CYBER SMART GUJARAT

Complete Cybersecurity Awareness Masterclass

ગુજરાત અને ભારતમાં Cyber Fraud થી કેવી રીતે બચવું?

Fraud ઓળખો · ફોન સુરક્ષિત રાખો · યોગ્ય સમયે report કરો



Presented by Nirmal Rabari

આજે આપણે શું શીખવાના છીએ?

- આ Masterclass પૂર્ણ થયા પછી તમે:
- 25+ પ્રકારના Cyber Frauds ઓળખી શકશો.
- Fraudster કેવી રીતે લોકોને ફસાવે છે તે સમજી શકશો.
- Fake Calls, Messages અને Websites ઓળખી શકશો.
- તમારા Bank Account અને Smartphone સુરક્ષિત રાખી શકશો.
- WhatsApp, Instagram અને Gmail સુરક્ષિત કરી શકશો.



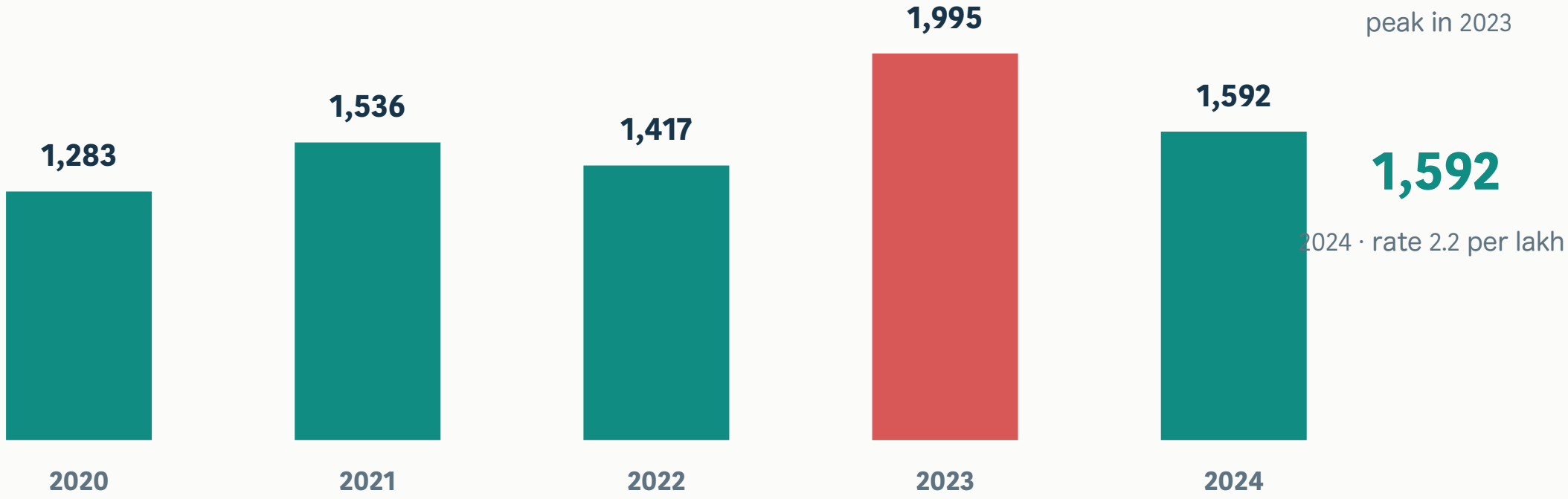
એક પ્રશ્ન: શું તમે સુરક્ષિત છો?

- Audience Interaction:
- શું તમે ક્યારેય અજાણી Link પર Click કરી છે?
- શું તમે WhatsApp પર આવેલી APK File Download કરી છે?
- શું તમે કોઈને OTP આપ્યો છે?
- શું તમે અજાણ્યા વ્યક્તિને Screen Sharing Access આપ્યો છે?
- શું તમે Google પરથી મળેલા Customer Care Number પર ફોન કર્યો છે?



ગુજરાતમાં નોંધાયેલા Cybercrime કેસ

NCRB police-registered cases — reported year; not all complaints or attempted frauds.



1,995

peak in 2023

1,592

2024 · rate 2.2 per lakh

ભારતમાં Financial Cyber Fraud reports

NCRP complaints and reported amounts; 2025 figure is provisional as reported in Parliament.

વર્ષ	REPORTS	રિપોર્ટ થયેલી રકમ
2021	2.63 lakh	₹551 cr
2022	6.94 lakh	₹2,290 cr
2023	13.10 lakh	₹7,465 cr
2024	19.19 lakh	₹22,848 cr
2025	24.03 lakh	₹22,495 cr

Report count વધી શકે છે જ્યારે reported amount ઘટે; બંને અલગ માપ છે.

ગુજરાત: NCRP cyber-fraud reports

આંકડા inceptionથી 28 Feb 2025 સુધી; આ અલગ reporting measures છે.

3,67,754

incidents reported

₹2,745.90 cr

amount reported

₹556.98 cr

amount marked lien

₹10.32 cr

amount refunded

Lien, refund અને reported amount સીધી સરખામણીથી recovery rate ન કાઢો.

7. ડર | FEAR

Cybercriminals ઘણી વાર technology કરતાં human psychologyનો વધુ ઉપયોગ કરે છે.

Fraudster શું કરાવે છે?

- Bank account બંધ થશે
- Police Complaint / Digital Arrest
- Aadhaarનો ગુનામાં ઉપયોગ થયો
- Electricity કપાશે / Illegal Parcel



જોડાયેલા fraud

Digital Arrest · Fake KYC · Electricity Bill · Fake Police/CBI · Courier Scam

ગભરાઈને નિર્ણય ન લો. Call કાપો, પૈસા ન મોકલો, official channelથી verify કરો.

8. લાલચ | GREED

Cybercriminals ઘણી વાર technology કરતાં human psychologyનો વધુ ઉપયોગ કરે છે.

