercrime.gov.in

or call 1930

• This is the official government portal for reporting cybercrimes

• You can report anonymously or with your details

• Available 24x7 in multiple languages

• File a complaint with all documented evidence

7. ***LocalPoliceStation***

• File an FIR (First Information Report) at your nearest police station

• Cyber crimes fall under the Information Technology Act, 2000

• Request a copy of the FIR for your records

• If local police are unresponsive, approach the Cyber Cell of your state police

8. ***FinancialFraud*** :

• For banking fraud: Contact your bank's fraud reporting cell

Website: cms.rbi.org.in

• For UPI fraud: Report through NPCI (National Payments Corporation of India)

• For credit card fraud: Contact your credit card company immediately

• Unified Helpline: Call 155260 for reporting financial cyber fraud

9. ***OtherReportingChannels***:

• Reserve Bank of India: File a complaint on RBI's SACHET portal for banking grievances

Website: sachet.rbi.org.in

• TRAI (for telecom fraud): Report via the TRAI SMS service by forwarding the message to 1909 or

Website: sancharsaathi.gov.in

• SEBI (for investment fraud): complaints.sebi.gov.in

• Consumer Forum: If applicable, file a consumer complaint

Follow-UpActions

1. ***MonitorYourAccounts***

• Check all bank statements and transaction histories regularly

• Set up alerts for all transactions

• Review credit reports through CIBIL or other credit bureaus

• Watch for any unauthorized accounts opened in your name

2. ***InformYourContacts***

• If your email or social media was compromised, warn your contacts

• Alert them not to open any suspicious messages from your accounts

• This prevents the attack from spreading to others

3. ***LegalandDocumentation***

• Keep copies of all complaints filed (cybercrime portal, FIR, bank complaints)

• Follow up regularly on your complaint status

• Note down complaint/FIR numbers for future reference

• Consider consulting a lawyer if significant financial loss has occurred

4. ***CreditandIdentityProtection***

• Place a fraud alert on your credit reports

• Consider freezing your credit to prevent new accounts being opened

• Monitor for identity theft indicators

CommonTypesofCyberAttackstoBeAwareOf

• Phishing: Fake emails, messages, or websites designed to steal credentials

• Vishing: Phone calls impersonating banks, government officials, or tech support

• UPI/QR Code Fraud: Fake payment requests or malicious QR codes

• Online Shopping Scams: Fake e-commerce websites or fraudulent sellers

• Investment Scams: Promises of high returns through cryptocurrency, stocks, or trading

• Job Scams: Fake job offers requesting advance payments

• Romance Scams: Fraudsters building relationships to extract money

• Lottery/Prize Scams: Fake notifications of winning prizes requiring fees

ImportantContactNumbers

• Cybercrime Helpline: 1930

• Financial Fraud Helpline: 155260

• National Consumer Helpline: 1915

• Emergency Services: 112

Remember

Time is critical in cyber fraud cases. The faster you report and act, the higher the chances of recovering your funds and preventing further damage. Do not feel embarrassed about falling for a scam—these attacks are sophisticated and can happen to anyone. Reporting helps protect others and aids law enforcement in tracking down criminals.

Stay vigilant, stay safe online.

WELCOME TO 2026

7.1.2026 – 21st Episode – Odia -- 

Today is the first Wednesday of the month- 7th January 2026 which means it's ***CyberJagr*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities***- is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

ସମ୍ପ୍ରତି ଭୋଟର ତାଲିକାର ସଂଶୋଧନ -- ଅଭିଯାନ ସମସ୍ତରେ ସ୍ତନ୍ତ୍ର ସଘନ ସଂଶୋଧନ (ସ୍ପଶୋଲ୍ ଇଣ୍ଟନ୍ସିଭି ରିଭିଜନ -SIR) ନାମରେ ଏକ ନୂତନ ସାଇବର ଠକେଇ ଦ୍ରୁତ ଗତିରେ ବୃଦ୍ଧି ପାଉଥିବାରୁ ମୋବାଇଲ୍ ଗ୍ରାହକମାନଙ୍କୁ ସଶକ୍ତ କରିବା ଏବଂ ସମୋନଙ୍କର ସୁରକ୍ଷାକୁ ସୁଦୃଢ଼ କରିବା ଅତ୍ୟନ୍ତ ଜରୁରୀ ହୋଇପଡ଼ିଛି। ଆଜିର ଏହି ୨୧ତମ ସାଇବର ଜାଗୃତି ଦିବସ ରେ ଏପରି ଠକେଇ ବିଷୟରେ ସଚତେନ କରିବା ସହିତ ଏହାକୁ ଏଡାଇବାର ଉପାୟ ବର୍ଣ୍ଣନା କରାଯିବ ।

ଭାରତର ନିର୍ବାଚନ କମିସନର - ECI ଅନୁଯାୟୀ, ଏହି ଅଭିଯାନର ମୁଖ୍ୟ ଉଦ୍ଦଶ୍ୟେ ହଉଛି ଏକ ଭୋଟର ତାଲିକା ପ୍ରସ୍ତୁତ କରିବା ଯାହା ସମ୍ପୂର୍ଣ୍ଣ ସଠିକ୍, ପ୍ରତ୍ୟେକେ ଯୋଗ୍ୟ ଭୋଟରଙ୍କ ନାମ ସଠିକ୍ ଭାବରେ ଅନ୍ତର୍ଭୁକ୍ତ ଏବଂ ଏଥିରେ କୌଣସି ଡୁପ୍ଲିକଟେ, ନକଲି କିମ୍ବା ଅଯୋଗ୍ୟ ନାମ ରହିବନାହିଁ। ଏହାକୁ ଆଧାର୍ୟ କରି ଏହି ସମସ୍ତରେ, ସାଇବର ଠକମାନେ SIR ଆଳରେ ଲୋକଙ୍କୁ ନିଜର ଶିକାର କରୁଛନ୍ତି। ଏପର୍ଯ୍ୟନ୍ତ, ଏପରି ଅନେକ ମାମଲା ସାମ୍ନାକୁ ଆସିଛି ଯେଉଁଠାରେ ଭୋଟର ତାଲିକା ଅପଡଟେ୍ କରିବା ନାମରେ ଲୋକଙ୍କୁ ଠକିବାକୁ ଚଷ୍ଟେ। କରାଯାଇଥିଲା। ସାଇବର ଠକମାନେ SIR ନାମରେ ଲୋକଙ୍କୁ ନକଲି ଲିଙ୍କ୍ ଏବଂ APK ଫାଇଲ୍ ପଠାଉଛନ୍ତି। ସମୋନେ ନିର୍ବାଚନ ଅଧିକାରୀ ବୋଲି ପରିଚୟ ଦେଇ ଫୋନ୍ କରନ୍ତି ଏବଂ କୁହନ୍ତି, 'ଭୋଟର ତାଲିକାରୁ ଆପଣଙ୍କ ନାମ କଟାଯାଇପାରେ, ତୁରନ୍ତ ଏହି ଫର୍ମ ପୂରଣ କରନ୍ତୁ।' ଲୋକମାନେ ସହେି ଲିଙ୍କ୍ କିମ୍ବା ଫାଇଲ୍ ଖୋଲିବା ମାତ୍ରେ ଠକମାନେ ସମୋନଙ୍କ ମୋବାଇଲ୍ ଆକ୍ସସେ୍ ପାଇଯାଆନ୍ତି। ଏହା ପରେ, ସମୋନେ ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟ ଖାଲି କରିବା କିମ୍ବା ଫୋନରେ ଥିବା ଡାଟା ଚୋରି କରିବା ପାଇଁ OTP ମାଗନ୍ତି। ତଣ୍ଟେ SIR ଫର୍ମ ନାମରେ ହଉଥିବା ଠକେଇ ପ୍ରତି ସତର୍କ ରହିବାକୁ ନିମ୍ନ ତଥ୍ୟ ଗୁଡ଼ିକୁ ଅନୁସରଣ କରନ୍ତୁ !

