राजस्थान स्कूल शिक्षा परिषद्

राजीव गांधी विद्या भवन, द्वितीय तल, शिक्षा संकुल
जवाहरलाल नेहरू मार्ग, जयपुर – 17
फोन नं. 0141–2715518, Email :- rajsmsa.girlsedu@rajasthan.gov.in

क्रमांक: रास्कूशिप/जय/जेण्डर प्रकोष्ठ/ऑनलाईन सेफ्टी/2022–23/ 5118 दिनांक: 8/9/22

मुख्य जिला शिक्षा अधिकारी
एवं पदेन जिला परियोजना समन्वयक,
समस्त जिले।

विषय :– वार्षिक कार्य योजना एवं बजट सत्र 2022–23 साईबर सुरक्षा एवं डिजिटल लर्निंग कौशल गतिविधि अन्तर्गत विस्तृत दिशा–निर्देश।

संदर्भ :– मार्गदर्शिका क्रमांक 2978 दिनांक 12.07.2022 के क्रम में।

उपर्युक्त विषयान्तर्गत संदर्भित पत्र में लेख है कि विद्यार्थियों में डिजिटल लर्निंग के कौशल का विकास करने हेतु आवश्यक है कि उन्हें उपलब्ध माध्यमों की जानकारी हो और उसको उपयोग करना आता हो। डिजिटल संसार के लिये बच्चों को तैयार करने के साथ–साथ, साईबर–क्राईम से बचाव के लिये तैयार करना भी उतना ही आवश्यक है। इस हेतु प्रत्येक विद्यालय को साईबर सुरक्षा जागरूकता विषय पर गतिविधि आयोजन हेतु 500/– रूपये प्रति विद्यालय की दर से 53095 प्रारंभिक विद्यालयों एवं 15360 माध्यमिक विद्यालयों को राशि प्रदान की जा रही है, जिसमें विद्यालय स्तर पर निम्नानुसार राशि को उपयोग किया जाना अपेक्षित है।

- विगत सत्र 2021–22 में राजस्थान स्कूल शिक्षा परिषद द्वारा साईबर सुरक्षा जागरूकता पर विद्यार्थियों हेतु कक्षा 06–08 एवं कक्षा 09–12 हेतु पृथक–पृथक हस्तपुस्तिका का निर्माण कर मुद्रण हेतु प्रति विद्यालय 1800/– रूपये की राशि हस्तांतरित की गई थी तथा साईबर सुरक्षा पर शिक्षक–प्रशिक्षण मॉडयूल का मुद्रण कर प्रति विद्यालय प्रेषित किया जा चुका है।
- निदेशक, माध्यमिक शिक्षा, राजस्थान, बीकानेर द्वारा शिविरा पंचाग सत्र 2022–23 क्रमांक 250 दिनांक 21.06.2022 में नो बैग डे गतिविधि अन्तर्गत साईबर सुरक्षा एवं डिजिटल लर्निंग कौशल गतिविधि को बिन्दु संख्या 13 पर सम्मिलित किया गया है। अतः शिविरा पंचाग अनुसार विद्यालयों में साईबर सुरक्षा संबंधित सत्रों का आयोजन किया जाना सुनिश्चित करें।
- साईबर सुरक्षा पर विद्यार्थियों हेतु राजस्थान स्कूल शिक्षा परिषद द्वारा यूनिसेफ के माध्यम से साईबर पीस फाउन्डेशन के सहयोग द्वारा साईबर गेम तैयार किया गया है, जिसकी परीक्षण प्रक्रिया प्रक्रियाधीन है। परीक्षण प्रक्रिया उपरांत इस गेम को विद्यार्थियों को उपयोग में लिये जाने हेतु प्रदान किया जायेगा। जिसके माध्यम से विद्यार्थियों में खेल–खेल में ही प्रश्नोत्तरी द्वारा साईबर सुरक्षा हेतु समझ विकसित की जा सकेगी।
- प्रत्येक विद्यालय में 30 नवम्बर को राष्ट्रीय साईबर सुरक्षा जागरूकता दिवस का आयोजन किया जाये, जिसमें साईबर सुरक्षा से संबंधित पोस्टर/चित्रकला, निबंध/लेख, वाद–विवाद/आशुभाषण प्रतियागिताओं का आयोजन किया जाये। इस प्रतियोगिता को ई–रक्षा प्रतियोगिता के नाम से जाना जायें। प्रतियोगिताओं में उत्कृष्ट प्रदर्शन करने वाले विद्यार्थियों को 500/– रूपये की राशि में से नकद प्रोत्साहन राशि अथवा उपहार स्वरूप पुरस्कार प्रदान किया जाये तथा साईबर सुरक्षा

1.

प्रतिभागिता सर्टिफिकेट भी प्रदान किया जाये। तथा विजेता विद्यार्थियों की उपलब्धियों को पत्र–पत्रिका में प्रकाशित करवाया जाये।

- विद्यार्थियों को इस प्रतियोगिता के बारे में आयोजित दिवस से पूर्व जानकारी प्रदान की जाये एवं मैन्टर शिक्षक द्वारा भाग लेने वाले विद्यार्थियों की दिनांक 25 नवम्बर तक सूची तैयार की जाये। प्रतियोगिता से पूर्व संचार के माध्यमों से प्रतियोगिता के संबंध में प्रचार–प्रसार किया जाये।
- विद्यार्थियों को जिम्मेदार जागरूक नागरिक बनाने की दिशा में साईबर खतरों की पहचान करना एवं साईबर घटना का शिकार होने पर रिर्पोटिंग से संबंधित जानकारी प्रदान की जाये जिससे विद्यार्थी स्वंय को साईबर अपराध से सुरक्षित किये जाने में सहयोग प्राप्त कर सके।

उक्त स्वीकृति निम्न शर्तो के अधीन प्रदान की जाती है :–

- जिस मद के लिये राशि उपलब्ध कराई जा रही है, व्यय उसी मद में किया जाये।
- व्यय राशि का उपयोगिता प्रमाण–पत्र निर्धारित प्रपत्र में भिजवाया जाना सुनिश्चित करें।
- राशि का उपयोग, योजना के दिशा–निर्देश, एमएचआरडी की गाईडलाईन एवं लोक उपापन में पादरर्शिता अधिनियम 2012 एवं नियम 2013 एवं वित्तीय नियमों की पूर्ण पालना करते हुए विहित प्रक्रियानुसार किया जाना सुनिश्चित करें।
- राजस्थान स्कूल शिक्षा परिषद द्वारा मॉनीटरिंग प्रपत्र में सूचना प्रतिमाह प्रकोष्ठ को भिजवाया जाना सुनिश्चित करें।
- निर्धारित गतिविधि हेतु व्यय की प्रविष्टि प्रत्येक माह की 07 तारीख तक प्रबंध पोर्टल पर किया जाना सुनिश्चित करें।

संलग्न :– उपरोक्तानुसार

(डॉ0 मोहन लाल यादव)
राज्य परियोजना निदेशक

प्रतिलिपि :आवश्यक कार्यवाही हेतु प्रेषित :–

1 निजी सचिव, निदेशक माध्यमिक एवं प्रारंभिक शिक्षा, बीकानेर।
2 निजी सहायक, अतिरिक्त राज्य परियोजना निदेशक, द्वितीय राजस्थान स्कूल शिक्षा परिषद, जयपुर।
3 मुख्य ब्लॉक शिक्षा अधिकारी, संबंधित ब्लॉक।
4 समस्त पीईईओ।
5 संबंधित सहयोगी संस्थाएं, बालिका शिक्षा प्रकोष्ठ।
6 विषय विशेषज्ञ बाल संरक्षण, यूनिसेफ।
7 रक्षित पत्रावली।

(शीलावती मीणा)
अति. राज्य परियोजना निदेशक–2

राजस्थान स्कूल शिक्षा परिषद्

राजीव गांधी भवन, द्वितीय तल, शिक्षा संकुल
जवाहरलाल नेहरू मार्ग, जयपुर – 17

फोन नं. 0141–2715550, 2715517

फैक्स नं. 0141–2701822

क्रमांक : रास्कूशिप/जय/बा.शि./साईबर सेफ्टी/2022–23/5119

दिनांक : 8/9/22

प्रशासनिक स्वीकृति

सत्र 2022–23 में वार्षिक कार्य योजना एवं बजट अन्तर्गत जेण्डर इक्विटी हेतु विशेष प्रोजेक्ट में छात्रों हेतु ऑनलाईन सुरक्षा एवं डिजिटल लर्निंग कौशल गतिविधि हेतु 500/– रूपये की दर से प्रारंभिक शिक्षा के 53095 विद्यालयों हेतु 265.48 लाख रूपये एवं माध्यमिक शिक्षा के 15360 विद्यालयों हेतु 76.80 लाख रूपये इस प्रकार कुल 342.28 लाख रूपये प्रावधानित किये गये है। अतः प्रारंभिक शिक्षा हेतु जिलेवार निम्नानुसार राशि हस्तांतरित किये जाने की स्वीकृति प्रदान की जाती है :–

(Rs. in lakhs)