Fraudster શું કરાવે છે?

- ₹5,000 → ₹50,000નો વાયદો
- દરરોજ guaranteed profit
- Free gift / cashback
- Work from home: ₹10,000 daily



જોડાયેલા fraud

Investment · Trading · Task · Lottery · Fake Job · Gaming Top-up

Guaranteed return પર રોકાઓ. Platform જાતે verify કરો; કોઈ “unlock fee” ન આપો.

9. આળસ | LAZINESS

Cybercriminals ઘણી વાર technology કરતાં human psychologyનો વધુ ઉપયોગ કરે છે.

Fraudster શું કરાવે છે?

- SMS link તરત click
- WhatsApp APK install
- Search resultમાંથી customer care call
- Unknown USSD code / permissions
- Screenshotને payment proof માનવું



જોડાયેલા fraud

APK · Phishing · Fake Customer Care · Call Forwarding · QR / Fake Payment

Link, app, number અને bank transaction — ચારેય verify કર્યાં પછી જ આગળ વધો.

લાગણી ઓળખો. નિર્ણય પરત મેળવો.

ત્રણ triggers માટે ત્રણ વિરામ.

ડર લાગે	→	રોકાઈ જાઓ
લાલચ થાય	→	વિચારી લો
shortcut દેખાય	→	VERIFY કરો

STOP · THINK · VERIFY · ACT

Phone પહેલાં mindને manipulate કરવાનો પ્રયાસ થાય છે.

Fraudsterનો પાંચ પગલાનો ચક્ર

- *The Five-Step Fraud Cycle
- Target Selection – કોને ફસાવવો તે પસંદ કરવું.
- Contact – Call, WhatsApp, SMS, Email અથવા Social Media.
- Trust Building – Police, Bank, Government અથવા Companyનું નામ વાપરવું.
- Manipulation – Fear, Greed, Urgency અથવા Emotional Pressure.
- Financial/Data Theft – પૈસા, OTP, Password અથવા Personal Data મેળવવું.



Top 10 cyber frauds ઓળખો

દરેકમાં નકલી ઓળખ, દબાણ અથવા payment/data request તપાસો.

01 UPI / QR payment

02 Digital Arrest

03 Investment / trading

04 APK / fake app

05 OTP / KYC

06 Fake customer care

07 Call forwarding

08 Job / task

09 Online shopping

10 AI voice / deepfake

ATTACK 01 / 25 · UPI Payment Fraud શું છે?

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **UPI = Unified Payments Interface.**
- UPI દ્વારા બેંક ખાતાઓ વચ્ચે Digital Payment થાય છે.
- Common Fraud Methods:
- Fake Payment Screenshot
- Fake Collect Request



ATTACK 01 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 01 · UPI Payment Fraud શું છે?

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Recipient ને જાણીતા channelથી confirm કરો.**
- Collect request approve કરતા પહેલાં amount અને payee તપાસો.
- UPI PIN ફક્ત payment authorize કરવા; receive કરવા નહીં.
- Payment તમારા bank appમાં સફળ દેખાય પછી જ વસ્તુ આપો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 02 / 25 · How to Identify?

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **પૈસા મેળવવા માટે PIN માંગવો.**
- Unknown Collect Request.
- Fake Payment Screenshot.
- Unknown Person દ્વારા Screen Sharing.
- Payment Confirm કર્યા વગર વસ્તુ આપવાનું દબાણ.



ATTACK 02 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 02 · How to Identify?

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **UPI PIN, OTP અથવા screen sharing ક્યારેય ન આપો.**
- Collect requestને ધ્યાનથી વાંચો; અજાણી request decline કરો.
- તમારા bank appમાં transaction status જાતે જુઓ.
- તાકીદ/કેશબેકના દબાણમાં નિર્ણય ન લો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 03 / 25 · QR Code Scam

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **QR Codeનો ઉપયોગ Payment અને Information Access માટે થાય છે.**
- Fraudster શું કરે છે?
- Fake QR Code મોકલે છે.
- Payment Receive કરાવવાનું કહે છે.
- QR Scan કર્યા પછી UPI Appમાં Payment Request ખોલે છે.



ATTACK 03 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 03 · QR Code Scam

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **QR scan કરવાથી સામાન્ય રીતે payment request ખુલે છે; પૈસા મેળવવા QR scan કરવો પડતો નથી.**
- Payee name અને રકમ તપાસો.
- અજાણ્યા QRથી login અથવા payment ન કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 04 / 25 · OTP Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **OTP = One-Time Password.**
- OTP Account Verification અને Transaction Authentication માટે ઉપયોગમાં લેવાય છે.
- Fake Bank Call
- Fake KYC Update
- Fake Customer Support



ATTACK 04 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 04 · OTP Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **OTP કોઈ caller/message સાથે share ન કરો.**
- Bankના official app/siteથી account તપાસો.
- શંકાસ્પદ call કાપી bank card/official site પરના નંબરથી સંપર્ક કરો.



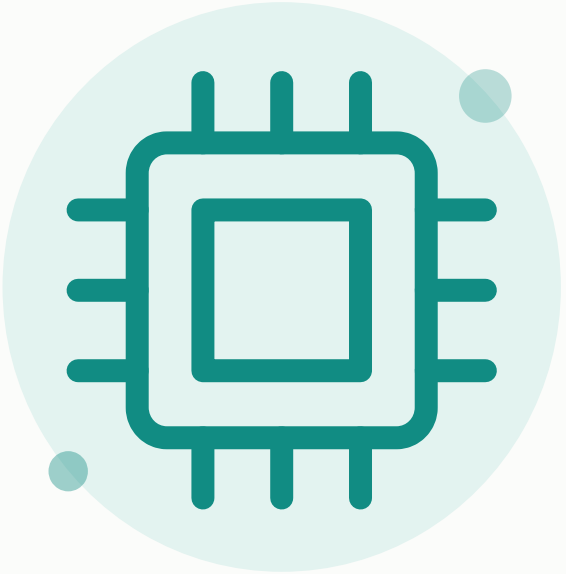
DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 05 / 25 · KYC Update Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **KYC = Know Your Customer.**
- Banks અને Financial Institutions Customer Identity Verify કરવા KYCનો ઉપયોગ કરે છે.
- Fraud કેવી રીતે થાય છે?
- Fake SMS આવે છે.
- Account Block કરવાની ધમકી મળે છે.