ଏପରି ପରିସ୍ଥିତିରେ, ମସେଜେରେ ମିଳିଥିବା ଲିଙ୍କ୍ ନକଲି କି ନାହିଁ ତାହା ଜାଣିବା ବହୁତ ଗୁରୁତ୍ପୂର୍ଣ୍ଣ? ଯଦି ମସେଜେରେ ମିଳିଥିବା ଲିଙ୍କ୍ ଆପଣଙ୍କୁ SIR, ଭୋଟର ଯାଞ୍ଚ କିମ୍ବା ସରକାରୀ କାମ ନାମରେ କିଛି ଡାଉନଲୋଡ୍ କରିବାକୁ କିମ୍ବା ତୁରନ୍ତ କ୍ଲିକ୍ କରିବାକୁ କୁହେ, ତବେେ ଏହା ଏକ ଠକେଇ। ନକଲି ଲିଙ୍କ୍ଗୁଡ଼ିକୁ ସାବଧାନତାର ସହ ଚିହ୍ନଟ କରିବା ପାଇଁ କିଛି ସଙ୍କତେ ବୁଝନ୍ତୁ-

* ଏକ ଅଜଣା ନମ୍ବର/WhatsAppରୁ ଲିଙ୍କ୍ ପ୍ରାପ୍ତ ହୋଇଛି

* ଲିଙ୍କରେ ଭୁଲ ସ୍ପଲେିଂ ଡୋମନେ୍

* ମସେଜେରେ ଭୟ କିମ୍ବା ଜରୁରୀତା

* ଆପଣଙ୍କୁ ତୁରନ୍ତ ଲିଙ୍କ୍ କ୍ଲିକ୍ କରିବାକୁ ଚଷ୍ଟେ। କରନ୍ତୁ

ଏପରି କୌଣସି ଲିଙ୍କ୍ ଖୋଲନ୍ତୁ ନାହିଁ ଏବଂ ତୁରନ୍ତ ଡିଲିଟ୍ କରନ୍ତୁ ନାହିଁ। ଦୟାକରି ଧ୍ୟାନ ଦିଅନ୍ତୁ, SIR ପାଇଁ କୌଣସି ସରକାରୀ କଲ୍

ଆସନୋହିଁ। ଏହି ପ୍ରକ୍ରିୟାରେ, କବେଳ ଆପଣଙ୍କର ବୁଥ୍ ଲଭେଲ୍ ଅଫିସର (BLO) ଆପଣଙ୍କ ଘରକୁ ସୂଚନା ସଂଗ୍ରହ କରିବାକୁ କିମ୍ବା ଏକ ସରକାରୀ ନୋଟିସ୍ ଦବୋକୁ ଆସନ୍ତି। ତଣ୍ଟେ ଆପଣଙ୍କୁ କୌଣସି ଲିଙ୍କ୍ ଉପରେ କ୍ଲିକ୍ କରିବାକୁ, APK ଡାଉନଲୋଡ୍ କରିବାକୁ କିମ୍ବା OTP ସଯୋର କରିବାକୁ ପଡିବ ନାହିଁ।

ଆସନ୍ତୁ SIR ରେ ଆପଣଙ୍କର ଭୋଟର ଆଇଡି ଅପଡଟେ୍ କରିବାର ସଠିକ୍ ଉପାୟ ବିଷୟରେ ବୁଝିବା। ଏଥିପାଇଁ, ଆପଣଙ୍କୁ କୌଣସି ଲିଙ୍କ୍ ଉପରେ କ୍ଲିକ୍ କରିବାକୁ, APK ଡାଉନଲୋଡ୍ କରିବାକୁ କିମ୍ବା OTP ସଯୋର କରିବାକୁ ପଡିବ ନାହିଁ। BLO ଆପଣଙ୍କ କଲୋନୀ କିମ୍ବା ୱାର୍ଡକୁ ଆସି ଗଣନା ଫର୍ମ (EF) ପ୍ରଦାନ କରନ୍ତି। ଫର୍ମ ନବୋ ସମସ୍ତରେ, ଆପଣଙ୍କର ଭୋଟର ପରିଚୟ ପତ୍ର ଦଖୋନ୍ତୁ, ଆପଣଙ୍କର ମୋବାଇଲ୍ ନମ୍ବର ଦିଅନ୍ତୁ ଏବଂ ଫର୍ମ ଗ୍ରହଣ କରିବା ସମସ୍ତରେ ସ୍ୱାକ୍ଷର କରନ୍ତୁ। ପ୍ରଦତ୍ତ ଫର୍ମଟି 710 ଦିନ ମଧ୍ୟରେ ପୂରଣ ଏବଂ ଦାଖଲ କରିବାକୁ ପଡିବ। ପ୍ରଥମ ସ୍ତମ୍ଭରେ, ଆପଣଙ୍କର ନାମ, ଜନ୍ମ ତାରିଖ, ମୋବାଇଲ୍ ନମ୍ବର ଏବଂ ପିତାମାତା/ପତି/ପତ୍ନୀଙ୍କ ନାମ ପୂରଣ କରନ୍ତୁ। ଆଧାର ଇଚ୍ଛାଧୀନ। ଯଦି ଆପଣ କିମ୍ବା ଆପଣଙ୍କର ସମ୍ପର୍କୀୟ 2003 ଭୋଟର ତାଲିକାରେ ଥିଲେ, ତବେେ ଦ୍ୱିତୀୟ/ତୃତୀୟ ସ୍ତମ୍ଭରେ ସହେି ବିବରଣୀ ପୂରଣ କରନ୍ତୁ। ନଚତେ୍, ଏହାକୁ ଖାଲି ରଖନ୍ତୁ। ପୂରଣ ହୋଇଥିବା ଫର୍ମଟିକୁ BLOକୁ ଫରୋଇ ଦିଅନ୍ତୁ। BLO ଏହାକୁ ସ୍କାନ କରିବେ ଏବଂ ECI ଆପ୍ରେ ଅପଡଟେ୍ କରିବେ। ଫର୍ମ ଦାଖଲ କରିବା ପରେ, ପ୍ରଥମ ଡ୍ରାଫ୍ଟ ତାଲିକା ପ୍ରକାଶିତ ହବୋ ପରେ ଆପଣଙ୍କ ନାମ ଯାଞ୍ଚ କରନ୍ତୁ। ଯଦି ନାମ ସଠିକ୍ ଦଖୋଯାଉଛି, ତବେେ ଆପଣଙ୍କର ଭୋଟର ପରିଚୟ ପତ୍ର ଅପଡଟେ୍ କରାଯାଇଛି। ଯଦି ନାମ ହଜିଯାଇଛି କିମ୍ବା ଭୁଲ ଅଛି, ତବେେ ନିର୍ବାଚନ ପଞ୍ଜିକରଣ ଅଧିକାରୀ (ERO)ଙ୍କୁ ଯାଇ ସଂଶୋଧନ କିମ୍ବା ଅନ୍ତର୍ଭୁକ୍ତି ପାଇଁ ପୁନର୍ବାର ଆବଦେନ କରନ୍ତୁ। ଏଥର, ଡକ୍ୟୁମଣ୍ଟେ ଅନୁରୋଧ କରାଯାଇପାରେ।

• ଆପଣ ଅନଲାଇନରେ ମଧ୍ୟସ୍ଥ ଗଣନା ଫର୍ମ ପୂରଣ କରିପାରିବେ। ଏଥିପାଇଁ ସର୍ତ୍ତ ହେଉଛି ଭେ।ଟର ତାଲିକା ଏବଂ ଆଧାରରେ ଥିବା ନାମର ସ୍ପଲିଂ ମଳେ ଖାଇବା ଉଚିତ ଏବଂ ଆଧାରକୁ ମେ।ବାଇଲ୍ ନମ୍ବର ସହିତ ଲିଙ୍କ୍ କରାଯିବା ଉଚିତ। ଅନଲାଇନ୍ ଦାଖଲ ସଫଳ ହେବା ମାତ୍ରେ, ଏହା ଡ୍ରାଫ୍ଟ-ଡାଟାବେସେରେ ଯାଏ।

ଯଦି ଆପଣ ଗଣନା ଫର୍ମ (EF) ପାଇନାହାଁନ୍ତି କିମ୍ବା BLO ଆସିନାହାଁନ୍ତି, ତେବେ ଭେ।ଟର ହେଲ୍ପଲାଇନ୍ ଆପ୍ (VHA), 1950 ହେଲ୍ପଲାଇନ୍,କିମ୍ବା voters.eci.gov.in ରେ ଅଭିଯେ।ଗ ପଞ୍ଜୀକରଣ କରନ୍ତୁ। ଆପଣ ସ୍ଥାନୀୟ ERO ସହିତ ମଧ୍ୟସ୍ଥ ଯେ।ଗାଯେ।ଗ କରିପାରିବେ। ଯଦି ଆପଣ SIR ନାମରେ ଅନଲାଇନ୍ ଠକେଇର ଶିକାର ହୁଅନ୍ତି, ତେବେ ବିଳମ୍ବ ନକରି କିଛି ତୁରନ୍ତ ପଦକ୍ଷେପ ନିଅନ୍ତୁ।