BUDGET SHEET FOR THE YEAR 2022-23			
Sr.No.	DISTRICT	No. of Schools (ele)	Total fund to be issued for ele
1	AJMER	1334	6.670
2	ALWAR	2034	10.170
3	BANSWARA	2733	13.665
4	BARAN	1282	6.410
5	BARMER	4091	20.455
6	BHARATPUR	1201	6.005
7	BHILWARA	2311	11.555
8	BIKANER	1594	7.970
9	BUNDI	975	4.875
10	CHITTAURGARH	1405	7.025
11	CHURU	896	4.480
12	DAUSA	1184	5.920
13	DHAULPUR	849	4.245
14	DUNGARPUR	2274	11.370
15	GANGANAGAR	1456	7.280
16	HANUMANGARH	730	3.650
17	JAIPUR	2767	13.835
18	JAISALMER	1096	5.480
19	JALOR	1482	7.410
20	JHALAWAR	1361	6.805
21	JHUNJHUNUN	1010	5.050
22	JODHPUR	2839	14.195
23	KARAULI	1119	5.595
24	KOTA	775	3.875
25	NAGAUR	2292	11.460
26	PALI	1340	6.700
27	PRATAPGARH	1509	7.545
28	RAJSAMAND	1420	7.100

29	S.MADHOPUR	780	3.900
30	SIKAR	1347	6.735
31	SIROHI	760	3.800
32	TONK	1167	5.835
33	UDAIPUR	3682	18.410
	TOTAL	53095	265.475

(अक्षरे रूपये दो करोड़ पैंसठ लाख सैंतालीस हजार पांच सौ रूपये मात्र)

उक्त स्वीकृति निम्न शर्तो के अधीन प्रदान की जाती है :–

- जिस मद के लिये राशि उपलब्ध कराई जा रही है, व्यय उसी मद में किया जाये।
- व्यय राशि का उपयोगिता प्रमाण–पत्र निर्धारित प्रपत्र में भिजवाया जाना सुनिश्चित करें।
- राशि का उपयोग, योजना के दिशा–निर्देश, शिक्षा मंत्रालय, भारत सरकार की गाईडलाईन एवं लोक उपापन में पादरर्शिता अधिनियम 2012 एवं नियम 2013 एवं वित्तीय नियमों की पूर्ण पालना करते हुए विहित प्रक्रियानुसार किया जाना सुनिश्चित करें।
- उक्त राशि का व्यय वार्षिक कार्ययोजना वर्ष 2022–23 की पीएबी में स्वीकृत अनुसार मद 79.0.537 में से किया जायेगा।

(डॉ0 मोहन लाल यादव)
राज्य परियोजना निदेशक

दिनांक :

क्रमांक : रास्कूशिप/जय/बा.शि./साईबर सेफ्टी/2022–23/

प्रतिलिपि :– सूचनार्थ एवं आवश्यक कार्यवाही हेतु –

1. निजी सचिव, आयुक्त, राजस्थान स्कूल शिक्षा परिषद, जयपुर।
2. निजी सचिव, राज्य परियोजना निदेशक, राजस्थान स्कूल शिक्षा परिषद, जयपुर।
3. निजी सचिव, अतिरिक्त राज्य परियोजना निदेशक, राजस्थान स्कूल शिक्षा परिषद, जयपुर।
4. वित्तीय सलाहकार, राजस्थान स्कूल शिक्षा परिषद, जयपुर।
5. रक्षित प्रत्रावली।

(शीलावती मीणा)
अतिरिक्त राज्य परियोजना निदेशक–2

RCSCE राजस्थान स्कूल शिक्षा परिषद्
स्कूल शिक्षा विभाग, राजस्थान सरकार

राजस्थान स्कूल शिक्षा परिषद्

आज़ादी का अमृत महोत्सव

सर्वपल्ली डॉ0 राधाकृष्णन शिक्षा संकुल, ब्लॉक–5, द्वितीय एवं तृतीय तल
जवाहर लाल नेहरू मार्ग, जयपुर–302017 फोन : 0141–2700366, E-Mail : rajssa_acctt@yahoo.co.in

क्रमांक :रा.स्कू.शि.प./जय/ जेण्डर एवं इक्विटी/2022–23/5120 दिनांक 8/9/22

प्रशासनिक, वित्तीय एवं आहरण सीमा स्वीकृति

वार्षिक कार्ययोजना एवं बजट 2022–23 में जेण्डर इक्विटी हेतु विशेष प्रोजेक्ट में छात्रों हेतु ऑनलाईन सुरक्षा एवं डिजिटल लर्निंग कौशल गतिविधि अन्तर्गत माध्यमिक एवं उच्च माध्यमिक विद्यालयों हेतु निम्नानुसार जिलों को राजस्थान स्कूल शिक्षा परिषद् का समग्र शिक्षा के **"संचालन पोर्टल"** Single Nodal Account (SNA), SBI **खाता संख्या 40469910973, गांधीनगर, जयपुर** से आपके जिले के सम्मुख अंकित आहरण सीमा तक प्रशासनिक एवं वित्तीय स्वीकृति तथा राशि के आहरण करने की स्वीकृति प्रदान की जाती है:–

क्र. सं.	जिले का नाम	खाता धारक का नाम	आहरण सीमा (राशि लाखों में)
1	अजमेर	जिला परियोजना समन्वयक, समग्र शिक्षा, अजमेर	2.62500
2	अलवर	जिला परियोजना समन्वयक, समग्र शिक्षा, अलवर	3.97500
3	बांसवाड़ा	जिला परियोजना समन्वयक, समग्र शिक्षा, बांसवाड़ा	2.32000
4	बारां	जिला परियोजना समन्वयक, समग्र शिक्षा, बारां	1.54500
5	बाड़मेर	जिला परियोजना समन्वयक, समग्र शिक्षा, बाड़मेर	3.60500
6	भरतपुर	जिला परियोजना समन्वयक, समग्र शिक्षा, भरतपुर	2.77500
7	भीलवाड़ा	जिला परियोजना समन्वयक, समग्र शिक्षा, भीलवाड़ा	2.89000
8	बीकानेर	जिला परियोजना समन्वयक, समग्र शिक्षा, बीकानेर	2.23500
9	बून्दी	जिला परियोजना समन्वयक, समग्र शिक्षा, बून्दी	1.37500
10	चित्तौडगढ	जिला परियोजना समन्वयक, समग्र शिक्षा, चित्तोडगढ	2.05500
11	चूरू	जिला परियोजना समन्वयक, समग्र शिक्षा, चूरू	2.56500
12	दौसा	जिला परियोजना समन्वयक, समग्र शिक्षा, दौसा	1.92500
13	धौलपुर	जिला परियोजना समन्वयक, समग्र शिक्षा, धौलपुर	1.45500
14	डूंगरपुर	जिला परियोजना समन्वयक, समग्र शिक्षा, डूंगरपुर	1.99500
15	श्रीगंगानगर	जिला परियोजना समन्वयक, समग्र शिक्षा, श्रीगंगानगर	2.43500
16	हनुमानगढ़	जिला परियोजना समन्वयक, समग्र शिक्षा, हनुमानगढ़	1.82000
17	जयपुर (शहर)	जिला परियोजना समन्वयक, समग्र शिक्षा, जयपुर	4.93000
18	जैसलमेर	जिला परियोजना समन्वयक, समग्र शिक्षा, जैसलमेर	0.96000
19	जालौर	जिला परियोजना समन्वयक, समग्र शिक्षा, जालौर	1.98000

क्र. सं.	जिले का नाम		आहरण सीमा (राशि लाखों में)
20	झालावाड़	जिला परियोजना समन्वयक, समग्र शिक्षा, झालावाड़	1.64000
21	झुन्झुनूं	जिला परियोजना समन्वयक, समग्र शिक्षा, झुन्झुनूं	2.65000
22	जोधपुर (शहर)	जिला परियोजना समन्वयक, समग्र शिक्षा, जोधपुर	3.58000
23	करौली	जिला परियोजना समन्वयक, समग्र शिक्षा, करौली	1.62000
24	कोटा	जिला परियोजना समन्वयक, समग्र शिक्षा, कोटा	1.60500
25	नागौर	जिला परियोजना समन्वयक, समग्र शिक्षा, नागौर	3.78000
26	पाली	जिला परियोजना समन्वयक, समग्र शिक्षा, पाली	2.50500
27	प्रतापगढ़	जिला परियोजना समन्वयक, समग्र शिक्षा, प्रतापगढ़	1.07000
28	राजसमन्द	जिला परियोजना समन्वयक, समग्र शिक्षा, राजसमन्द	1.50500
29	सवाई माधोपुर	जिला परियोजना समन्वयक, समग्र शिक्षा, सवाई माधोपुर	1.54000
30	सीकर	जिला परियोजना समन्वयक, समग्र शिक्षा, सीकर	3.20000
31	सिरोही	जिला परियोजना समन्वयक, समग्र शिक्षा, सिरोही	1.19500
32	टोंक	जिला परियोजना समन्वयक, समग्र शिक्षा, टोंक	1.69000
33	उदयपुर (शहर)	जिला परियोजना समन्वयक, समग्र शिक्षा, उदयपुर	3.75500
		कुल राशि रू.	**76.80000**

(राशि अक्षरे छियत्तर लाख अस्सी हजार रूपये मात्र)