ATTACK 05 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 05 · KYC Update Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **SMS link ખોલવાને બદલે bank appમાં KYC status તપાસો.**
- OTP, PIN, CVV અથવા password ન આપો.
- Bankના official channelથી જ KYC પૂર્ણ કરો.



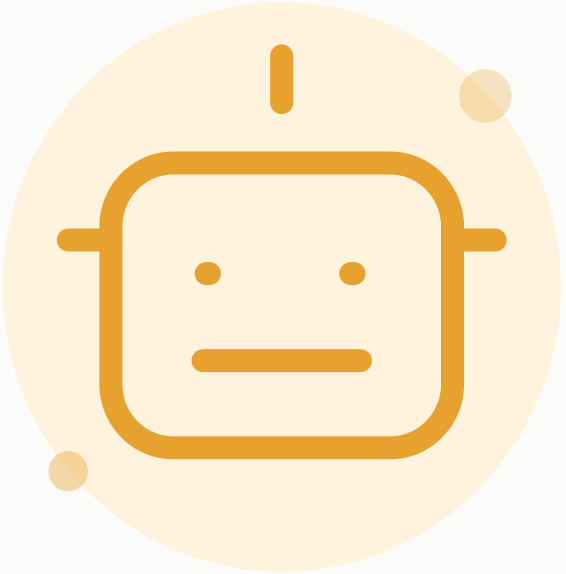
DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 06 / 25 · Digital Arrest Scam

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- ***One of the Most Dangerous Social Engineering Scams**
- Fraudster પોતાને નીચે મુજબ ઓળખાવે છે:
- Police Officer
- CBI Officer
- Customs Officer



ATTACK 06 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 06 · Digital Arrest Scam

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Call disconnect કરો; પૈસા transfer ન કરો.**
- Official police station/channelને તમે જાતે સંપર્ક કરો.
- પરિવાર સાથે વાત કરો; financial fraud થાય તો 1930 પર તરત સંપર્ક કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 07 / 25 · Investment & Trading Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fraudster શું બતાવે છે?**
- Guaranteed Returns
- 5% Daily Profit
- VIP Trading Group
- Fake SEBI Registration



ATTACK 07 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 07 · Investment & Trading Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **SEBI registration અને broker official sourceથી તપાસો.**
- Guaranteed returns અને અજાણ્યા groupsથી સાવચેત રહો.
- Fake dashboardનો profit સાચો ન માનો; withdrawal fee પર અટકો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 08 / 25 · Job & Work From Home Scam

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Common Scams:**
- YouTube Video Like Task
- Google Review Task
- Telegram Task
- Data Entry Scam



ATTACK 08 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 08 · Job & Work From Home Scam

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Job મેળવવા advance fee ન આપો.**
- Company website, email domain અને offer letter verify કરો.
- Unknown apps/links install ન કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 09 / 25 · Online Shopping Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fake Shopping Websites**
- Instagram Store Fraud
- Fake Discounts
- Prepaid Order Scam
- Fake Delivery Messages



ATTACK 09 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 09 · Online Shopping Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Domain, seller reviews, contact details અને payee name તપાસો.**
- ખૂબ ઓછા ભાવ અથવા prepaid-only deal પર રોકાઓ.
- Trusted marketplace અથવા official brand site વાપરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 10 / 25 · Fake Customer Care Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fraudster Fake Customer Care Number Internet પર મૂકે છે.**
- Victim Google Search કરીને Number પર ફોન કરે છે.
- પછી Fraudster:
- OTP માંગે છે.
- UPI Payment કરાવે છે.



ATTACK 10 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 10 · Fake Customer Care Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Customer-care નંબર official app/site અથવા card પરથી મેળવો.**
- OTP, UPI PIN અથવા remote access ન આપો.
- Search-result નંબરને official હોવાનું માની ન લો.



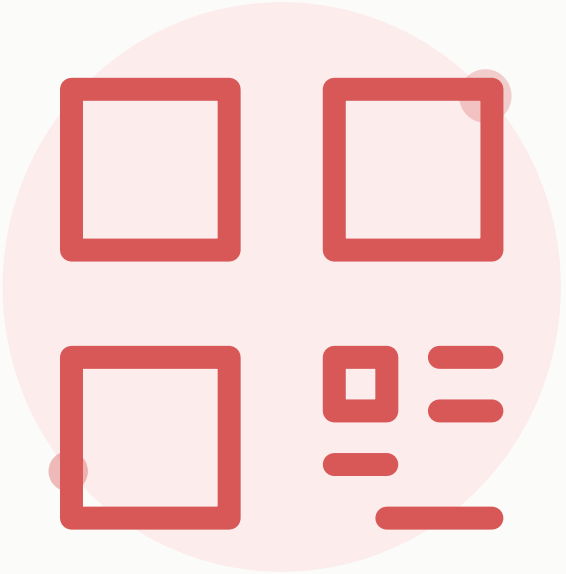
DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 11 / 25 · Electricity Bill & Government Scheme Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Common Messages:**
- Electricity Bill Pending.
- Your Connection Will Be Disconnected.
- Government Subsidy Approved.
- LPG Subsidy Pending.



ATTACK 11 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 11 · Electricity Bill & Government Scheme Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Bill અને subsidy official utility/government portalમાં જાતે ચકાસો.**
- SMS/WhatsApp linkથી APK install ન કરો.
- Urgent disconnection threatમાં callerને payment ન કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 12 / 25 · Loan App Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fraud કેવી રીતે થાય છે?**
- Instant Loan Advertisement.
- Fake Loan Application.
- Excessive Permissions.
- Contact List Access.