* ତୁରନ୍ତ ବ୍ୟାଙ୍କ/ାଲଟେ୍ କାର୍ଡ ଏବଂ କାରବାରକୁ ଅବରେ।ଧ କରନ୍ତୁ।

* ଗ୍ରାହକ ସବୋକୁ କଲ୍ କରନ୍ତୁ ଏବଂ କାର୍ଡ, UPI, କିମ୍ବା ନଟେ୍ ବ୍ୟାଙ୍କିଂ ସବୋ ବନ୍ଦ କରନ୍ତୁ।

* ଯକେୌଣସି ଅଜଣା ଆପ୍ (ଯପେରିକି SIR.apk) ତୁରନ୍ତ ଅନଇନଷ୍ଟଲ୍ କରନ୍ତୁ।

* ଆବଶ୍ୟକ ହଲେେ ଫେ।ନ୍ ରିସ୍ମାର୍ଟ କରନ୍ତୁ ଏବଂ ଫ୍ୟାକ୍ଟ୍ରି ରିସଟେ୍ କରନ୍ତୁ।

* ଇମଲେ୍, UPI, ବ୍ୟାଙ୍କିଂ ଆପ୍ ଏବଂ ସେ।ସିଆଲ ମିଡିଆ ପାଇଁ ତୁରନ୍ତ ପାସାର୍ଡ ପରିବର୍ତ୍ତନ କରନ୍ତୁ।

• ତୁରନ୍ତ ସାଇବର-କ୍ରାଇମ ହେଲ୍ପଲାଇନ୍ 1930 କୁ କଲ୍ କରନ୍ତୁ।

• cybercrime.gov.in ରେ ଏକ ଅନଲାଇନ୍ ଅଭିଯେ।ଗ ଦାଖଲ କରନ୍ତୁ।

* ସ୍କ୍ରିନସଟ୍, କଲ୍ ରକେର୍ଡ, ମସେଜ୍, ଲିଙ୍କ୍ ଇତ୍ୟାଦି ପ୍ରମାଣ ଅପଲେ।ଡ୍ କରନ୍ତୁ।

* ଆପଣଙ୍କର ନିକଟସ୍ଥ ସାଇବର ପେ।ଲିସ ଷ୍ଟେସନକୁ ମଧ୍ୟସ୍ଥ ରିପେ।ର୍ଟ କରନ୍ତୁ।

କବେଳ SIR ନାମରେ ହେଉଥିବା ଠକେଇକୁ ଏଡାଇବା ପାଇଁ ଆପଣଙ୍କର ସତର୍କତା ହେଉଛି ଏହାକୁ ଏଡାଇବାର ସହଜ ଉପାୟ। ମନରେଖନ୍ତୁ, ନିର୍ବାଚନ କମିଶନ କିମ୍ବା BLO କବେବେି କୌଣସି ଲିଙ୍କ୍ ଉପରେ କ୍ଲିକ୍ କରିବାକୁ, APK ଫାଇଲ୍ ଡାଉନଲେ।ଡ୍ କରିବାକୁ, OTP ସଯୋର କରିବାକୁ କିମ୍ବା ବ୍ୟାଙ୍କ ବିବରଣୀ ପ୍ରଦାନ କରିବାକୁ କୁହନ୍ତି ନାହିଁ। ସର୍ବଦା ନିଶ୍ଚିତ କରନ୍ତୁ ଯେ BLO ଆପଣଙ୍କ ଅଞ୍ଚଳ ପାଇଁ ନିଯୁକ୍ତ କର୍ମଚାରୀ, ସମୋନଙ୍କର ଏକ ସରକାରୀ ପରିଚୟପତ୍ର ଅଛି, ଏବଂ ସମୋନେ ଆପଣଙ୍କ ଘର କିମ୍ବା ଅଞ୍ଚଳକୁ ଯାଇ ଗଣନା ଫର୍ମ ପ୍ରଦାନ କରୁଛନ୍ତି। ଯକେୌଣସି କଲ୍, ମସେଜ୍ କିମ୍ବା ହ୍ୱାଟ୍ସଆପ୍ ଲିଙ୍କ୍ ର ସତ୍ୟତା ନିଶ୍ଚିତ କରିବା ପରେ କବେଳ ଏହାକୁ ବିଶ୍ୱାସ କରନ୍ତୁ।

N.B. TheupcomingCyberJagruktaDiwasscheduledfor 4th February 2026
willexploreanincreasinglydangerous .e.SIM

Swapsfraudthatcancompromiseyourentiredigitallifewithinminutes. Inthisscam, fraudstersimpersonateyouandconvinceyourmobileserviceprovidertotransferyourphonenumbertoaSIMcardintheirpossession. Oncesuccessful, theyreceiveallyourincomingcalls, textmessages, andone-timepasswords (OTPs), givingthemaccesstoyourbankaccounts, email, socialmedia, andothersensitiveaccounts.

4.2.26- 22nd EpisodeToday is the first Wednesday of the month- 4th February 2026 which means it's *CyberJagrooktaDiwas* . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, *ElderRecreationActivities*- is conducting monthly awareness programs as part of its Digital Pathasala - *EmpoweringElders*.

In its 22nd Episode of the *CyberJagruktaDiwasllexploreanincreasinglydangerouscy .e.SIMSwapsfraudthatcancompromiseyourentiredigitallifewithinminutes .Theprocessofprotectiontosuchscamalsoexplainindetails* .

***WhatisSIMSwapFraud*?**

In this scam, fraudsters impersonate you and convince your mobile service provider to transfer your phone number to a SIM card in their possession. Once successful, they receive all your incoming calls, text messages, and one-time passwords (OTPs), giving them access to your bank accounts, email, social media, and other sensitive accounts.

***HowDoesThisScamWork*?**

*** Information Gathering: Fraudsters collect your personal details through phishing calls, fake websites, or data breaches**

*** Impersonation: They contact your mobile carrier pretending to be you, claiming a lost or damaged SIM card**

*** SIM Activation: Once approved, your number is transferred to their SIM card**

*** Account Takeover: They intercept OTPs and reset passwords to access your banking and other accounts**

*** Financial Theft: Money is quickly transferred from your accounts before you realize what happened.**

WarningSignsofSIMSwapAttack

*** Sudden loss of mobile network signal without explanation**

*** Inability to make calls or send messages**

*** Receiving notifications about SIM card changes you didn't request**

*** Unexpected password reset emails or messages**

*** Friends or family reporting strange messages from your number**

HowtoProtectYourself

***ImmediatePrecautions*:**

*** Set up a strong PIN or password with your mobile service provider for any SIM-related changes**

*** Enable two-factor authentication (2FA) using authenticator apps rather than SMS when possible**

*** Never share OTPs, Aadhaar numbers, or personal details over phone calls or messages**

*** Be cautious of calls claiming to be from telecom companies, banks, or government agencies**

*** Register for the "Do Not Disturb" (DND) service to reduce spam calls**

***AdditionalSafetyMeasures*:**

*** Regularly monitor your bank statements and account activity**

*** Link your Aadhaar and mobile number to prevent unauthorized SIM replacements**

*** Inform your mobile carrier immediately if you notice any suspicious activity**

*** Keep your personal information private on social media platforms**

*** Contact your bank immediately if your phone loses signal unexpectedly**

***IfYouBecomeaVictim*:**

*** Immediately contact your mobile service provider to block the fraudulent SIM**

*** Report to local police and file a cybercrime complaint at cybercrime.gov.in**

*** Contact your bank to freeze accounts and cards**

*** Change passwords for all important accounts using a secure device**

*** Inform family members and contacts about the breach**

***Remember*: Your mobile number is the gateway to your digital identity. Protecting it is protecting your life savings and personal security.**

Let us stay alert, stay informed, and stay safe in this digital age.

Spread awareness. Protect your loved ones.

N.B. TheupcomingCyberJagruktaDiwasscheduledfor* 4*thMarch* 2026 *willexploremobileAPK-basedfrauds wherecybercriminalstrickcustomersintoinstallingmaliciousmobileapplications usingtempered .apkfilesofgenuineApps andtostaysafefromsuchscam

4.3.26-23rd Episode

Today is the first Wednesday of the month- 4th March 2026 which means it's *CyberJagrooktaDiwas* . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, *ElderRecreationActivities*- is conducting monthly awareness programs as part of its Digital Pathasala - *EmpoweringElders*.

Inits* 23 *oftheCyberJagruktaDiwasllexploreanincreasinglhoneAPK-basedfrauds , howtheAPKScamworks , howtoStaySafefromsuchscam .

***WhatisMobileAPK-BasedFraud*?**

APK stands for Android Package Kit. It is the file format used to install apps on Android mobile phones. Normally, we install apps safely from the Google Play Store. But fraudsters send fake APK files through:

*** WhatsApp**

*** SMS links**

*** Email**

*** Telegram**

*** Fake websites**

When someone installs these files, the fraudsters secretly gain access to the mobile phone.This type of cybercrime is called APK-based fraud or APK scam.

HowDoestheAPKScamWork?