नोट:उक्त राशि का आहरण संबंधित प्रयोजन के व्यय के लिए राजस्थान लोक उपापन में पारदर्शिता अधिनियम 2012 एवं नियम 2013 तथा तत्संबंधी नियमों/निर्धारित मापदण्डों, योजना के दिशानिर्देशों की पालना करते हुये किया जावें। किसी अन्य प्रयोजनार्थ राशि आहरण किसी भी परिस्थिति में नहीं किया जावेगा।

इस राशि का व्यय वित्तीय वर्ष 2022–23 के प्रावधान के विरूद्ध किया जाना है।

राज्य परियोजना निदेशक,
समग्र शिक्षा,

दिनांक :

क्रमांक :

प्रतिलिपि : निम्नांकित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित है :–

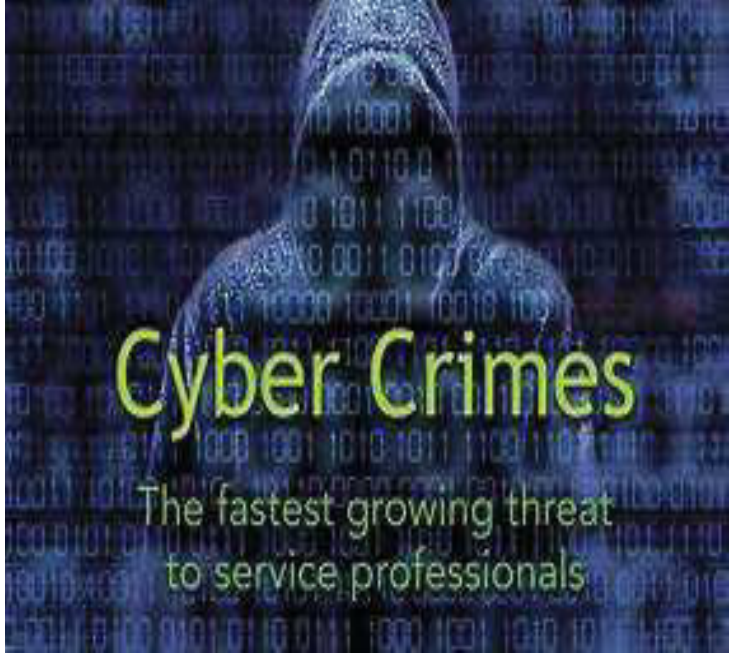
1. निजी सचिव, आयुक्त एवं राज्य परियोजना निदेशक, रा.स्कू.शि.प., जयपुर।
2. कोषाधिकारी, कोष कार्यालय, सचिवालय, जयपुर।
3. कोषाधिकारी, कोष कार्यालय,.....।
4. अति. जिला परियोजना समन्वयक, समग्र शिक्षा, कार्यालय, जिला.....।
5. रक्षित पत्रावली।

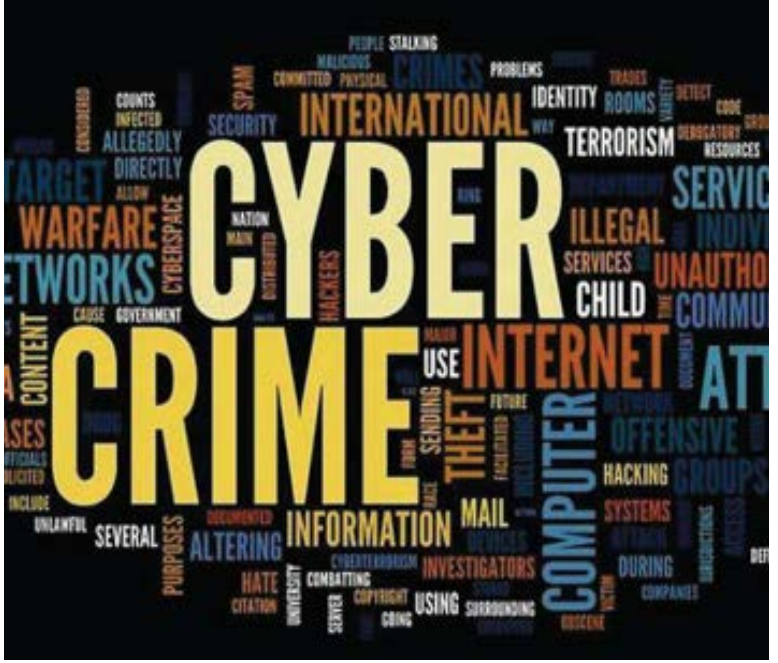
अति. राज्य परियोजना
निदेशक–द्वितीय

एक कदम सजगता की ओर

सायबर अपराध निर्देशिका

सायबर अपराध के प्रकार एवं बचने के उपाय


Cyber Crimes
The fastest growing threat
to service professionals


CYBER
CRIME
INTERNATIONAL
TERRORISM
WARFARE
INTERNET
COMPUTER
THEFT
HACKING
INFORMATION
ALTERING
ILLEGAL
CHILD
SECURITY
SPAM
IDENTITY
CONTENT
SYSTEMS
MAIL
INVESTIGATORS
USING
SEVERAL
PURPOSES
HATE
OFFENSIVE


CYBER
CRIME.

व्हाट्सअप फ्राड


128.199.87.230
Startpage
WhatsApp
Congratulations!! You've been invited to try Whatsapp Calling!
Invite Your 10 Active Whatsapp Friends to Activate Whatsapp Calling
• As soon as you click on "Invite Now", your whatsapp will open and you can send invitation to any of your friends
• You'll have to invite minimum 10 active friends one by one
• You can click on "Continue" after inviting 10 friends to activate voice calling on Whatsapp
Invite Now
Continue


WHATSAPP
ACCOUNT
HACKED?
HACKED
Learning
Ocean


WhatsApp
Your subscription is ending soon
Please update your payment information now
UPDATE YOUR PAYMENT INFORMATION
Our records indicate that your WhatsApp trial service is exceeding the one year period. At the completion of your trial period your WhatsApp will no longer be able to send or receive message. To continue using WhatsApp without interuption, we need you to subscribe for any of our subscription periods.
To avoid service interruption, please subscribe by visiting your account page below.
Sign in to the customer portal with your Number
We appreciate your prompt attention to this matter, and look forward to continuing to meet your communication needs.
Sincerely,
The WhatsApp Team
Account information
Service: WhatsApp Subscription
Helpful resources
Sign in to the service portal.
Have Questions? Visit the Community.

व्हाट्सअप के उपयोग से सावधानी बरतें

- व्हाट्सअप के प्राइवेसी सेटिंग में प्रोफाईल फोटो स्टेटस आदि में " only for contacts" सेव करें।
- व्हाट्सअप में 2 स्टेप वेरीफिकेशन का प्रयोग करें।
- अपने स्वंय के नाम से जारी सिम से व्हाट्सअप का संचालन करें।
- यदि व्हाट्सअप संबंधी किसी भी प्रकार का OTP आता है तो उसे किसी के साथ शेयर ना करें।
- मोबाईल गुम या चोरी हो जाने पर तत्काल व्हाट्सअप deactivate करें
- व्हाट्सअप वेब समय–2 पर चैक करें। कहीं कोई आपका व्हाट्सअप QR कोड स्कैन करके उपयोग तो नहीं कर रहा है।

व्हाट्सअप का उपयोग करते समय निम्न बातों पर विशेष ध्यान रखना चाहिए –

- अनजान नम्बर से आने वाले विडियो/आडियो काल रिसीव न करें।
- अनजान व्हाट्सअप ग्रुप से न जुडें तथा अंजान नम्बर से आने वाले ग्रुप्स इन्विटेशन लिंक को टच ना करें।
- व्हाट्सअप में अपनी निजी/परिवारिक जानकारी शेयर नहीं करें।
- किसी भी विडियो/फोटो/मैसेज/लिंक की पुष्टि के बिना शेयर या वायरल न करें।
- सांम्प्रदायिक तथा आपत्तिजनक विडियो/फोटो/मैसेज/लिंक का प्रचार–प्रसार, पोस्ट न करें। व्हाट्सअप में आने वाले लक्की ड्रा/लाटरी/ईनाम के प्रलोभन वाले मैसेज पर कोई प्रतिक्रिया न देवें।

किसी भी फोटो/विडियो/मैसेज की सत्यता जाने बगैर फारवर्ड न करें।

- प्रत्येक ग्रुप में विभिन्न प्रकार की फोटो विडियो आते–जाते रहते है, उस विडियो/फोटो/मैसेज की सत्यता जांचे बिना किसी अन्य को शेयर या लाईक नहीं करना चाहिए। ऑटो डाउनलोड मोड ऑफ रखें।
- ऐसा विडियो/फोटो/मैसेज जो किसी अन्य व्यक्ति के आर्थिक, सामाजिक, राजनैतिक, स्तर को क्षति या बदनाम कर सकता है, शेयर या फॉरवर्ड न करें।
- यदि आपके द्वारा प्रेषित किसी मैसेज से किसी दूसरे व्यक्ति को क्षति कारित होती है अथवा शांति भंग होती है, ऐसी स्थिति में आप भी आपराधिक कृत्य के भागीदार बन जायेगें।