ATTACK 12 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 12 · Loan App Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **RBI-regulated lender તપાસો અને loan agreement વાંચો.**
- App permissions મર્યાદિત રાખો; contacts/gallery access ન આપો જો જરૂરી ન હોય.
- Harassmentના પુરાવા સાચવો અને ફરિયાદ કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 13 / 25 · Romance & Matrimonial Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Common Techniques:**
- Fake Identity.
- Fake Marriage Proposal.
- Emotional Manipulation.
- Fake Emergency.



ATTACK 13 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 13 · Romance & Matrimonial Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **ઓળખ independent રીતે verify કરો; trusted family/friendને કહો.**
- પૈસા, gift charges અથવા private documents મોકલશો નહીં.
- Urgency અને secrecyના દબાણને red flag માનો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 14 / 25 · Sextortion & Blackmail

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fraudster Victimને Video Call અથવા Fake Profile દ્વારા ફસાવે છે.**
- પછી:
- Recording કરવાની ધમકી.
- Private Photos Leak કરવાની ધમકી.
- Money Demand.



ATTACK 14 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 14 · Sextortion & Blackmail

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- ***Victimએ શું કરવું?**
- Panic ન કરો.
- પૈસા ચૂકવવાની ઉતાવળ ન કરો.
- પુરાવા સાચવો.
- Account Privacy વધારવી.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 15 / 25 · SIM Swap Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **SIM Swap એટલે Victimના Mobile Numberનું Unauthorized SIM Replacement અથવા Transfer.**
- Fraudster શું કરવાનો પ્રયાસ કરે છે?
- Personal Details મેળવવા.
- Fake Identity Documents વાપરવા.
- Telecom Operatorને છેતરવા.



ATTACK 15 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 15 · SIM Swap Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **SIM પર અચાનક No Service આવે તો operatorને તરત સંપર્ક કરો.**
- Bankને જાણ કરો અને મહત્વના account passwords સુરક્ષિત કરો.
- Account activity અને transaction alerts તપાસો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 16 / 25 · Identity Theft & Digital Credentials Theft

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **કોઈ વ્યક્તિ તમારી ઓળખનો ગેરકાયદેસર ઉપયોગ કરે તેને Identity Theft કહેવાય છે.**
- Sensitive Information:
- Aadhaar Number
- PAN Number
- Passport Details



ATTACK 16 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 16 · Identity Theft & Digital Credentials Theft

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Documents પર purpose/date watermark મૂકો; જરૂરી હોય તેટલું જ share કરો.**
- Aadhaar biometric lockનો વિકલ્પ સમજો.
- Strong unique password અને 2FA વાપરો; activity ચકાસો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 17 / 25 · APK Fraud: Fake Android Applications

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **APK = Android Package Kit.**
- Android Application Install કરવા માટે વપરાતું Package Format.
- Fraudster APK દ્વારા શું કરવાનો પ્રયાસ કરી શકે?
- Fake Banking App.
- Fake KYC App.



ATTACK 17 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 17 · APK Fraud: Fake Android Applications

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Official app store/websiteમાંથી જ install કરો; Play Protect ચાલુ રાખો.**
- Unknown sources અને unnecessary Accessibility/SMS permissionsથી દૂર રહો.
- Install થઈ ગયું હોય તો clean deviceથી bankને જાણ કરો; suspicious app/permissions દૂર કરો; evidence સાચવો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 18 / 25 · Call Forwarding / Call Transfer Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Call Forwarding એક Legitimate Telecom Feature છે.**
- તેનો ઉપયોગ Calls બીજા Number પર Forward કરવા માટે થાય છે.
- Fraud કેવી રીતે થાય છે?
- Fraudster Fake Customer Support બનીને Call કરે છે.
- કહે છે કે તમારા Numberમાં Network Problem છે.



ATTACK 18 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 18 · Call Forwarding / Call Transfer Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **અજાણ્યા callerના કહેવા પર કોઈ code dial ન કરો.**
- Phone settings અથવા operator appમાં forwarding તપાસો.
- Unknown forwarding હોય તો operatorને સંપર્ક કરો અને bank accounts સુરક્ષિત કરો.



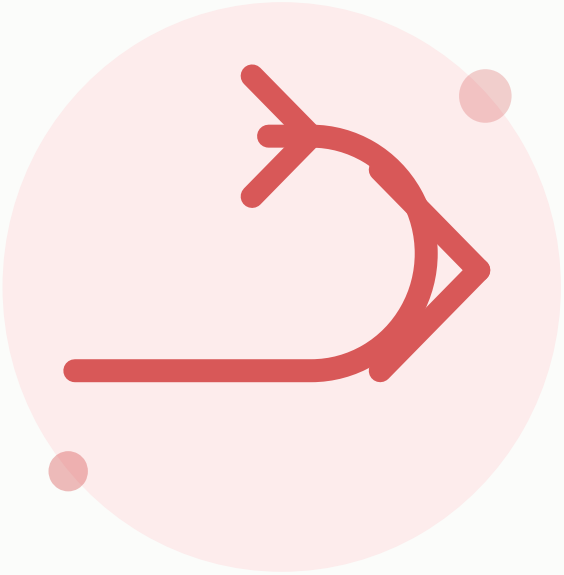
DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 19 / 25 · Juice Jacking & Public USB Charging Risk

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Juice Jacking એટલે Compromised USB Charging Equipment દ્વારા Data Access અથવા Malware Deliveryનો સંભવિત જોખમ.**
- Public Charging Points ક્યાં હોય છે?
- Airports.
- Railway Stations.
- Shopping Malls.



ATTACK 19 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 19 · Juice Jacking & Public USB Charging Risk

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **પોતાનો charger/adapter અથવા power bank વાપરો.**
- USB data blocker વાપરી શકો; file transfer મંજૂર ન કરો.
- Unknown computer સાથે phone જોડવાનું ટાળો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 20 / 25 · Top-Up / Recharge / Gaming Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Common Examples:**
- Fake Mobile Recharge.
- Fake Cashback.
- Gaming Account Top-Up.
- Free UC / Diamonds Offers.