Let us understand step-by-step in very simple language:

1 *TrapMessage*You receive a message such as:

*** "Your bank account will be blocked. Update KYC immediately."**

*** "You have won a prize."**

*** "Electricity will be disconnected."**

*** "Download this app for pension verification."**

It may appear to be from:

*** SBI / other banks**

*** Electricity department**

*** Income Tax**

*** Government schemes**

The message contains a link to download an APK file.

2.*InstallationoftheFakeApp*

The link does NOT open the Play Store.Instead, it downloads a file ending in .apk

The phone may show:"Install from Unknown Source?"If the user clicks Allow and installs it, the danger begins.

3 *PermissionControl*

The fake app asks for permissions:

*** SMS access**

*** Contacts**

*** Screen recording**

*** Accessibility control**

*** Banking access**

Many elders unknowingly press Allow.

4 *FraudExecution*

Once permissions are granted, the fraudster can:

*** Read your OTP messages**

*** Record your screen**

*** Control your phone remotely**

*** Access your bank app**

*** Transfer money without your knowledge**

Even if you delete the app later, damage may already be done.

WhyEldersAreTargeted

Fraudsters target senior citizens because:

*** They trust official-looking messages**

*** They may not know about APK files**

*** They may panic if message mentions bank or pension**

*** They may not understand mobile permissions**

So awareness is protection.

HowtoStaySafefromAPKFraud

Refrain from downloading or clicking on files sent by unfamiliar contacts.

You may install an App - C-DAC M-Kavach2 from Google's play store which is a free and a comprehensive Android mobile security solution developed by the Centre for Development of Advanced Computing (C-DAC) under the Ministry of Electronics and Information Technology. It can be used to prevent APK scams by blocking malicious apps and fake links before they can harm your mobile phone

Never download unexpected files with malicious extensions like “.apk", ”.exe” etc.

Download apps only from Google Play store or Apple App store. Activate Security Features on Devices such as “Disable Auto Download” setting to prevent auto downloading of files from untrusted sources.

Report immediately to the bank and report on Govt. Cyber Fraud Helpline - 1930 or on portal www.cybercrime.gov.in in case of fraud.

AwarenessMessage

In today’s digital world, mobile phone is like a bank locker.

If we install unknown APK files, it is like giving locker keys to strangers.

Digital knowledge is digital protection.

Letusstayalert, staycalm, andstaysafe.

1.4.26 -24th EpisodeToday is the first Wednesday of the month- 1st April 2026 which means it's *CyberJagrooktaDiwas* . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, *ElderRecreationActivities*- is conducting monthly awareness programs as part of its Digital Pathasala - *EmpoweringElders*.

Inits 24thEpisodeoftheCyberJagruktaDiwaswewillexplainsomeonlinetoolstostop onlinescamsbeforetheycauseharm.

Today, online scams, cyber fraud, and financial scams affect thousands of families every day. As smartphones, digital payments, and online services become part of daily life, scam awareness has become a key part of healthy aging and vibrant living. As smartphones, digital payments, and online services become part of daily life, cyber fraud affects thousands of families every day.

So scam awareness has become a key part of healthy aging and digital hygiene,

The present goal is not to restrict digital freedom but to empower senior citizens with confidence and safety online.The below tips will help them to identify the signs which can indicate that a website or a phone call or a message could be a scam.

*** *Quickcheck* :With a single click on this website https://www.scamadviser.com you can check any suspected phon call or website for scams. You can also check IBAN (International Bank Account Number) for its genuineness that helps banks to process transfers around the world .**

*** *GoogleSafeBrowsing* is a service from Google that warns users when they attempt to visit a dangerous website or download dangerous files. You can search to see whether a website is currently dangerous by clicking this website https://transparencyreport.google.com/safe-browsing/search?hl=en_GB**

*** *VirusTotal* is an online tool acquired by Google that analyzes suspicious files and URLs to detect types of malware and malicious content using antivirus engines and website scanners . You can visit this website https://www.virustotal.com/gui/home/url and upload or enter the file or URL: To analyse a file, click on the 'choose file' button and select the file from your device. You can also drag and drop the file onto the VirusTotal website.**

*** *WebsiteReputatio* :In today's digital world, not all websites are what they appear to be. Cybercriminals often exploit cloned websites or subtle domain variations (known as typosquatting) to impersonate reputable organisations.That's why our Free Website**

Reputation Checker helps you detect potentially malicious websites and is an essential first step in practising good cybersecurity hygiene with using website https://www.urlvoid.com/?hl=en-IN

*** *DiscoverRatingsforan* :It's a free online tool that grades your site against key metrics like performance, mobile readiness .**

Website visitors often gain important in-for-ma-tion through reviews and customer website ratings, allowing them to gauge the opinions of other users before investing money in a product, service, or business .For this purpose you can use website like https://safeweb.norton.com/?hl=en-IN

*** *OnlineShoppingChecker* :With the rise of online shopping scams—especially those involving "limited-time offers" sent via WhatsApp or social media—this tool is quite useful. If you see an ad for a very cheap product on a site you've never heard of, you can paste the link into the checker to see if it has been flagged as suspicious. It can help detect "Cloned" sites that are trying to look like famous Indian retailers (like Flipkart or Amazon) but have a slightly different URL. Thus this website https://www.f-secure.com/en/online-shopping-checker is designed to help you verify the "trustworthiness" of an online store before you make a purchase.**

Digitalknowledgeisdigitalprotection.

Letusstayalert, staycalm, andstaysafe.

6.5.26- 25th Episosd -

Today is the first Wednesday of the month- 6th May 2026 which means it's ***CyberJagro*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders***.

Inits 25***thEpisodeoftheCyberJagruktaDiwaswewillexplainsomeTax-relatedScamsduringreturnseasoninIndiaandhowtoprotectyourselfandwhattodoifyou getasuspiciousmessage*** .

The 2026 tax filing season—for 2025 returns now begins. Scammers are ramping up efforts to steal taxpayers' information and money.

Followings are some tax-related scams to watch out for this year.

1️⃣ Fake phone call impersonating Income Tax Department .You receive a call from someone claiming to be an Income Tax Officer. They say your PAN is linked to suspicious transactions or that you owe additional tax. They demand immediate payment via UPI or bank transfer to avoid arrest or penalty.

Redflagstowatchfor

• Caller creates panic — threat of 'arrest' or 'account freeze'
• Asks you to pay via UPI, Google Pay, or Paytm immediately
• Claims your PAN card is 'blocked' or 'blacklisted'
• Refuses to give an official notice reference number
• Asks you to keep the call secret

2️⃣ Fake SMS / WhatsApp / email promising a large refund . You get an SMS or email saying you have a pending refund of ₹15,000–₹1,00,000. A link is shared asking you to 'verify' your bank account and enter your net banking credentials, OTP, or Aadhaar OTP to receive the refund.

Redflagstowatchfor

• Refund amount is unusually high or unexpected
• Link does not go to incometax.gov.in
• Asks for bank login details, OTP or card number
• Urgent deadline — 'claim within 24 hours'
• Sender email is a Gmail / Yahoo address, not gov.in

3️⃣ Phishing Emails mimicking official ITD communications. An email arrives with the ITD logo and official-looking letterhead, claiming a 'tax demand notice' or 'scrutiny notice'. You are asked to click a link and fill a form with your PAN, Aadhaar, and bank details to 'respond' to the notice.

Redflagstowatchfor

• Email sent from non-gov.in domain (e.g. itdindia@gmail.com)
• Grammar errors or unusual formatting in the email
• Link in email leads to a site different from incometax.gov.in
• Asks you to 'download' a form that may be malware
• Notice reference number cannot be verified on portal

4️⃣ Fake ITR Filing Apps & CA Impersonators

A fake app on Play Store or a 'CA' reached via social media offers to file your ITR at very low charges. They collect your Form 16, PAN, Aadhaar, bank details and login credentials — then either steal your refund, sell your data, or hold your return hostage for more money.

Redflagstowatchfor

• App is not the official Income Tax Department app
• Agent asks for your e-filing portal login credentials
• Charges an upfront 'fee' to release your own refund
• Cannot share a professional registration or GST number
• Contact only via WhatsApp, no verifiable office address

5️⃣ Fake websites that mirror incometax.gov.in

Search results or sponsored ads show sites like 'incometax-efiling.co.in' or 'incometaxportalindia.com'. These sites look identical to the real portal. When you log in, your credentials are harvested and later used to divert refunds to fraudsters' bank accounts.

Redflagstowatchfor

• URL is not exactly https://www.incometax.gov.in
• Site appears in an ad (not organic search result)
• No green padlock or unusual SSL certificate issuer
• Portal asks for extra info not normally required
• Password field does not show asterisks / hidden text

6️⃣ Fake communities offering tax advice to steal data .You are added to a WhatsApp or Telegram group titled 'ITR Help 2025-26' or 'Tax Refund Fast Track'. Admins pose as CA professionals and offer to 'quickly' process your refund. They collect your documents, charge fees, and disappear — or commit identity fraud using your Aadhaar and PAN.