फेसबुक

फेसबुक उपयोग करते समय इन बातों का ध्यान रखे

- किसी अंजान व्यक्ति ग्रुप से सम्पर्क न बनाये
- पासवर्ड स्ट्रॉग रखें
- समय–समय पर पासवर्ड बदलते रहें।
- मोबाईल नम्बर/नाम/एवं जन्म तिथि को कभी भी पासवर्ड न रखें
- अन्जान व्यक्ति द्वारा भेजे गये लिंक को क्लिक ना करें
- प्रोफाईल फोटो को सेफगार्ड से सुरक्षित रखें
- टू फेक्टर ऑथेंटिकेशन का उपयोग करें
- यात्रा एवं खरीदी बिक्री से संबधित जानकारी शेयर न करें
- हनीट्रेप के मामलों से बचें
- यू.आर.एल का प्रयोग
- अनजान फेसबुक या सोशल मीडिया दोस्त के द्वारा झूठे गिफट को प्राप्त करने के लिए अनजान व्यक्ति के बैंक खाता में पैसा जता कर देना

अन्य सोशल साईट

- इंस्टाग्राम/ट्वीटर/हाईक/हैलो/वी–चैट/यू–ट्यूब
- जैसे सोशल साईट पर पर्सनल/प्राईवेट/कामुक/अश्लील फोटो एवं विडियो न डाले।
- फेसबुक/व्हाट्सअप की तरह ही अन्य सोशल साईट में भी सावधानी बरतनी चाहिए।
- पासवर्ड स्ट्रांग रखना चाहिए।
- अपना पासवर्ड किसी अन्य से शेयर न करें।
- किसी अन्य के मोबाईल/कम्प्यूटर/लैपटाप से सोशल मीडिया का उपयोग करने के बाद लॉग आउट/डिलीट करना सुनिश्चित करें। कोशिश करें कि अन्य के साधन का उपयोग न करना पडे।

गूगल

पिछले कुछ समय से हम लोग गूगल पर ज्यादा विश्वास करने लगे हैं, कुछ भी जानकारी हासिल करनी हो तो हम तुरंत गूगल साईट में जाकर सर्च कर लेते हैं तथा उस जानकारी पर विश्वास भी कर लेते हैं, इसी बात का फायदा अपराधी भी उठाते हैं। साईटों की फर्जी कॉपी कर अपना नंबर डाल देते हैं। जो गूगल सर्च इंजन में दिखता है। उन नम्बरों पर हम सम्पर्क करते हैं तो अपराधी से हमारा सम्पर्क हो जाता है और हम फ्राड के शिकार हो जाते है। अतः गूगल से निकाले गये फोन नम्बरों की जांच कर विश्वस्त होने के बाद ही आगे की कार्यवाही करें, जहां तक हो सके कैश ऑन डिलीवरी से भुगतान करें।

गूगल सर्च करने पर कई तरह की फर्जी कंपनियों के वेबसाईट मिलते हैं, जो सस्ते में सामान बेचने का ऑफर करते हैं। ऐसी कम्पनी सामान की डिलीवरी के पूर्व अग्रिम भुगतान मांगती है जिन्हे कभी भी अग्रिम भुगतान न करें।

कैश रिफण्ड करने की बात कह कर भी अपराधी ठगी करते हैं। उनके द्वारा भेजे गये लिंक पर क्लिक न करें और न ही उनके झांसे में आयें। ऐसे लिंक पर क्लिक करने से आपके मोबाईल में कुछ ऐसे सॉफटवेयर इंस्टॉल हो जाते हैं जिनसे आपके मोबाईल का पूरा डाटा सामने वाले के पास चला जाता है।

मैट्रिमोनियल वेबसाईट/एप

घर बैठे इंटरनेट के माध्यम से वर–वधू की तलाश विकल्प के लिए अनेक वेबसाइट एप्लीकेशन मौजूद है। जिसमें लडका लडकी का सम्पूर्ण विवरण रहता है। जिसके आधार पर लडका लडकी की प्रोफाईल बनाई जाती है। उक्त प्रोफाईल में लडका लडकी को पंजीकृत होने पर एक आई.डी. नंबर दिया जाता है। और उनकी फोटो, रुचि, उम्र, परिवार, शारीरिक बनावट, शिक्षा आदि सम्पूर्ण जानकारी होती है।

मैट्रिमोनियल वेबसाईट/एप (ध्यान रखने वाली बातें)

- बहुत ही सावधानी व सुरक्षा से वांछित साइट का चुनाव करें।
- निजी जानकारी पुष्टि उपरांत ही शेयर करें।
- लडका लडकी का चुनाव करते समय पूर्ण रुप से जांच पडताल करें।
- अच्छे रिश्ते का लालच देकर पंजीयन शुल्क के नाम से वसूली की जा सकती है।
- संबधित स्थान में अपने परिचित रिश्तेदार दोस्तों से जानकारी एकत्र करें।
- किसी भी बहाने से रुपये की मांग होने पर सावधानी बरतें।
- रिश्ते पक्का होने के नाम से अनजान लिंक/क्यू.आर. कोड आदि पर भुगतान न करें।
- धोखाधडी होने पर तत्काल पुलिस को सूचित करें।
- रुपये मांगने वालों से रिश्ता न बनाऐं।
- अति विश्वास में आकर आपत्तिजनक फोटो एंड वीडियो शेयर न करें।
- अलग–अलग मोबाइल नम्बर से फोन आने पर अकाउण्ट को डिलीट करें।
- सोशल मीडिया का उपयोग न करने वाले फर्जी हो सकते है क्योंकि वह अपनी पहचान छिपाते है।
- प्रत्यक्ष रुप से मिलने के उपरांत ही घर परिवार देखकर शादी करें।

ऑनलाईन डेटिंग वेबसाइट/एप

फ्राड के तरीके

- अपराधी विभिन्न सोशल साईट से फोटो तथा उसकी विस्तृत जानकारी प्राप्त कर डेटिंग एप पर फेक प्रोफाईल बनाते है, तथा फेक आई.डी. से फ्रेंड रिक्वेस्ट भेजते है।
- रिक्वेस्ट कन्फर्म होने पर चैटिंग शुरु कर लडके लडकी को फंसाते है।
- अपराधी दोस्ती गहरी होने के बाद, किसी ना किसी बहाने से रुपये मांगते है।
- अपराधी पैसे ज्यादातर फेक नम्बर पर बनाये गये पेटीएम एकाउण्ट में लेते है।
- डेटिंग एप में चैटिंग के दौरान अंतरंग वीडियो, चैट, आपत्तिजनक फोटो स्क्रीन सेवर से रिकार्ड कर सोशल मीडिया में अपलोड करने की धमकी देकर रुपये की मांग करते है।

ध्यान रखने वाली बातें

- जब भी आप ऑनलाईन एप डाउनलोड करे तो अपनी निजी जानकारी तुरंत साझा न करें।
- ऑनलाईन दोस्तों को निजी फोटो शेयर न करें।
- यदि आप डेटिंग एप पर चैटिंग कर रहे है तो भावुकता भरी बातें न करे, आप ठगी के शिकार हो सकते है।
- कुछ दिनों की चैटिंग के बाद रुपये की मांग या उपहार देने का लालच दे, तो सतर्क रहें।
- प्राप्त किसी अनजान लिंक को क्लिक न करें।

ए.टी.एम कार्ड का विवरण

ए.टी.एम. फ्राड / ए.टी.एम. क्लोनिंग

ए.टी.एम. बूथ में होने वाले अपराध

- ए.टी.एम. कार्ड की अदला बदली कर।
- ए.टी.एम. कार्ड रीडर लगाकर।
- ए.टी.एम. कार्ड का उपयोग दूसरे को देने पर।
- ए.टी.एम. बूथ के की–बोर्ड कैंसिल बटन को खराब कर कैंसिल के जगह कंटिन्यू विकल्प से।
- ए.टी.एम. बूथ पर कैमरा लगाकर ए.टी.एम. क्लोनिंग कर।
- स्किमर का उपयोग कर।

ए.टी.एम. बूथ (ए.टी.एम. कार्ड उपयोग करने की सावधानियां)

- ए.टी.एम. बूथ पर ए.टी.एम. कार्ड का उपयोग किसी अन्य व्यक्ति को न करने दें।
- ए.टी.एम. बूथ पर चारों तरफ ध्यान से देखें कि पोर्टेबल कैमरा/स्पाई कैमरा की–बोर्ड के ऊपर जहां से पिनकोड कवर हो रहा है उसे रिकार्ड तो नहीं कर रहा।
- ए.टी.एम. कार्ड डालने वाली जगह को ध्यान से देखें, कोई कार्ड रीडर डिवाइस या चिप तो नहीं लगा है।
- ए.टी.एम. कार्डके उपयोग करने हेतु किसी अन्य को ना भेजें।
- ए.टी.एम. कार्ड का पिन किसी से शेयर ना करें।
- ए.टी.एम. बूथ पर पिन डालते समय हाथ से कवर रखें।
- राशि निकालने के बाद कैसिंल बटन जरुर क्लिक करें।
- ए.टी.एम. से तब तक बाहर न निकले जब तक स्क्रीन का दोबारा होम पेज पर ना आ जाए।
- ए.टी.एम. बूथ पर पहले से कोई व्यक्ति मौजूद है तो पहले उसे पैसे निकालने दे, और यदि आप अंदर है तो कोई और उसी समय अंदर आए तो उसे बाहर भेजें।
- समय–समय पर ए.टी.एम. पिन बदलते रहें।