ATTACK 20 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 20 · Top-Up / Recharge / Gaming Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Official app/game store અને payment channel વાપરો.**
- Credentials share ન કરો; free currency/cashback linksથી સાવચેત રહો.
- Payment પહેલાં merchantનું નામ verify કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 21 / 25 · Credit Card / Debit Card Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Common Fraud Types:**
- Card Skimming.
- Card Details Theft.
- Fake Payment Gateway.
- Card-Not-Present Fraud.



ATTACK 21 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 21 · Credit Card / Debit Card Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Transaction alerts ચાલુ કરો; card ગુમ થાય તો તરત block કરો.**
- Unknown websiteમાં card details ન આપો.
- ATM/terminalમાં suspicious device દેખાય તો ઉપયોગ ન કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 22 / 25 · Social Media Account Hacking

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Platforms:**
- Instagram
- Facebook
- WhatsApp
- Telegram



ATTACK 22 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 22 · Social Media Account Hacking

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **દરેક account માટે અલગ strong password અને 2FA વાપરો.**
- Login activity/linked devices તપાસો; અજાણ્યા sessions logout કરો.
- Recovery email અને phone updated રાખો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 23 / 25 · Mule Account Fraud

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Money Mule એટલે એવી વ્યક્તિ જેનું Bank Account ગેરકાયદેસર રીતે Fraudના પૈસા મેળવવા અથવા આગળ Transfer કરવા વપરાય.**
- Fraudster શું કહે છે?
- "તમારા Accountમાં પૈસા આવશે. અમને Transfer કરી આપો. તમને Commission મળશે."
- આથી વ્યક્તિ અનજાણતાં Money Laundering Networkનો ભાગ બની શકે છે.
- *Protection:



ATTACK 23 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 23 · Mule Account Fraud

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Bank account ભાડે ન આપો કે અજાણ્યા પૈસા આગળ transfer ન કરો.**
- Account details share ન કરો; શંકાસ્પદ transaction bankને જણાવો.
- Investigationમાં bank/policeને સહકાર આપો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 24 / 25 · Digital Arrest, Fake Courier & Customs Scam

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **Fraudster તમને કહે છે:**
- "તમારા નામે Illegal Parcel મળ્યું છે."
- પછી:
- Fake Courier Company Call.
- Fake Customs Notice.



ATTACK 24 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 24 · Digital Arrest, Fake Courier & Customs Scam

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **Courierને official trackingથી verify કરો.**
- Fake police/customs threat પર પૈસા કે personal details ન આપો.
- Official police/courier channelનો તમે જાતે સંપર્ક કરો.



DO NOT PANIC · STOP · VERIFY · REPORT

ATTACK 25 / 25 · WhatsApp Account Takeover

આ હુમલો કેવી રીતે શરૂ થાય છે અને કઈ માહિતી/પૈસા મેળવવાનો પ્રયાસ થાય છે.

ATTACK PATTERN

- **OTP Theft.**
- Linked Device Misuse.
- Fake Support Call.
- QR Code Login Trick.
- SIM Swap.



ATTACK 25 · ઓળખો → રોકાઓ → સ્વતંત્ર રીતે Verify કરો

PROTECT 25 · WhatsApp Account Takeover

એક મિનિટમાં ઉપયોગી સુરક્ષા પગલાં.

તમારે શું કરવું?

- **WhatsApp Two-step verification ચાલુ કરો.**
- Linked Devices તપાસો અને અજાણ્યા device logout કરો.
- OTP share ન કરો; recovery email અને phone lock સુરક્ષિત રાખો.



DO NOT PANIC · STOP · VERIFY · REPORT

Website Spoofing & Fake URLs

- Fraudster Genuine Website જેવી દેખાતી Fake Website બનાવે છે.
- Example:
- Genuine: bankname.com
- Fake: bankname-secure-login.example
- *How to Identify?
- Domain Name તપાસો.



Malware, Spyware & Ransomware

- Malware = Malicious Software.
- Types:
- Virus
- Trojan
- Spyware
- Ransomware



Offline backup રાખો; ransomware માંગે તે ચૂકવવાથી recoveryની ખાતરી નથી.

AI દ્વારા થતા નવા Cyber Frauds

- AI Fraudstersને વધુ Realistic Content બનાવવામાં મદદ કરી શકે છે.
- Common Threats:
- AI Voice Cloning.
- Deepfake Video.
- Fake Identity.
- AI-Generated Phishing.



AI Voice Cloning Scam

- Example:
- તમને ફોન આવે છે.
- "પપ્પા, હું મુશ્કેલીમાં છું. મને અત્યારે ₹50,000 મોકલો."
- અવાજ તમારા પુત્ર અથવા પરિવારના સભ્ય જેવો લાગે છે.
- પરંતુ આ AI Voice Cloning હોઈ શકે છે.
- *Protection:



Deepfake Video Scam

- Deepfake Technologyનો ઉપયોગ કરીને કોઈ વ્યક્તિનો Face અથવા Voice બદલાઈ શકે છે.
- Common Risks:
- Fake CEO Video.
- Fake Government Official.
- Fake Investment Expert.
- Fake Celebrity Endorsement.



AI Prompt & Data Privacy Risks

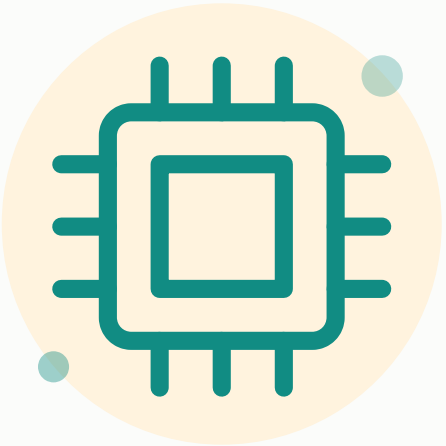
- AI Tools વાપરતી વખતે શું Upload ન કરવું?
- Bank Password.
- OTP.
- Customer Database.
- Aadhaar / PAN Documents.
- Company Confidential Documents.