Redflagstowatchfor

• Added to the group without your consent
• Group promises 'instant refund' or 'fast processing'
• Asks you to forward Aadhaar, PAN, Form 16 in the group
• Members post 'success screenshots' (fabricated)
• Admin uses a personal mobile number, not a firm number

How to protect yourself -Verify before you act

• Always log in directly to incometax.gov.in
• Check your refund status only via official portal

• Cross-verify ITD notices via AIS / 26AS
• Never trust links in SMS or WhatsApp
• Call 1800-103-0025 to confirm any ITD notice
Guard your credentials
• Never share OTP, PAN, Aadhaar or bank details over phone
• ITD never asks for payment via UPI or wallet
• Use strong, unique password on the e-filing portal
• Enable 2-factor authentication wherever possible
• Keep your registered email & mobile updated on portal
Be tech-savvy online
• Check URL — always https://www.incometax.gov.in
• Beware of lookalike domains (e.g. incometax-refund.in)
• Don't install apps from unknown links
• Avoid filing taxes from public Wi-Fi
• Clear session after every portal use
Spot pressure tactics
• Scammers create urgency — "pay now or face arrest"
• Real ITD officers don't call asking for immediate payment
• Any "unbelievably high" refund claim is a red flag
• Offers of tax savings for a fee upfront are scams
• Hang up and call back on official numbers
If you receive a suspicious message or call — do this
1. Do not panic or act immediately. Scammers rely on urgency. Take a breath and pause before doing anything.
2. Do not share any information — no OTP, PAN, Aadhaar, bank details, or passwords, regardless of how convincing the caller sounds.
3. Do not click any links. If you receive a suspicious email or SMS, do not tap any links or download attachments.
4. Verify independently. Log in directly to incometax.gov.in or call the ITD helpline 1800-103-0025 to check if any notice is genuine.
5. Report immediately on the Cyber Crime portal (cybercrime.gov.in) or call the National Cyber Helpline 1930. The sooner you report, the better the chance of stopping the fraud.
6. Inform your bank if you have already made a payment. Request a transaction freeze or reversal without delay.
7. Warn family and friends. Share the incident so others in your circle don't fall for the same scam.
Helplines & official portals
National Cyber Helpline1930Immediate cyber fraud response
ITD Help Desk1800-103-0025Verify income tax notices
Cyber Crime Portalcybercrime.gov.inReport online fraud
IT e-Filing Portalincometax.gov.inOnly official filing portal
Remember :
■ Income Tax Dept never demands UPI payment
■ No legitimate refund needs a fee to process
■ Never share OTP with anyone — ever
■ Lookalike URLs are traps
■ Always verify on incometax.gov.in directly
■ When in doubt — call 1930
■ Report scams to protect others too
***Letusstayalert*, *staycalm*, *andstaysafe*.**
3.6.2026 -- 26th Episode --Today is the first Wednesday of the month- 3rd June 26 which means it's ***CyberJagrooktaDiwas*** . It is celebrated on the first wednesday of every month to creat awareness and to sensitize users about safeguarding against cyber frauds and cyber crimes. In line with this, ***ElderRecreationActivities-era*** is conducting monthly awareness programs as part of its Digital Pathasala - ***EmpoweringElders***.

Inits
26thEpisodeoftheCyberJagruktaDiwaswewillfocusonUIDAI'snewredesignedAadhaarcard - "***mAadhaar***" ,***majorchanges***, ***whythischange***? , ***whatwillitbelike***?, ***howtodownloadonline*** , ***completedetails***…
The Unique Identification Authority of India is replacing the older Aadhaar with a redesigned Aadhaar platform that focuses heavily on selective data sharing and stronger authentication methods.
WhytoneedredesignnewmAadhaar
1️⃣ For Privacy Protection: Currently hotels, event organizers, and private offices take photocopies of existing Aadhaar cards and store names, addresses, DOBs, and Aadhaar numbers. This is a major risk for data leaks and it will be impossible with the new Aadhaar.
2️⃣ An upgrade new QR code-based system is designed to meet world-class security standards.
OldAadhaarvsNewmAadhaar — KeyDifferences
Only Photo & QR code will be visible on the new card ,where as
Name ,Aadhaar number , Address , Date of birth & Gender will no longer be visible.This means that no personal information will be printed on the new card.
WhatisintheQRcodeonnewAadhaar ? It contains Name,
Aadhaar number, DOB, Address,
Gender and Biometric verification data (in encrypted form).All of these will be encrypted.
Onlythefollowingcandecodethis QRcode:
● Government authorized scanners ● UIDAI official apps
● Verification devices. But holes,
event managers, offices, or anyone else will not be able to view the data by taking a photocopy.
N.B. As per an official memorandum issued by UIDAI, the free document update service will now be available until June 14, 2027. The facility was previously scheduled to remain free only until June 15, 2026.
HowtodownloadmAadhaaronline
For downloading the card , use the official mAadhaar / Aadhaar App on your mobile phone.
• 1. Open & install " mAadhaar" or "Aadhaar" by UIDAI from Google Play Store/ Apple App Store .Please note the developer name should be UIDAI. Avoid fake apps or APK downloads from unknown websites.
• 2.After installation , select your preferred language .The app supports English, Hindi, Odia and several Indian languages.
• 3. Accept Terms &Conditions .
• 4. Create Security PIN - You will be asked to create a 4-digit PIN/password .This PIN protects your Aadhaar details. So choose an easy but secure PIN.
• Add YourAadhaar Profile - Tap -“Add Aadhaar” or “Register Aadhaar”
• Then enter your 12-digit Aadhaar Number - Enter Captcha code - Tap “Send OTP”
• Verify OTP (UIDAI will send an OTP to your Aadhaar-linked mobile number.) -Enter OTP -Tap Verify (YourAadhaar profile will now appear on the app.)
HowtoDownloade-AadhaarPDF
After profile setup , Open the app - Go to “My Aadhaar” - Tap “Download Aadhaar”- Enter your PIN - Aadhaar PDF will download to your phone.
The downloaded e-Aadhaar is legally valid.
PasswordtoOpenAadhaarPDF
The PDF password is first 4 letters of your name in CAPITAL letters plus your birth year.
Example
Name: Ramesh Kumar ,Birth Year: 1965 , Password:RAME1965
UsefulFeaturesofmAadhaar
You can:
• Carry Aadhaar digitally
• Show QR code for verification
• Download e-Aadhaar

• Lock/Unlock biometrics
• Generate VID (Virtual ID)
• Add family members' profiles
• Use Aadhaar without carrying photocopy
Foranyqueries*, *pleaserefer
UIDAI Official Website (https://uidai.gov.in)
OR myAadhaar Portal (https://myaadhaar.uidai.gov.in.)
N.B. TheupcomingCyberJagruktaDiwasscheduledfor 1st July 2026 ***willfocusonthelatestscamsnowfoundmostcommonlyinIndia. ItwillbecirculatedwithOdiaLanguage.***(ବର୍ତ୍ତମାନ ଭାରତରେ ସାଧାରଣତଃ ଦେଖାଯାଉଥିବା ନୂତନତମ ସ୍କାମ୍)
1.7.2026 – 27th Episode --ଆଜି ମାସର ପ୍ରଥମ ବୁଧବାର - ୧ ଜୁଲାଇ '୨୬, ଅର୍ଥାତ୍ ଆଜି ସାଇବର ଜାଗୃତି ଦିବସ 1 ସାଇବର ଠକେଇ ବିରୁଦ୍ଧରେ ସୁରକ୍ଷା ସମ୍ବନ୍ଧୀୟ ସଚେତନତା ସୃଷ୍ଟି କରିବା ପାଇଁ ପ୍ରତି ମାସର ପ୍ରଥମ ବୁଧବାରରେ ଏହା ସାରା ଭାରତରେ ପାଳନ କରାଯାଏ। ତତ୍ ଅନୁଯାୟୀ, ***ElderRecreationActivies-era***ଏହାର ଡିଜିଟାଲ୍ ପାଠଶାଳା (Digital Pathasala) କାର୍ଯ୍ୟକ୍ରମର ଏକ ଅଂଶ ଭାବରେ ପ୍ରତି ମାସର ପ୍ରଥମ ବୁଧବାରେ ଉକ୍ତ .ସଚେତନତା କାର୍ଯ୍ୟକ୍ରମ କରିଆସୁଛି