ए.टी.एम. कार्ड उपयोग करने के तरीके

- संभव हो तो जिस स्थान पर सुरक्षा गार्ड हो उस ए.टी.एम. का उपयोग करें, जरुरत पडने पर गार्ड से सहयोग लें।
- सुनसान स्थान पर बने ए.टी.एम. से कैश निकालने से बचें।
- ए.टी.एम. बूथ में हीं कैश गिनती करें, बाहर नहीं।
- मोबाईल पर ए.टी.एम. कार्ड का पिन सेव न करें।
- अपने बैंक में मोबाईल नम्बर पंजीकृत कराये जिससे लेनदेन के सारे मैसेज प्राप्त हो।
- ए.टी.एम. के पास संदिग्ध लोग दिखे तो पुलिस को सूचित करें।
- ए.टी.एम. मशीन पर पिन डालने के बाद कैश नहीं है का मैसेज ना आए तो तत्काल बैंक को सूचित करें।

फ्रॉड का शिकार होने पर त्वरित किये जाने वाले उपाय

- यदि आप भूलवश सायबर अपराध का शिकार हो जाते है तो–
- सर्वप्रथम डेबिड या क्रेडिट कार्ड को ब्लॉक करें और संबन्धित बैंक एवं नजदीकी पुलिस स्टेशन को सूचित करें।
- मोबाईल पर आपके बैंक से आने वाले मैसेज को इग्नोर ना करें, तत्काल बैंक से सम्पर्क करें।

शिकायत कैसे करें

निम्न जानकारी के साथ नजदीकी पुलिस स्टेशन में जाकर रिपोर्ट दर्ज कराऐं –

- बैंक खाता संख्या/स्टेटमेंट की जानकारी
- ए.टी.एम. कार्ड का विवरण
- आरोपी का मोबाईल नम्बर
- मोबाईल पर आये मैसेज का स्क्रीन शॉट

ए.टी.एम. एवं क्रेडिट कार्ड संबंधित टेलीफ्राड

अपराधी बैंक मैनेजर बन कर फोन करते है, और ए.टी.एम. कार्ड/क्रेडिट कार्ड ब्लॉक होने का झांसा देकर कार्ड का 16 डिजिट का नंबर एवं कार्ड के पीछे अंकित सी.वी.वी. नंबर, कार्ड वैलेडिटी डेट पूछ कर धोखाधडी करते है।

अपराधी निम्न अन्य बहाने बनाकर भी धोखाधडी करते है –

- ए.टी.एम. कार्ड/क्रेडिट कार्ड ब्लॉक होने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड को आधार से लिंक कराने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड की लिमिट बढाने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड के कैशबैक ऑफर के नाम पर।

ऐसा कहकर सायबर अपराधी टेलीफोन के माध्यम से आपके क्रेडिट कार्ड एवं ए.टी.एम. कार्ड तथा बैंक अकाउण्ट की जानकारी प्राप्त कर बैंक अकाउण्ट से राशि डेबिट कर लेते है।

यह सायबर अपराधी निम्नलिखित जानकारी प्राप्त करता है

- डेबिट कार्ड / क्रेडिट कार्ड का 16 अंको का नंबर
- कार्ड की वैलिडिटी डेट
- कार्ड के पीछे सी.वी.वी. नंबर (3 अंको का)
- आपके मोबाईल नम्बर पर आए हुए ओटीपी
- इंटरनेट बैंकिंग का यूजर आई.डी. एवं पासवर्ड
- यू.पी.आई. आई.डी. पासवर्ड की जानकारी।

बचने के उपाय

- बैंक कभी अपने किसी भी ग्राहक से बैंक खाते की जानकारी नहीं मांगता। अतः ऐसे कॉल आने पर प्रतिक्रिया नहीं दे।
- यदि आपके पास ऐसा कॉल आता है तो आप अपने फोन कॉल को कट कर अपने बैंक एवं नजदीकी पुलिस थाने पर संपर्क करें।
- किसी भी वास्तविक कारण के बिना किसी अन्य व्यक्ति को अपनी पहचान व जानकारी न दें।
- इन्टरनेट बैंकिंग इस्तमाल करते समय कृपया अधिकृत बेवसाइट का ही उपयोग करें। (https://) एवं URL के साइड में ताले का चिन्ह वाली साइट पर ही जाए।
- अनजान ईमेल/एस.एम.एस से प्राप्त लिंक पर क्लिक न करें।
- इंटरनेट बैकिंग इस्तेमाल करने के लिए फ्री वाईफाई या पब्लिक इंटरनेट का इस्तेमाल करते समय सावधानी बरतें।

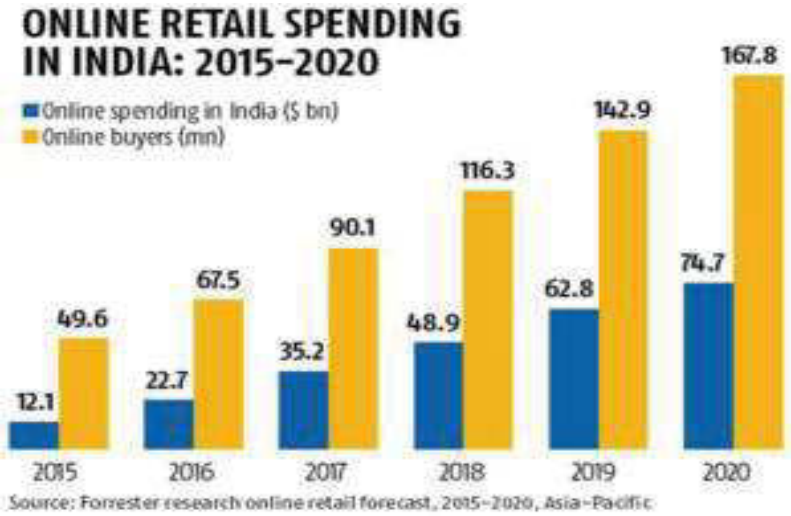
ओ.एल.एक्स/क्विकर फ्राड से बचने के उपाय

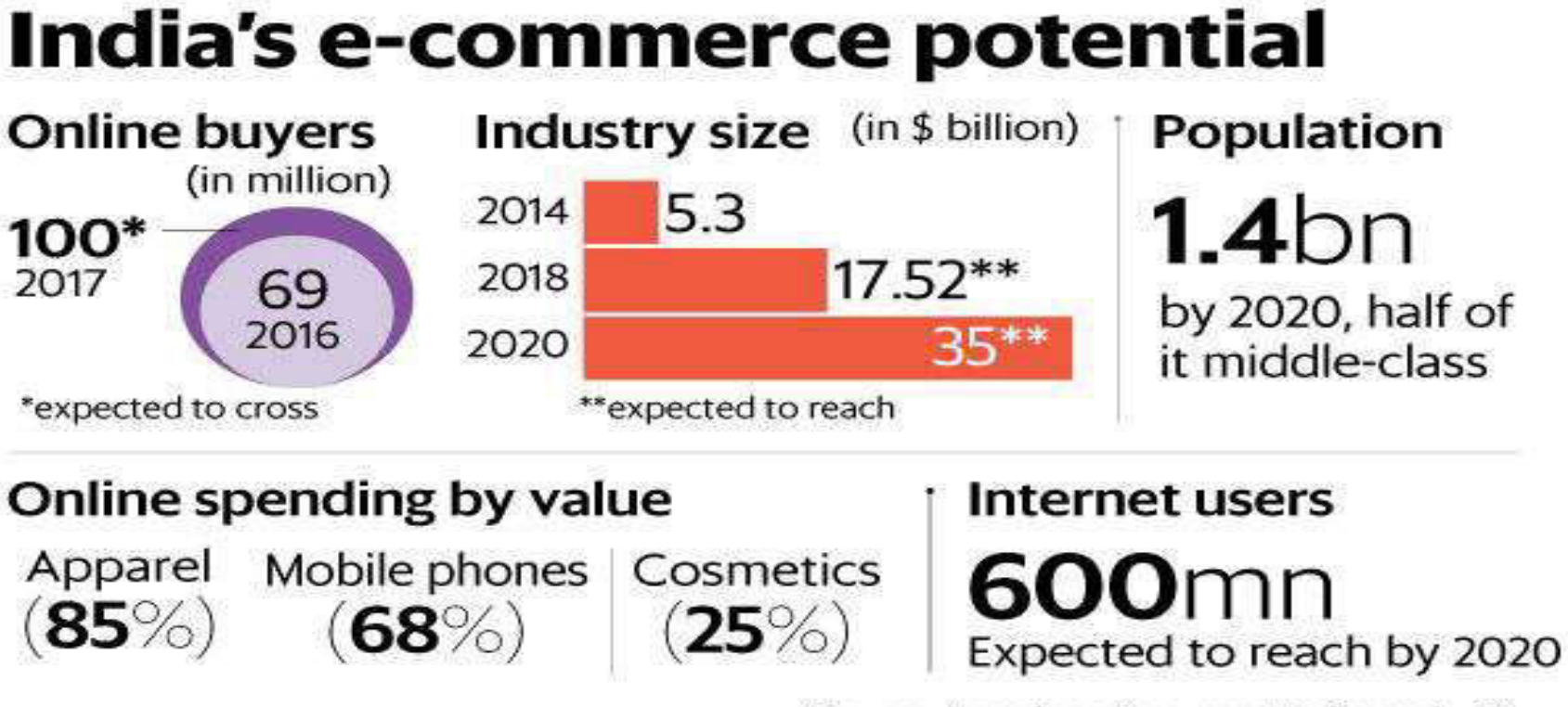
- कोई भी वाहन/मोबाईल/अन्य सामान को खरीदते एवं बेचते समय सावधानी बरते।
- वाहन/मोबाईल/अन्य सामान पसंद आने पर तत्काल भुगतान न करें। एडवांस रकम के नाम पर आपसे धोखाधडी हो सकती है।
- ओ.एल.एक्स/क्विकर आदि पर पुलिस/आर्मी/अर्धसैनिक बल के सुरक्षाकर्मी के पहचान पत्र के नाम पर ठगी की जा रही है तत्काल विश्वास न करें।
- पुलिस/आर्मी/अर्धसैनिक बल के पहचान का भी दुरुपयोग ठग के द्वारा किया जा रहा है। अतः उनके पहचान/नंबर का भी जांच पडताल करने के उपरांत ही खरीदी/बिक्री करें। विडियो कॉल/प्रत्यक्ष रुप से देखकर सामान की खरीद करें।