Public AI toolમાં secrets, passwords, customer data અથવા confidential files upload ન કરો.

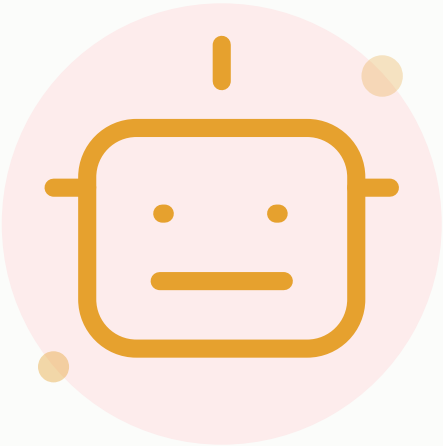
AI Agents & Business Security

- AI Agentsને Email, CRM, Documents અને Business Toolsની Access હોઈ શકે છે.
- Potential Risks:
- Unauthorized Actions.
- Prompt Injection.
- Sensitive Data Leakage.
- Excessive Permissions.



Practical Demo 1: Fake vs Genuine SMS

- *Message A:
- Your bank account will be blocked today. Click this link immediately to update KYC.
- *Message B:
- Your bank has recorded a transaction. Check your official bank app for details.
- Audience Questions:
- Which message creates urgency?



SMS ઓળખો · T · G · S · P

Demo 1 પછી: Header suffix category બતાવી શકે છે; sender identity અને link અલગથી verify કરો.

T · TRANSACTION

Transactionની પુષ્ટિ/જાણ. Link હોય તો official appમાં જાતે ખોલીને તપાસો.

G · GOVERNMENT

Government સંદેશા. Scheme/benefit official .gov.in portalથી ચકાસો.

S · SERVICE

તમે લીધેલી service માટે updates. Unexpected APK, OTP અથવા payment request પર રોકાઓ.

P · PROMOTION

Offer/marketing. Cashback માટે PIN/OTP ન આપો; અજાણી link ન ખોલો.



Practical Demo 2: APK Fraud Awareness

- Official App Store.
- App Developer Name.
- App Permissions.
- Play Protect.
- Unknown Sources Setting.
- Accessibility Permission.



APKના નામો બદલાય છે · જોખમ એક જ

Demo 2 પછી: નીચેના નામો માત્ર ઓળખ માટેના scam examples છે; install/demo ન કરો.

ELECTRICITY / LIGHT BILL

lightbill.apk · gasbill.apk

SERVICE / CHANNEL

channel.apk · chnnale.apk

TAX / RETURN

itr.apk · gsr-3b.apk · gstr-3b.apk

યાદ રાખો

ફાઇલનું નામ સાચું હોવાનો પુરાવો નથી. Official Play Store/website સિવાયની APK install ન કરો.



Practical Demo 3: Call Forwarding Safety

- Phone Call Settings.
- Call Forwarding Menu.
- Active Forwarding Status.
- Telecom Operator Support.
- Ask:
- "શું તમે ક્યારેય કોઈ અજાણ્યા વ્યક્તિના કહેવા પર Dial Code Enter કર્યો છે?"



Call forwarding scam · કોડનું દબાણ ઓળખો

Demo 3 પછી: caller તમને “network fix”, delivery અથવા KYC કહી dialing pattern કરાવે છે.

SCAM PATTERN

કોડ + અજાણ્યો destination number + # જેવી request. Caller OTP-call access મેળવવાનો પ્રયાસ કરી શકે.

DoT STATUS

*401# આધારિત USSD call-forwarding facility 15 Apr 2024થી આગળની સૂચના સુધી suspend કરાઈ હતી. કોઈ અજાણ્યો code dial ન કરો.

સેફ ડેમો

ફક્ત screenshot/mock dialer. વાસ્તવિક SIM અથવા real code પર Call દબાવશો નહીં.



Forwarding તપાસો અને સુરક્ષિત રીતે બંધ કરો

કોઈ universal disable code માનશો નહીં. તમારા operator અને handset માટે official steps લો.

ANDROID

Phone app → Settings → Calling accounts/SIM → Call forwarding → દરેક condition તપાસો → અજાણ્યું હોય તો Disable.

iPHONE

Settings → Apps → Phone → Call Forwarding (menu model/iOS પ્રમાણે બદલાય) → status તપાસો/બંધ કરો.

JIO-SPECIFIC CODES

Jio mobile માટે જ: *402 all · *404 no answer · *406 busy · *410 unreachable · *413 all. Official Jio Helpમાં confirm કરો.

IF SOMETHING LOOKS WRONG

Operatorના official app/site/known numberથી call કરો; Bankને alert કરો; account activity તપાસો.



Jio Call Forwarding · disable codes

Jio mobile voice service માટે official FAQમાં દર્શાવેલા deactivation codes; અન્ય operator/deviceમાં વાપરશો નહીં.

***402**

Unconditional forwarding બંધ

***404**

No answer forwarding બંધ

***406**

Busy forwarding બંધ

***410 · *413**

Not reachable બંધ · all forwarding બંધ



Practical Demo 4: UPI Safety

- Show:
- UPI ID Verification.
- Payment Recipient Name.
- Collect Request.
- Transaction History.
- Payment Alerts.



UPI AutoPay · mandate પહેલાં સમજો

Demo 4 પછી: recurring debitનું control તમારી UPI appમાં છે.

MANDATE REVIEW

UPI app → Manage Bank Accounts / UPI AutoPay → merchant, amount/limit, frequency, validity અને next debit તપાસો.