ଆଜିର ୨୬ ତମ ଧାରାବାହିକ ସଚେତନତା କାର୍ଯ୍ୟକ୍ରମରେ ବର୍ତ୍ତମାନ ଭାରତରେ ଦେଖାଯାଉଥିବା ନୂତନତମ ସାଇବର ଅପରାଧ ଓ ଏହାକୁ ଏଆଇ (AI) ବା କୃତ୍ରିମ ବୁଦ୍ଧିମତ୍ତାର ବ୍ୟବହାର କରି କିପରି ସୁରକ୍ଷା ଦିଆଯାଇପାରିବ ତାହା ଆଲେ।ଚନା ହବେ 1
ଭାରତ ଏବେ ସାଇବର ଅପରାଧ ଏବଂ ପ୍ରତାରଣାମୂଳକ ଫେ।ନକଲ୍/ମେସେଜ୍ ମାମଲାରେ ବିଶ୍ୱରେ ପଞ୍ଚମ ସ୍ଥାନରେ ରହିଛି। ବିଭିନ୍ନ ରିପେ।ର୍ଟ ଅନୁସାରେ, ସମୁଦାୟ ସ୍କାମ୍ ମଧ୍ୟରୁ ବ୍ୟବସାୟିକ ବିଜ୍ଞାପନ ଓ ଟଲିମାର୍କଟିଂ ୩୬%, ଆର୍ଥିକ ସେବା ୧୮% ଏବଂ ଅତି ବିପଜ୍ଜନକ ଠକେଇ ବା ସ୍କାମ୍ ୧୨% ରହିଛି। ସାଧାରଣ ଲେ।କଙ୍କୁ ଟାର୍ଗଟ୍ କରୁଥିବା କିଛି ପ୍ରମୁଖ ସାଇବର ଅପରାଧ ଏବଂ ସଗୁଡ଼ିକରୁ ସୁରକ୍ଷିତ ରହିବାର ଉପାୟ ନିମ୍ନରେ ଦିଆଗଲା:

🔴 ପ୍ରମୁଖ ସାଇବର ଅପରାଧ
● ଭୟ ଦେଖାଇ ଏବଂ ଜରୁରୀ ପରିସ୍ଥିତି ସୃଷ୍ଟି କରି ଠକେଇ ("ଡିଜିଟାଲ୍ ଆରେଷ୍ଟ" ଧମକ): ସ୍କାମର୍ମାନେ CBI କିମ୍ବା ପେ।ଲିସ ଅଫିସର ସାଜି ଭିଡିଓ କଲ୍ କରନ୍ତି। ଆପଣଙ୍କ ଆଧାର କାର୍ଡ କିମ୍ବା ଫେ।ନ ନମ୍ବର କୌଣସି ବେଆଇନ ପାର୍ସଲ ବା ମନି ଲଣ୍ଡରିଂ ସହ ଜଡ଼ିତ ଅଛି ବେ।ଲି ମିଥ୍ୟା ଅଭିଯେ।ଗ ଆଣନ୍ତି। କସେ୍ ରଫାଦଫା କରିବା ପାଇଁ ଅନଲାଇନ୍ ଟଙ୍କା ମାଗନ୍ତି ଏବଂ ଟଙ୍କା ନଦେବା ଯାଏଁ ଭିଡିଓ କଲ୍ରେ ରହିବାକୁ ବାଧ୍ୟ କରନ୍ତି।
● AI ଡିପ୍ଫକେ୍ ଓ ଭଏସ୍ କ୍ଲେ।ନିଂ (AI Deepfake& Voice Cloning): AI ସାହାଯ୍ୟରେ ଆପଣଙ୍କ ସମ୍ପର୍କୀୟଙ୍କ ନକଲି ସ୍ୱର କିମ୍ବା ଭିଡିଓ ତିଆରି କରି ଜରୁରୀକାଳୀନ ପରିସ୍ଥିତି ଦର୍ଶାଇ ଟଙ୍କା ମାଗିଥାନ୍ତି।
● ନକଲି ପାର୍ଟ-ଟାଇମ୍ ଚାକିରି ଏବଂ ବିନିଯେ।ଗ ଠକେଇ (Investment & Part-time Job Scams): ୟୁଟ୍ୟୁବ୍ ଭିଡିଓ ଲାଇକ୍ କରିବା କିମ୍ବା ଘରେ ବସି କ୍ରିପ୍ଟେ।/ଷ୍ଟକ୍ ମାର୍କେଟରେ ଅଳ୍ପ ଟଙ୍କା ଲଗାଇ ବଡ଼ ଲାଭ ପାଇବାର ପ୍ରଲେ।ଭନ ଦେଖାଇ ଲକ୍ଷ ଲକ୍ଷ ଟଙ୍କା ଲୁଟି ନିଅନ୍ତି।
● ବିଦ୍ୟୁତ୍ ଏବଂ ମେ।ବାଇଲ୍ ସଂଯେ।ଗ ବିଚ୍ଛିନ୍ନ ଭୟ: ଗ୍ରାହକଙ୍କ ପାଖକୁ ମେସେଜ୍ ଆସେ ଯେ, ବାକି ବିଲ୍ କିମ୍ବା ଅପଡେଟ୍ ନଥିବା ଯେ।ଗୁଁ ଆଜି ରାତିରେ ବିଦ୍ୟୁତ୍ କିମ୍ବା ସିମ୍ କାର୍ଡ କାଟି ଦିଆଯିବ। ସେଥିରେ ଏକ ନକଲି କଷ୍ଟମର କେୟାର ନମ୍ବର ଥାଏ, ଯାହା ମାଧ୍ୟମରେ ସେମାନେ ବ୍ୟାଙ୍କ ସୂଚନା ଚେ।ରି କରନ୍ତି।
● ୟୁଏସ୍ଏସ୍ଡି କଲ୍ ଫରାର୍ଡିଂ ସ୍କାମ୍ (USSD Call Forwarding): କେ।ରିଅର ବା ଡଲିଭରି ବଏ ସାଜି ଏକ ନିର୍ଦ୍ଦିଷ୍ଟ କେ।ଡ୍ (ଯେପରିକି *21*) ଡାଏଲ୍ କରିବାକୁ କୁହନ୍ତି, ଯାହାଦ୍ୱାରା ଆପଣଙ୍କ ଓଟିପି (OTP) ଓ କଲ୍ ଅପରାଧୀଙ୍କ ପାଖକୁ ଚାଲିଯାଏ।
● ନକଲି ଲେ।ନ୍ ଆପ୍ (Instant Loan App Scam): ସହଜରେ ଲେ।ନ୍ ଦେବା ବାହାନାରେ ଆପ୍ ମାଧ୍ୟମରେ ମେ।ବାଇଲ୍ ଡାଟା ଚେ।ରି କରନ୍ତି ଏବଂ ପରେ ବ୍ଲାକମେଲ୍ କରନ୍ତି।
● QR କେ।ଡ୍ ମାଧ୍ୟମରେ ଠକେଇ: OLX ଭଳି ପ୍ଲାଟଫର୍ମରେ ସାମଗ୍ରୀ ବିକ୍ରି କରୁଥିବା ଲେ।କଙ୍କୁ ଏହା ମାଧ୍ୟମରେ ଟାର୍ଗଟ୍ କରାଯାଏ। କ୍ରତା ସାଜିଥିବା ଠକ ଜଣକ ଟଙ୍କା ପଠାଇବା ବଦଳରେ ଏକ "Receive Money" QR କେ।ଡ୍ ପଠାଏ, ଯାହାକୁ ସ୍କାନ୍ କଲେ ଆପଣଙ୍କ ଆକାଉଣ୍ଟରୁ ଟଙ୍କା କଟିଯାଏ।

🟢 ସାଇବର ଅପରାଧରୁ ସୁରକ୍ଷା ପାଇବାର ଉପାୟ (Prevention Measures)ସାଇବର ଆକ୍ରମଣରୁ ବଞ୍ଚିବା ପାଇଁ ଏହି ସାଧାରଣ ନିୟମଗୁଡ଼ିକ ପ୍ରତି ଧ୍ୟାନ ଦିଅନ୍ତୁ:
● ସାଇବର ଅପରାଧ ସୁରକ୍ଷାର ମୂଳମନ୍ତ୍ର - କୌଣସି ଅଜଣା ଲିଙ୍କ୍ ଉପରେ କ୍ଲିକ୍ କରନ୍ତୁନାହିଁ 1 ଆପଣଙ୍କ ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟ OTP କାହା ସହିତ ସେୟାର କରନ୍ତୁନାହିଁ 1 କୌଣସି ସରକାରୀ ସଂସ୍ଥା ଭିଡିଓ କଲ୍ ରେ ଆରେଷ୍ଟ କରନେ।ହିଁ 1
• ଭୟଭୀତ ହୁଅନ୍ତୁ ନାହିଁ: ଯଦି କହେି ପେ।ଲିସ ବା କେ।ର୍ଟ ନାଁରେ ଡରାନ୍ତି, ତେବେ ଜାଣିରଖନ୍ତୁ ଯେ ଭାରତୀୟ ଆଇନରେ ଡିଜିଟାଲ୍ ଆରେଷ୍ଟର କୌଣସି ପ୍ରାବଧାନ ନାହିଁ। ତୁରନ୍ତ କଲ୍ କାଟି ଦିଅନ୍ତୁ।