- ओ.एल.एक्स/क्विकर आदि पर खरीदी/बिक्री हेतु पोस्ट की गई वाहन/मोबाईल/अन्य सामान की केवल फोटो को देखकर सौदा न करें, सामान को जांच परख कर ही लेनदेन करें।
- ओ.एल.एक्स/क्विकर पर वाहन बेचते/खरीदते समय किसी लेन–देन भुगतान हेतु किसी लिंक पर क्लिक, ऑनलाईन पेमेंट न करें। (01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यू.आर. कोड भेजकर आप के साथ ठगी हो सकती है)
- ऑनलाईन सामान खरीदते समय कैश ऑन डिलीवरी विकल्प का ही उपयोग करें।
- कम कीमत, आकर्षक मूल्य के झांसे में ना आयें।

ई–कामर्स साईट


Top 5 E-Commerce Websites in India
MYNTRA.com
India's Largest Online Fashion Store
snapdeal.com
JABONG.COM
amazon.in
flipkart.com


ONLINE RETAIL SPENDING IN INDIA: 2015–2020
Online spending in India ($ bn)
Online buyers (mn)
12.1
49.6
22.7
67.5
35.2
90.1
48.9
116.3
62.8
142.9
74.7
167.8
2015
2016
2017
2018
2019
2020
Source: Forrester research online retail forecast, 2015–2020, Asia–Pacific


India's e-commerce potential
Online buyers
(in million)
100*
2017
69
2016
*expected to cross
Industry size (in $ billion)
2014
5.3
2018
17.52**
2020
35**
**expected to reach
Population
1.4bn
by 2020, half of it middle-class
Online spending by value
Apparel
(85%)
Mobile phones
(68%)
Cosmetics
(25%)
Internet users
600mn
Expected to reach by 2020
Source: Assocham-Resurgent India study, EY

ई–कामर्स साईट

इंटरनेट के माध्यम से व्यापार का संचालन, खरीदी बिक्री हेतु ग्राहकों के लिए सेवाएं उपलब्ध कराना ही ई–कामर्स है।

ई–कामर्स साईट में अपराध के तरीके

- अपराधी ऑनलाईन खरीदी/बिक्री या सेवा देने वाली विभिन्न कंपनी के साईट्स को कॉपी कर फर्जी साईट बनाकर फर्जी नंबर डिस्पले करते है। लोग इन फर्जी साईट पर जाकर ऑनलाईन सामान आर्डर कर पैसे का अग्रिम भुगतान करते हैं और ठगी का शिकार हो जाते है। सही साईट्स का चयन करे तथा फर्जी साईट्स से बचे।
- अपराधी कहते है कि आप हमारे लक्की कस्टमर है आपका मोबाईल नंबर लक्की ड्रा में निकला है, आपने कार/कोई मंहगी वस्तु/नगद राशि जीती है कहकर धोखाधडी करते है।
- ऑनलाईन पेमेंट न करें। (01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यू.आर. कोड भेजकर आप के साथ ठगी हो सकती है)

ई–कामर्स साईट में अपराध के तरीके

- लक्की ड्रा से जीती हुई कार/मोटर साईकिल/अन्य सामान के रजिस्ट्रेशन/ट्रांसपोर्टेशन/इंश्योरेंस/सर्विस शुल्क/जी.एस.टी. आदि का झांसा देकर फर्जी खाते में पैसा जमा करा लेते है।
- अपराधी नगद राशि भेजने के नाम पर बैंक/ए.टी.एम. संबन्धित सभी प्रकार की जानकारी एवं ओ.टी.पी. प्राप्त कर खाता से पैसे आहरण कर लेते है।
- किसी प्रकार के ईनाम/लक्की ड्रा/प्रलोभन/आकर्षक स्कीमके झांसे में न आवें।
- ई कामर्स साईट पर वाहन/अन्य सामान क्रय विक्रय करते समय किसी रकम का भुगतान हेतु किसी लिंक पर क्लिक, आनलाईन पेमेंट न करें।(01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यू.आर. कोड भेजकर आप के साथ ठगी हो सकती है)

ऑनलाईन शोपिंग फ्राड

ऑनलाईन शोपिंग करते समय निम्न सावधानियां बरतने की जरुरत है

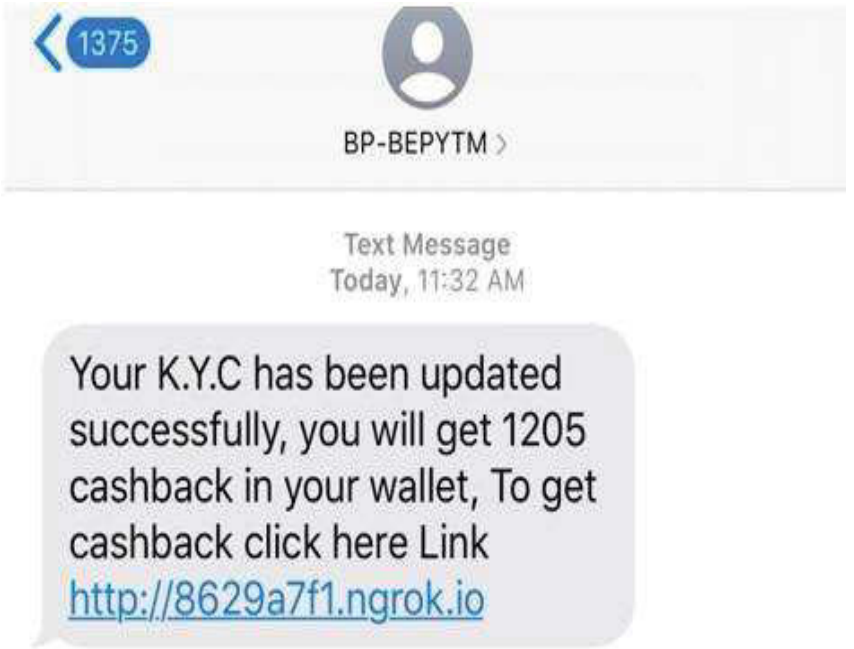
- अनजान व्यक्ति /अनजान वेबसाइट पर अपने बैंक एकाउण्ट डेबिट/क्रेडिट कार्ड से संबन्धित जानकारी साझा न करें।
- कम्प्यूटर या मोबाईल पर आपरेटिंग सिस्टम/एंटी वायरस को समय–समय पर अपडेट करते रहें।
- किसी ऑनलाइन पोर्टल में खरीददारी करने से पहले यह सुनिश्चित कर लें कि सही वेबसाइट/एप का उपयोग कर रहे हैं।
- https & http – जिस वेबसाइट से सामान खरीद रहे है, उसके एड्रेस (यू.आर.एल) में https होना चाहिए, ना कि http क्योंकि s का मतलब सिक्यूरिटी की गारंटी से है।
- ऐसे वेबासाईट या एप से खरीददारी करें जिसमें ऑफिस का पता ई मेल व हेल्प लाईन का नंबर सही व स्पष्ट हो।

ऑनलाईन शोपिंग करते समय निम्न सावधानियां बरतने की जरुरत है

- गलत वेबसाईट लालच/आकर्षक/लुभावने आफर करते हैं और हमारी जानकारी चुराने का माध्यम बन जाते है।
- ऑनलाईन शापिंग करने के बाद निश्चित हो जाना महंगा पड सकता है। बैंक स्टेटमेंट का समय समय पर जांच करते रहना चाहिए।
- ऑनलाईन शापिंग के कुछ समय/दिन बाद यदि उसकी शापिंग का हवाला देकर यदि कोई अनजान फोन कर्ता लुभावनी बात करता है तो उसके झांसे में न आयें।
- सामान प्राप्त करने के बाद उसे डिलीवरी बॉय के सामने ही चेक करें गडबडी होने पर डिलीवरी बॉय के साथ/सामने ही फोटो खींच लें।
- केश ऑन डिलीवरी पेमेंट मोड का इस्तेमाल करें।