CONTROL

જરૂર ન હોય તો mandate pageથી Pause, Modify અથવા Revoke કરો; અજાણી mandate bank/UPI appને report કરો.

RECEIVING MONEY?

પૈસા મેળવવા UPI PIN નાખવાની જરૂર નથી. Collect request વાંચ્યા વગર approve ન કરો.



UPI PIN અને mPIN · બંને અલગ રાખો

કોઈ caller, screen-share helper અથવા support agentને PIN/OTP ન જણાવો.

UPI PIN

UPI payment authorization PIN; NPCI FAQ says bank transactions are authorized with UPI PIN. Never share it.

mPIN

Bank/mobile app login PIN છે; UPI PINથી અલગ હોઈ શકે. App અને bank પ્રમાણે ઉપયોગ બદલાય છે.

SAFETY RULE

PIN only in your trusted UPI app’s secure prompt after checking payee/amount. Receiving a payment never needs your PIN.

PROTECT THE APP

Phone lock + app lock/biometric, transaction alerts, updated app, and no screen sharing during payment.



UPI · દર મહિને 60-second security check

Transaction history, mandates અને bank alerts એક સાથે તપાસો.

1 · REVIEW

Recent UPI transactions અને active AutoPay mandates તપાસો.

2 · REVOKE

Unknown mandate pause/revoke કરો; app/bankના official helpથી confirmation લો.

3 · REPORT

Unauthorized debit હોય તો તરત bank/UPI appને જાણ કરો; financial cyber fraud માટે 1930 અને cybercrime.gov.in.



Practical Demo 5: WhatsApp & Google Security

- WhatsApp Two-Step Verification.
- Linked Devices.
- Gmail Security Checkup.
- Google Account Devices.
- Password Change.
- Recovery Email.



Cyber Fraud થાય તો First 5 Minutesમાં શું કરવું?

- *Emergency Action Plan
- Panic ન કરો.
- Further Payment બંધ કરો.
- Bank / UPI Providerનો Official Contact કરો.
- Account અથવા Card Block / Secure કરાવો.
- Financial Fraud માટે 1930 પર તરત Call કરો.



પહેલા Bank/UPI providerને જાણ કરો અને financial fraud માટે 1930 પર તરત call કરો.

Important Cybercrime Reporting Resources

- *National Cyber Crime Helpline: 1930
- *Online Complaint:
- Other Useful Resources:
- Bank's Official Fraud Helpline.
- Local Cyber Crime Police Station.
- CERT-In: https://www.cert-in.org.in/



Financial cyber fraud reporting helpline: 1930 · Portal: cybercrime.gov.in

What Evidence Should You Preserve?

- Evidence Checklist:
- Transaction ID / UTR.
- Bank Account Statement.
- Fraudster Phone Number.
- WhatsApp Chat.
- SMS.



If Your WhatsApp or Instagram Gets Hacked

- *Recovery Steps:
- Official Appમાંથી Account Recovery શરૂ કરો.
- Phone Number / Email Ownership Verify કરો.
- Unknown Sessions Logout કરો.
- Password બદલો.
- Two-Factor Authentication ચાલુ કરો.



If Your Phone Has a Suspicious APK

- *Action Plan:
- Suspicious Appનો Internet Access બંધ કરો.
- Clean Device પરથી Bankને જાણ કરો.
- Remote Access અને Accessibility Permissions તપાસો.
- Suspicious Application Remove કરો.
- Important Passwords Clean Device પરથી બદલો.



Cyber Safety Quiz: Question 1

- તમને કોઈ કહે કે ₹5,000 Receive કરવા UPI PIN નાખો.
- શું કરશો?
- A. PIN નાખીશ.
- B. Payment Request Accept કરીશ.
- C. Request Reject કરીશ અને Verify કરીશ.
- D. OTP આપીશ.



Cyber Safety Quiz: Question 2

- તમને WhatsApp પર Electricity Bill APK મળે છે.
- શું કરશો?
- A. Install કરીશ.
- B. મિત્રો સાથે Share કરીશ.
- C. Official Electricity Board Website પરથી Verify કરીશ.
- D. Appને તમામ Permissions આપીશ.



Cyber Safety Quiz: Question 3

- કોઈ Fake Police Officer Video Call પર કહે કે તમારું Account Illegal Activityમાં વપરાયું છે અને પૈસા મોકલો.
- શું કરશો?
- A. પૈસા મોકલી દઈશ.
- B. Account Details આપીશ.
- C. Call Disconnect કરીને Official Police અને Family સાથે Verify કરીશ.
- D. OTP આપીશ.



Cyber Safety Quiz: Question 4

- તમારા Phoneમાં અચાનક Network બંધ થઈ જાય અને Bank OTP આવવાનું બંધ થાય.
- શું કરશો?
- A. રાહ જોઈશ.
- B. તરત Telecom Operatorનો સંપર્ક કરીશ અને Bankને જાણ કરીશ.
- C. Unknown Link પર Click કરીશ.
- D. Password કોઈને આપીશ.



Cyber Safety Quiz: Question 5

- તમને પરિવારના સભ્યના અવાજમાં પૈસા માંગતો Call આવે.
- શું કરશો?
- A. તરત પૈસા મોકલી દઈશ.
- B. બીજી Verification Channelથી ઓળખ Confirm કરીશ.
- C. Bank OTP આપીશ.
- D. અજાણી વ્યક્તિને Payment કરીશ.



પ્રશ્નો અને જવાબો · 1/2

ટૂંકા જવાબો slide notesમાં; ચર્ચા માટે રોકાઓ.

Q1. શું માત્ર Link Click કરવાથી Bank Account ખાલી થઈ શકે?

Q2. શું UPI PIN કોઈને આપવો જોઈએ?

Q3. શું WhatsApp પર આવેલો APK File ખોલવો સુરક્ષિત છે?

Q4. શું Police Video Call પર Arrest કરી શકે?

Q5. શું Deleted Photos Recover થઈ શકે?