• ସମ୍ପର୍କୀୟଙ୍କୁ ଯାଞ୍ଚ କରନ୍ତୁ: ଯଦି କୌଣସି ବନ୍ଧୁ କିମ୍ବା ପରିବାର ଲୋକଙ୍କ ସ୍ୱରରେ ହଠାତ ଟଙ୍କା ମଗାଯାଏ, ତବେ ଅନ୍ୟ ନମ୍ବରରେ କଲ୍ କରି ସହେି ବ୍ୟକ୍ତିଙ୍କ ସହ ସିଧାସଳଖ କଥା ହୁଅନ୍ତୁ।
• ଦୁଇ-ସ୍ତରୀୟ ସୁରକ୍ଷା (2-Factor Authentication): ଆପଣଙ୍କର ସମସ୍ତ ସୋସିଆଲ ମିଡିଆ (WhatsApp, Facebook) ଏବଂ ବ୍ୟାଙ୍କିଙ୍ଗ୍ ଆପ୍ରରେ Two-Step Verification ସକ୍ରିୟ ରଖନ୍ତୁ।
• ସନ୍ଦହେଜନକ କୋଡ୍ ଡାଏଲ୍ କରନ୍ତୁ ନାହିଁ: କୌଣସି ଅଜଣା ବ୍ୟକ୍ତିଙ୍କ କହିବା ଅନୁସାରେ ନିଜ ମୋବାଇଲ୍ରୁ କୌଣସି USSD କୋଡ୍ ଡାଏଲ୍ କରନ୍ତୁ ନାହିଁ।
• ଅଫିସିଆଲ୍ ଆପ୍ ବ୍ୟବହାର କରନ୍ତୁ: ସର୍ବଦା Google Play Store କିମ୍ବା Apple App Store ରୁ ହିଁ ଯାଞ୍ଚ କରି ଆପ୍ ଡାଉନଲୋଡ୍ କରନ୍ତୁ।

🔵 ଠକେଇର ଶିକାର ହଲେେ କଣ କରିବେ? (Action Plan)ଯଦି ଆପଣ କୌଣସି ଆର୍ଥିକ ସାଇବର ଠକେଇର ଶିକାର ହୋଇଛନ୍ତି, ତବେେ ବିନା ବିଳମ୍ବରେ ଏହି ପଦକ୍ଷପେ ନିଅନ୍ତୁ:
● ୧୯୩୦ ହଲେ୍ପଲାଇନ୍: ତୁରନ୍ତ ସରକାରଙ୍କ ଜାତୀୟ ସାଇବର ଅପରାଧ ହଲେ୍ପଲାଇନ୍ ନମ୍ବର 1930 କୁ କଲ୍ କରି ଅଭିଯୋଗ କରନ୍ତୁ। ଏହାଦ୍ୱାରା ଆପଣଙ୍କ ଟଙ୍କା ଅପରାଧୀଙ୍କ ଆକାଉଣ୍ଟରେ ଫ୍ରିଜ୍ ହବୋର ସମ୍ଭାବନା ଥାଏ।
● ଅନଲାଇନ୍ ପୋର୍ଟାଲ୍: ଗୃହ ମନ୍ତ୍ରଣାଳୟର ସରକାରୀ ବେସାଇଟ୍ National Cyber Crime Reporting Portal କୁ ଯାଇ ନିଜର ଅଭିଯୋଗ ପଞ୍ଜିକରଣ କରନ୍ତୁ l
● ସଞ୍ଚାର ସାଥୀ ପୋର୍ଟାଲ (Sanchar Saathi): କନେ୍ଦ୍ର ସରକାରଙ୍କ ଏହି Sanchar Saathi(https://sancharsaathi.gov.in/ ବେସାଇଟ୍ ମାଧ୍ୟମରେ ଆପଣଙ୍କ ନାଁରେ କତେଟୋ ସିମ୍ ଚାଲିଛି ତାହା ଯାଞ୍ଚ କରିପାରିବେ ଏବଂ ହଜିଯାଇଥିବା ଫୋନ୍ ବ୍ଲକ୍ କରିପାରିବେ।
● ଚକ୍ଷୁ (Chakshu) ସବୋ: ସଞ୍ଚାର ସାଥୀ ପୋର୍ଟାଲରେ ଥିବା ଚକ୍ଷୁ ଟ୍ୟାବ୍ ମାଧ୍ୟମରେ ଆପଣ ପାଇଥିବା କୌଣସି ବି ପ୍ରତାରଣାମୂଳକ ମସେେଜ୍, କଲ୍ କିମ୍ବା ହ୍ୱାଟ୍ସଆପ୍ ସ୍କାମ୍ ବିଷୟରେ ସରକାରଙ୍କୁ ଜଣାଇପାରିବେ।
● ବ୍ୟାଙ୍କ୍କୁ ସୂଚନା: ତୁରନ୍ତ ଆପଣଙ୍କ ବ୍ୟାଙ୍କ୍କୁ ଯୋଗାଯୋଗ କରି ଏଟିଏମ୍ କାର୍ଡ ଓ ଆକାଉଣ୍ଟ ବ୍ଲକ୍ କରନ୍ତୁ।
ବି .ଦ୍ର . ଆସନ୍ତା ଅଗଷ୍ଟ ୫ ତାରିଖ ପ୍ରଥମ ବୁଧବାରେ ହବୋକୁ ଥିବା ବିଷୟ- " ସାଇବର ଠକେଇରୁ ରକ୍ଷା କରିବା ପାଇଁ ନିଜର ସ୍ମାର୍ଟଫୋନ୍ କୁ କିପରି ସଟେିଂ କରି ସୁରକ୍ଷିତ ରଖିହବେ " (In english)

5.8.26 –28th Episode -- Today, Wednesday, 5th August 2026, is the first Wednesday of the month – observed across India as ***JagrooktaDi*** (Cyber Awareness Day).
The first Wednesday of every month is dedicated to creating awareness about cyber safety and sensitizing citizens to protect themselves against cyber frauds and online crimes.
As part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders*** initiative, ***ElderRecreationActivities-era*** has been conducting a monthly Cyber JagruktaDiwas Awareness Programme to promote safe and confident use of digital technology among senior citizens.
🎯 Topic of the 28th Episode
HowtoSetUpYourSmartphonetoBlockMaliciousCallsandSpamMessages
In today's digital world, cybercriminals are increasingly using AI-powered voice scams to deceive innocent people.
Recently, social media reports claimed that people lost money from their bank accounts merely by answering a phone call. This is a myth. Simply answering a phone call cannot withdraw money from your bank account.
Financial fraud occurs only when victims are persuaded to:
❌ Share OTPs over the phone or enter them on the dial pad.
❌ Reveal UPI PIN, ATM PIN or banking passwords.
❌ Install remote-access applications such as AnyDesk or TeamViewer.
❌ Remain on fake "Digital Arrest" video calls until they transfer money out of fear.
❌ Click malicious links or install unauthorized APK files.
✅The Good News
Modern smartphones already include powerful built-in security features that can automatically identify and block spam calls and phishing messages.No paid application is required.
Below are the recommended settings.

🤖 Android Smartphones
(Google Pixel, Samsung Galaxy, OnePlus, Xiaomi, Realme and most Android phones)

☎ Enable Spam Call Protection

• Open the Phone app.
• Tap ⋮ (three dots) → Settings.
• Select Caller ID & Spam.
• Turn ON:
• See Caller & Spam ID
• Filter Spam Calls

This automatically blocks or silently filters suspected scam calls.

📱 Samsung Galaxy Phones

• Open Phone → Settings.
• Tap Caller ID and Spam Protection → Turn ON.
• Select Block Spam and Scam Calls.
• Choose Block All Spam and Scam Calls.

💬 Filter Spam SMS

• Open Google Messages.
• Tap your Profile icon.
• Select Messages Settings.
• Open Spam Protection.
• Turn ON Enable Spam Protection.

Suspicious lottery, courier, electricity bill and phishing messages will automatically move to the Spam folder.

🍎 iPhone (iOS)
Apple provides excellent built-in protection against unknown callers and spam texts.

☎ Silence Unknown Callers

• Open Settings.
• Go to Apps → Phone.
• Tap Silence Unknown Callers.
• Turn it ON.

Important: Save the phone numbers of family members, doctors, neighbours and close friends in your Contacts before enabling this feature.