लिंक फ्राड

सायबर अपराधी के द्वारा विभिन्न एप एवं टूल्स से तैयार लिंक लोगों के पास भेजे जाते है उसे क्लिक कर देने से हमारे मोबाईल में उपलब्ध बैंक संबंधी गोपनीय जानकारी जैसे ओ.टी.पी., पिन नम्बर आदि अपराधी के पास चले जाते है। अतः ऐसे अवांछित लिंक को क्लिक करने से बचना चाहिए।



लिंक फ्राड कैसे होता है

- ठग फोन से बात कर झांसा देकर लिंक भेजते है जिस पर हम लिंक क्लिक कर प्रतिक्रिया देते है।
- मेल/पोस्ट/मैसेज के माध्यम से लिंक भेजकर।
- 01 रु या 10 रु के भुगतान व सत्यापन/पंजीयन के बहाने।
- आकर्षक ईनाम/लाटरी/ लक्की ड्रा के नाम से लिंक भेज कर।
- सोशल मीडिया से लिंक भेजकर।

बचने के उपाय

- अनजान कोई भी लिंक को क्लिक न करें।
- मोबाईल पर आकर्षक ईनाम/लाटरी/लकी ड्रा के नाम पर भेजे गये लिंक को क्लिक न करें।
- सोशल मीडिया से भेजे गये अंजान लिंक पर क्लिक न करें।
- कभी भी आपको कोई ऐसा लिंक दिखे जो आपको अमीर बनाने का वादा करता हो, उस लिंक को क्लिक न करें।
- पेंशन/ईश्योरेंस/मैच्युरिटी के नाम पर भेजे

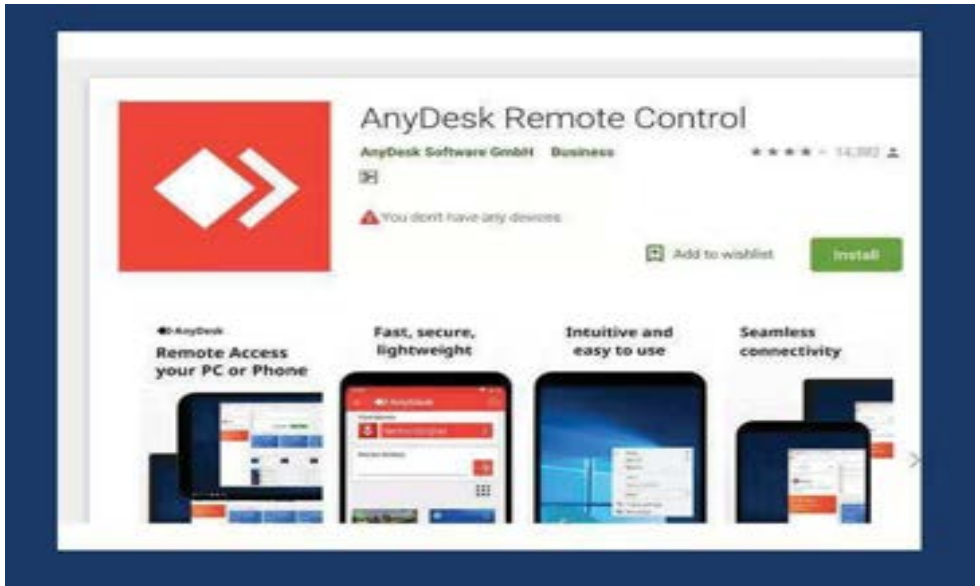
लिंक फ्राड

ध्यान मे रखने योग्य बातें :–

- फोन पर बैंक/एटीएम/ओटीपी की जानकारी न देवे।
- रजिस्ट्रेशन/सर्विस/एडवांस/कमीशन के नाम पर कोई भुगतान न करे।
- लोन के नाम से आये अनजान मेल/मैसेज/काल पर कोई प्रतिक्रिया न दें।
- लोन के नाम से 1 रुपये/10 रुपये का भुगतान, अनजान लिंक पर क्लिक न करें।
- लोन के नाम से अनजान व्यक्ति को अपनी व्यक्तिगत जानकारी एवं दस्तावेज न दें।
- कोशिश करें कि बैंक जाकर ही लोन के लिये आवेदन करे और दस्तावेज दें।

अवांछित एप डाउनलोड करना

साइबर क्रिमिनल द्वारा लोगो को झांसा देकर रिमोट एप्लीकेशन जैस टीम विवर, एनी–डेस्क, एयरड्रायड, क्रोम रिमोट डेस्कटॉप जैसे एप्लीकेशन डाउनलोड करा देते है जो हमारे मोबाईल को रिमोट के माध्यम से आरोपी अपने मोबाईल मे पैरेलल (सीधे) देख सकते है और इसी एप्लीकेशन के जरिये हमारे ओ.टी.पी. पिन नंबर एवं अन्य बैंक संबंधी गोपनीय जानकारी प्राप्त कर धोखाधडी करते है, अतः अनजान एप्लीकेश को अपने मोबाईल मे बिल्कुल भी डाउनलोड/इंस्टाल न करे।



लोन फ्राड

लोन देने के बहाने भी बहुत सारे क्रिमिनल हमें फोन कर तरह–तरह की लुभावने स्कीम का झांसा देकर पहले डाक्यूमेंटेंशन फीस के रुप मे 2000–3000 रु0 जमा करवाते है, हम अत्यधिक रकम नही होने से आसानी से उनके बताये खाते मे रकम जमा करा देते है, धीरे –धीरे आरोपी रकम बढाते जाते है और एक बडा रकम जमा करा कर हमसे धोधाखडी करते है। ऐसे कॉल एवं लोन देने वाले लोगो से हमें बचना चाहिए तथा लोन देने के लिए बने हुए वैध संस्थानों से ही लोन लेना चाहिए, अन्य के झांसे मे नही आना चाहिए।

लॉटरी फ्राड

आये दिन हमारे मोबाईल फोन पर लाटरी लगने, कैश बैक मिलने या अन्य आफर संबधी मैसेज आते रहते है जो सायबर अपराधियों द्वारा फैलाया गया जाल होता है। यदि हम इनके झांसे में आ जाते है तो वे लाटरी लगने का लालच देकर डाक्यूमेंटेशन चार्ज, जी.एस.टी. चार्ज, ट्रांसपोर्टेशन चार्ज रजिस्ट्रेशन के नाम से काफी बडी रकम अपने खाते में जमा करवा लेते है या धोखे से हमसे ओटीपी या पिन प्राप्त कर हमारे बैंक खातों में जमा राशि निकाल सकते है।

लॉटरी फ्राड

धोखाधडी का तरीका एवं बचाव संबंधी उपाय

- सायबर अपराधी इंडियन गवर्मेन्ट/डिजीटल भारत/प्रधानमंत्री/मुख्यमंत्री की फोटो का उपयोग कर भी ठगी करते है किसी भी लालच में आकर अनजान खाते में पैसा जमा न करें।
- व्हाट्सअप पर लोगों के पास अंजान नंबरों से काल आता है तथा व्हाट्सअप की तरफ से आपकी लॉटरी लगी है कहते हुए जीती हुई रकम प्राप्त करने के लिए मुबंई अथवा दिल्ली के किसी अन्य का नंबर देकर उसे मैनेजर बताते है और वह प्रोसेसिंग फीस (के.वाई.सी) अपडेट आदि नाम से भिन्न भिन्न फर्जी खातों में पैसा जमा कराते है। इससे बचे।
- कौन बनेगा करोडपति के नाम से कॉल या मैसेज कर/हिस्सा लेने के नाम से बैंक खातों में पैसा जमा कराते है ऐसे ठग अपराधियों के झांसे में न आयें।
- लॉटरी/गिफट या किसी अन्य चीज के लिए एकाउण्ट वेरिफिकेशन के नाम पर ओटीपी शेयर न करें।
- अनजान सोर्स से आये लुभावने स्कीम के यू.आर.एल. लिंक पर क्लिक न करें।

बीमा / पेंशन / ई.एम.आई फ्राड

साइबर अपराधियों द्वारा हमारे इंश्योरेंश / पेंशन / ई.एम.आई. / मोबाईल नंबर से संबन्धित जानकारी प्राप्त लोगों को फोन कर पर्सनल डिटेल जैसे पॉलिसी नंबर, नाम, बीमा की रकम, मैच्युरिटी दिनांक आदि बताते है, जिससे हम उनकी बातों में आकर कमीशन बचाने, अधिक लाभ प्राप्त करने के लालच में आकर तथा पॉलिसी लैप्स होने से बचाने के लिए आरोपियों के बताए अनुसार आरोपी के खाते में पैसा जमा कर देते है और ठगी के शिकार हो जाते है।

यदि अनजान काल आये तो आप सबसे पहले अपने नजदीकी बीमा कंपनी जाकर मिले तथा फोन काल के सम्बन्ध में जानकारी देवें। पुलिस एवं सायबर सैल से अविलंब सम्पर्क करें।