પ્રશ્નો અને જવાબો · 2/2

ટૂંકા જવાબો slide notesમાં; ચર્ચા માટે રોકાઓ.

Q6. શું Public Wi-Fi વાપરવું ખતરનાક છે?

Q7. શું Antivirus દરેક Virusથી બચાવી શકે?

Q8. શું Google પર દેખાતો Customer Care Number સાચો હોય છે?

Q9. શું Phoneમાં Camera અને Microphone Permissions આપવી જોખમી છે?

Q10. જો પૈસા કપાઈ જાય તો શું Bank Refund આપશે?

25 Golden Cybersecurity Rules · 1/3

દરરોજ ઉપયોગી થતી 8–9 સરળ સુરક્ષા આદતો.

1. **OTP કોઈને ન આપો.**
2. UPI PIN Share ન કરો.
3. Strong Password બનાવો.
4. દરેક Account માટે Unique Password રાખો.
5. 2FA ચાલુ રાખો.
6. Unknown APK Install ન કરો.
7. Unknown Links પર Click કરતાં પહેલાં Verify કરો.
8. Fake Customer Careથી સાવચેત રહો.
9. QR Code દ્વારા Payment પહેલાં Amount તપાસો.

25 Golden Cybersecurity Rules · 2/3

દરરોજ ઉપયોગી થતી 8–9 સરળ સુરક્ષા આદતો.

- **Fake Investment Schemesથી દૂર રહો.**

11. Job માટે Advance Payment ન કરો.
12. Public Wi-Fi પર Sensitive Work ટાળો.

- Unknown USB Charging Portથી સાવચેત રહો.

14. App Permissions તપાસો.
15. Device Updates કરો.

- Important Data Backup રાખો.

17. Bank Transaction Alerts ચાલુ રાખો.

25 Golden Cybersecurity Rules · 3/3

દરરોજ ઉપયોગી થતી 8–9 સરળ સુરક્ષા આદતો.

- **Social Media Privacy Settings તપાસો.**

19 Unknown Screen Sharing ટાળો.

20 Call Forwarding Settings તપાસો.

- Deepfake Voice અને Video Verify કરો.

22 Personal Documents અનાવશ્યક Share ન કરો.

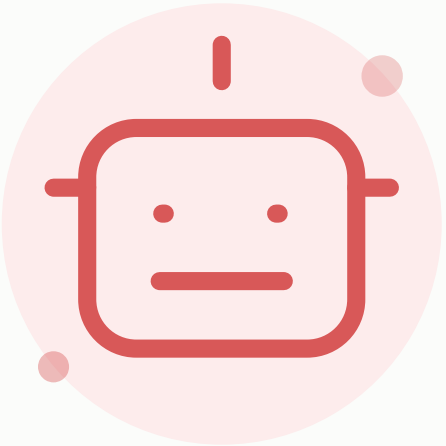
23 Business Data AI Toolsમાં Upload કરતાં પહેલાં તપાસો.

- Family સાથે Emergency Verification Code રાખો.

25 Fraud થાય તો તરત 1930 પર સંપર્ક કરો.

Family Digital Safety Plan

- દરેક પરિવારે નીચેના નિયમો બનાવવા જોઈએ:
- કોઈપણ Emergency Money Requestને Verify કરવી.
- પરિવાર માટે Verification Code રાખવો.
- બાળકોને Online Safety શીખવવી.
- Senior Citizensને Digital Arrest વિશે સમજાવવું.
- OTP અને Password કોઈને ન આપવો.



Business & Employee Cyber Safety

- દરેક Small Business માટે:
- Company Email Security.
- Employee Awareness Training.
- Customer Data Protection.
- Secure Website.
- Regular Backup.



દરેક payment instruction independent channelથી confirm કરો.

Case 1 · Electricity bill + APK

જૂથમાં 60 સેકન્ડ ચર્ચા કરો: trigger, red flag, safe next step.

SCENARIO

“આજે connection કપાશે. Bill જોવા આ APK install કરો.”

- કઈ વાત urgency બનાવે છે?
- Bill ક્યાંથી verify કરશો?
- App install થઈ ગઈ હોય તો હવે શું?

SMS/WhatsAppમાંથી APK નહીં; utilityની official app/site અથવા bill પરનું channel વાપરો.

Case 2 · Fake investment group

જૂથમાં 60 સેકન્ડ ચર્ચા કરો: trigger, red flag, safe next step.

SCENARIO

Groupમાં profit screenshots દેખાય છે. Withdraw કરવા “tax / unlock fee” માંગે છે.

- Dashboardમાં દેખાતો profit સાચો છે?
- Registration કોણ verify કરશે?
- વધુ transfer ક્યારે અટકાવશો?

Profit screenshot પુરાવો નથી. Regulator/platform અને withdrawal terms independently તપાસો.

Case 3 · Family emergency voice

જૂથમાં 60 સેકન્ડ ચર્ચા કરો: trigger, red flag, safe next step.

SCENARIO

ઓળખીતો અવાજ કહે છે: “હમણાં ₹50,000 મોકલો; કોઈને ન કહેશો.”

- AI voice હોઈ શકે?
- કયા બીજા channelથી confirm કરશો?
- Family verification phrase શું રહેશે?

મદદ પહેલાં saved number પર call back કરો; family verification phrase રાખો.

BE DIGITAL SMART.
BE CYBER SAFE.

સાયબર ક્રાઇમથી બચવા Hacker બનવાની જરૂર નથી.

- **સાવચેત રહો** — ઓળખો કે કયો દબાણનો ઉપાય છે.
- **Verify કરો** — Official channelથી જાતે તપાસો.
- **માહિતી સુરક્ષિત રાખો** — OTP, PIN અને passwords private રાખો.
- **ઝડપથી report કરો** — Financial cyber fraud માટે 1930 પર call કરો.



Presented by Nirmal Rabari

Mission: Help 10 Lakh Gujaratis learn AI, technology & digital safety.