💬 Filter Unknown Messages

• Open Settings.
• Go to Apps → Messages.
• Under Message Filtering, enable Filter Unknown Senders.

Your Messages app will automatically separate trusted contacts from unknown senders.

India-Specific Safety Measures
Activate Full DND (Do Not Disturb)
Use your telecom provider's official app:

• MyJio
• Airtel Thanks
• Vi App

Go to:Settings / Account → More Services → Do Not Disturb (DND)
Select:Full DND or Block All Promotional Calls.
This significantly reduces unwanted marketing and scam calls.

Secure Your WhatsApp
Many scammers target senior citizens through WhatsApp voice and video calls.
Open: WhatsApp → Settings → Privacy

• Turn ON Silence Unknown Callers.
• Open Groups.
• Change permission from Everyone to My Contacts.

This prevents strangers from adding you to fake investment, lottery or cryptocurrency groups.

Recommended App for Beginners

If configuring all these settings seems difficult, install Truecaller from the Google Play Store or Apple App Store. After installation:
• Grant required permissions.
• Open Manage Spam.
• Enable Automatically Reject Top Spammers.

⊘ NEVER SHARE

❌ OTP
❌ UPI PIN
❌ ATM PIN
❌ Debit/Credit Card Number
❌ CVV
❌ Internet Banking Password
❌Aadhaar OTP
❌ Screen-sharing permission
❌ Remote access to your mobile phone
❌Never install AnyDesk, TeamViewer, or any unknown APK file at the request of a caller.

Remember: No bank, RBI, police department, government office or genuine company will ever ask for these details over a phone call.

BlockaFraudulentNumber

Android

Phone → Recents → Long Press Number → Block / Report Spam

iPhone

Phone → Recents → Tap ⓘ → Block This Caller

AdditionalSafetyTips

✓ Keep Google Play Protect enabled.
✓ Use a strong screen lock (PIN, Fingerprint or Face ID).
✓ Enable Two-Factor Authentication wherever available.
✓ Review installed apps every month and remove unknown or unused apps.
✓ Check bank account and UPI transaction history regularly.
✓ Enable SMS or App notifications for every banking transaction.

WarningSignsThatYourPhoneMayBeCompromised

Be alert if you notice several of these signs together:
• Battery drains unusually fast.
• Phone becomes hot even when not in use.
• Sudden increase in mobile data usage.
• Unknown apps appear.
• Unexpected permission requests.
• Phone becomes unusually slow or crashes frequently.
• Strange clicking, echoes or static during calls.
• Screen lights up by itself or settings change automatically.
• Strange SMS containing random characters.
• Phone takes unusually long to shut down.

If multiple symptoms appear simultaneously, seek technical assistance immediately and perform a complete security check.

Remember

Cyber Safety begins with YOU.
Stay Alert.
Stay Informed.
Stay Protected.

Together, we can build a safer digital environment for every citizen—especially our senior citizens.

NextCyberJagruktaDiwas

The next Cyber JagruktaDiwas will be observed on Wednesday, 2nd September 2026.

Topic:
CreatingStrongPasswordsandManagingThemSecurelyintheDigitalAge
***Learnhowtocreateunbreakablepasswords*, *usepasswordmanagers*, *enablemulti-factorauthentication*, *andprotectyouronlineaccountsfromcybercriminals*.**

02.09.2026 – 29th Episode Today, Wednesday, 2nd September 2026, is the first Wednesday of the month – observed across India as ***erJagrooktaDiwas*** (Cyber Awareness Day).
The first Wednesday of every month is dedicated to creating awareness about cyber safety and sensitizing citizens to protect themselves against cyber frauds and online crimes.
As part of its 𝔻𝕚𝕘𝕚𝕥𝕒𝕝 ℙ𝕒𝕥𝕙𝕒𝕤𝕒𝕝𝕒 - ***EmpoweringElders*** initiative, ***ElderRecreationActivities-era*** has been conducting a monthly Cyber JagruktaDiwas Awareness Programme to promote safe and confident use of digital technology among senior citizens.
Topicofthe 29***thEpis --JAMDepositScam - Arecentdigitalpaymentfraud***
Whatisthe "***JAMDepositScam***"?The term "JAM Deposit Scam" does not appear to be an official RBI or Government classification of a particular scam. It is a relatively recent media/social-media term used for a fraud pattern in which a person receives an unexpected small credit/deposit, such as ₹500, ₹1,000 or ₹2,000, and is then manipulated into taking an unsafe action.
This should not be confused with the Government's JAM Trinity — Jan Dhan + Aadhaar + Mobile, which is a legitimate financial-inclusion system. (Press Information Bureau)
Howthescamtypicallyworks
A common pattern is:
❶ .Unexpected money appears .You receive an SMS/UPI notification saying that money has been credited to your account.
❷ .The fraudster creates curiosity or panic. You may receive a call/message such as:"We accidentally transferred ₹1,000 to your account. Please return it immediately."Or you may be told to open a particular UPI/banking app to "verify" the transaction.
❸ .The victim is persuaded to perform a transactionThe scammer may send a collect/payment request, QR code or link and say that entering the UPI PIN is necessary to receive/refund the money.
❹ .The victim enters the UPI PINThis is the critical point: a UPI PIN is used to authorise a payment, not to receive money. RBI specifically warns that entering a PIN/OTP is not required to receive money.
❺ .Money is debitedInstead of receiving money, the victim may unknowingly approve a payment to the fraudster.
Themostimportantlessonforseniorcitizens
● MONEY COMING IN → NO PIN REQUIRED
● MONEY GOING OUT → PIN/authorisation may be required
So if someone says:"Enter your UPI PIN to receive money" — STOP.It is a major red flag.
Butthereisanotherrelateddanger*: *the* "*MoneyMule*" *trap
This is particularly important to explain to elderly people.A fraudster may say:"I will deposit money into your account. You just transfer it to another account and keep ₹500 as commission."It may look like an easy way to earn money.
But the deposited money could actually be stolen or fraudulent money. Your account then becomes a money-mule account through which criminals move illegal funds.
RBI explicitly warns people not to allow others to use their bank account for movement of funds and says attractive offers to receive or forward money through your account can result in serious legal trouble. (Reserve Bank of India)
RBI also notes that even an innocent person recruited as a money mule can have their account suspended and may face investigation or legal action. (Reserve Bank of India)
Howelderlypeopleshouldprotectthemselves
Remember these 8 rules

1 ☐ Never enter UPI PIN to receive money.
2 ☐ Never scan a QR code to receive a refund/payment.
Scanning a QR code and entering your PIN generally authorises a payment.
3 ☐ Don't click a link sent by an unknown person to “claim”, “verify” or “reverse” a deposit.
4 ☐ Don't call back a suspicious number contained in an SMS.
Check with your bank using its official customer-care number.
5 ☐ If an unknown amount is credited, don't panic and don't immediately return it.
First verify the transaction in your actual bank/UPI transaction history.
6 ☐ Never allow anyone to use your bank account to receive or transfer money for a commission.
7 ☐ Never disclose OTP, UPI PIN, ATM PIN, CVV, internet-banking password or card details.
8 ☐ If money has actually been debited fraudulently, act immediately.

Whattodoifasuspiciousamountisdeposited

For an elderly person, I would recommend this simple procedure:
STOP → DON'T TOUCH → VERIFY → INFORM
STOP: Don't respond to the caller.
DON'T TOUCH: Don't click their link, scan their QR code or approve a UPI request.
VERIFY: Check the transaction independently in the official banking app/passbook/statement.
INFORM: If necessary, contact your bank through its official channel and ask how to handle the unexpected credit.
If the person has already lost money, immediately contact the bank and report the financial cyber fraud through 1930 and National Cyber Crime Reporting Portal. The official reporting system asks victims to provide transaction details, date, amount, account/UPI information and screenshots where available. (Cyber Crime Portal)

Onemoreimportantpoint

An unexpected credit doesn't automatically mean that your account has been hacked. The danger often begins when the victim, after seeing the unexpected credit, follows instructions from the fraudster and authorises a payment or reveals credentials.
So the awareness message should not be:
“If unknown money comes into your account, your account will immediately be emptied.”
A more accurate message is:
“An unexpected deposit is a warning sign. Don't let curiosity or panic make you authorise the next transaction.”

📌NextCyberJagruktaDiwas

The next Cyber JagruktaDiwas will be observed on Wednesday, 8th October 2026Topic: ***CreatingStrongPasswordsandManagingThemSecurelyintheDigitalAge*** --- ***Learnhowtocreateunbreakablepasswords***, ***usepasswordmanagers***, ***enablemulti-factorauthentication***, ***andprotectyouronlineaccountsfromcybercriminals***.

Courtesy
ElderRecreationActivities-era
www.eraindia.org.in