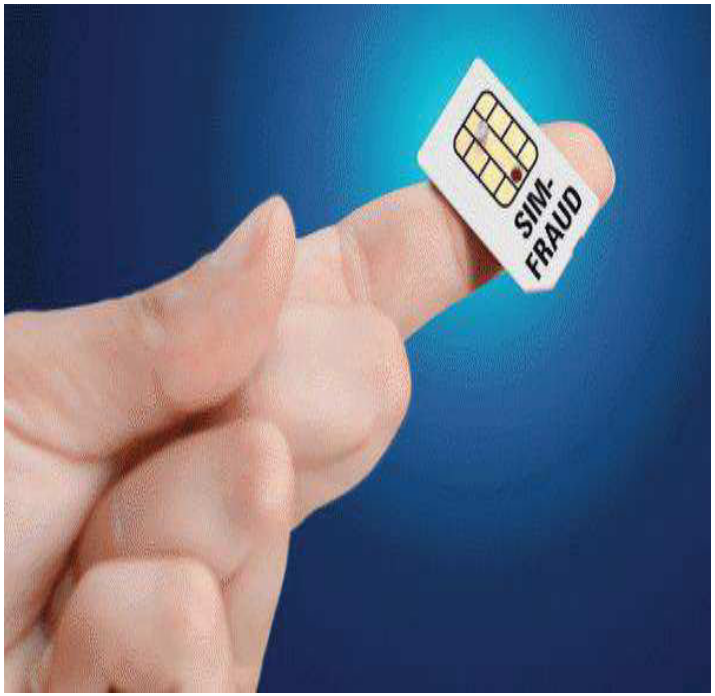
टॉवर फ्राड

- मकान/जमीन पर टॉवर लगाने तथा बहुत अधिक रकम किराये के रुप में देने का लालच देकर क्रिमिनल धोखाधडी करते है।
- फोन या अखबार में यदि इस प्रकार से टॉवर लगाने संबंधी फोन कॉल आये या विज्ञापन दिखे तो अच्छी तरह से इसकी सत्यता की जांच संबंधित फोन कम्पनी/पुलिस/सायबर सैल से करा कर ही पैसा खर्च करें अन्यथा फ्राड का शिकार हो सकते है।

- मोबाईल कम्पनी को यदि टावर लगाना होता है तो आवश्यकतानुसार क्षेत्र का भ्रमण/सर्वे कर स्वंय जमीन/प्लाट/मकान की खोज करते है। किसी भी खाली जमीन/प्लाट/मकान पर कंपनी टावर नहीं लगाती है।
- कोई भी कंपनी टॉवर लगाने से पहले किसी भी प्रकार के रकम की मांग नहीं करती है । अतः किसी के घोखे में न आयें।
- टावर के नाम से एडवांस/कमीशन के नाम पर भुगतान न करें।

सिम स्वैपिंग/सिम फ्राड

आपके द्वारा उपयोग की जा रही सिम (मोबाइल नम्बर) जिस भी कंपनी का है उसे बंद करवा कर अपराधी अपने पास रखें खाली/ब्लैंक सिम में परिवर्तित चालू कर आपके नंबर का गलत उपयोग करने लगते है।




1. The fraudster steals the bank customer's credentials and mobile number
2. The fraudster manipulates the mobile operator to perform a SIM swap on the customer's mobile number
3. The fraudster uses the customer's credentials to initiate a login to their online banking account
4. The bank sends an SMS OTP to the customer's mobile number
5. The OTP arrives on the fraudster's mobile device and is used to access the customer's account
SIM-SWAP FRAUD
BANK

कैसे होता है सिम स्वैपिंग

- अपराधी फर्जी नंबर से नेटवर्क सुधारने/इंटरनेट की स्पीड बडाने के लिए कॉल करते है । 3जी से 4जी या 5जी अपडेट करने तथा लाटरी/ईनाम आदि का बहाना बनाकर सिम के पीछे प्रिंट 20 अंको के आईसीसीआईडी कोड पूछ लेते है।
- सिम के पीछे सिम नम्बर 20 अंको का बताते ही अपराधी हमे 01 प्रेस करने को कहता है। 01 प्रेस करना हमारी सिम स्वैपिंग की स्वीकृति होती है।
- 20 अंको को बताने के बाद 01 ओटीपी मैसेज के रुप में आता है, जिसे बताते ही सिम स्वैपिंग हो जाता है।

बचने के उपाय

- किसी भी व्यक्ति को सिम के पीछे लिखे 20 अंको का नंबर नहीं बताना चाहिए।
- अगर आपका सिम कुछ घंटों के लिए अचानक बंद हो जाता है तो तुरंत अपने ऑपरेटर से संपर्क करें।
- जिस सिम (मोबाईल नम्बर) से आपका बैंक खाता लिंक है उसे सोशल मीडिया पर डिस्पले न करें।
- ओ.टी.पी. अन्जान व्यक्ति को कभी ना बताऐं।

जॉब फ्राड

वर्तमान समय में लोग घर बैठे ही नौकरी हेतु आवेदन कर रहे है, समाचार पत्र के विज्ञापन, मैसेज, मेल व कॉल पर प्रतिक्रिया दे कर व पैसे देकर धौखाधडी के शिकार बन जाते है।

जॉब फ्राड के तरीके

- लुभावनी/अधिक/आकर्षक सैलरी का प्रलोभन।
- अनजान ई–मेल/मैसेज/कॉल द्वारा।
- फर्जी कंपनी के नाम से फर्जी कॉल सेंटर द्वारा कॉल कर।
- फर्जी वेबसाइट द्वारा।
- जॉब के आवेदन व जॉब में लगने के लिए रुपये की मांग करना।
- अधिकतर जॉब ऑफर से सम्बन्धित फर्जी मेल उन कंपनी के नाम से आते है जिनके बारे में आप काफी अच्छे से जानते है।
- नौकरी के नाम से आवेदन/पंजीयन शुल्क एडवांस भुगतान के नाम पर।
- जॉब रिप्लेशमेंट/काल सेंटर के द्वारा वांछित कंपनी की जानकारी देने के एवज में ठगी।
- एडवांस ट्रेनिंग शुल्क के नाम से ठगी।

जॉब फ्राड पर ध्यान रखने योग्य बातें

- अधिकृत वेबसाइट/विभाग का ही चयन करें।
- नौकरी के संबंध में पूर्ण जांच पड़ताल करें।
- विज्ञापन पर जॉब के नाम से अपनी निजी जानकारी/दस्तावेज शेयर करते समय सावधानी बरतें।
- फर्जी सरकारी नौकरी के ऑफर को पहचानें।
- नौकरी से संबंधित अनचाहे ई–मेल पर कोई जवाब न दें।
- वेबसाइट पर दिखने वाले नौकरी से संबन्धित विज्ञापनों से बचें।
- असली और नकली वेबसाइट की पहचान करना सीखें।
- ऑनलाइन इंटरव्यू पर सावधानी बरतें।
- जॉब पोर्टल यानी नौकरी खोजने वाली वेबसाइट में पंजीकरण से पहले प्राइवेसी पॉलिसी अवश्य देखें।
- नौकरी के सम्बन्ध में अपने माता पिता या संरक्षक को अवश्य बतायें।
- यदि कोई वेबसाइट नौकरी दिलवाने का दावा करती है तो उस दावे से संबंधित खोजबीन अवश्य करें।
- यदि कोई व्यक्ति किसी कंपनी में जॉब दिलवाने का दावा करता है तो उस कंपनी में पूछताछ करें व उससे उसके उस कंपनी में होने का साक्ष्य मागें।
- समाचार पत्रों/गूगल डिस्प्ले पर आये विज्ञापन व प्राप्त मैसेज/मेल/कॉल पर रकम का भुगतान न करें।

फ्राड के तरीके	बचने के उपाय
➢ ऐसे साईट में संपर्क करने पर पूरी डिटेल्स जैसे आधार कार्ड, फोन नम्बर, बैंक डिटेल्स, फोटो आदि ले लिया जाता है। ➢ हस्ताक्षर लेकर धोखे से एग्रीमेंट पर साइन करा लेते है। ➢ 7 दिन में काम पूरा करने के लिए बोला जाता है। ➢ बात ऐसे किया जाता है कि आप इस वर्ग को 7 दिन में पूरा करके दिखाओ उसके बाद आप को परमानेंट हमारे कंपनी में जॉब दिया जायेगा। ➢ यदि आप काम छोडते है तो जालसाज द्वारा आप को फोन पर धमकी देते है आपके ई–मेल पर एग्रीमेंट के नाम पर कोर्ट का फर्जी नोटिस भेजते है।	➢ विश्वासपात्र साइट पर ही विजिट करें। ➢ कोई भी फ्रीलांसर जॉब साइट एग्रीमेंट के नाम पर पैसा नहीं मांगता। ➢ आपके ई–मेल पर आए फर्जी कोर्ट के नोटिस से न डरें। ➢ ऐसे जालसाजी के शिकार होने पर अपने नजदीकी पुलिस स्टेशन जाकर शिकायत करें।

फर्जी सरकारी नौकरी के ऑफर को पहचाने

- जाली व नकली वेबसाईट की पहचान करने का तरीका उनकी वेबसाईट की स्पेलिंग में अंतर होना, गलत लिखी होना आदि।
- सरकारी विभाग से सम्बन्धित उनकी अधिकृत वेबसाईट में .gov.in और सरकारी विभाग से सम्बन्धित नौकरी के विज्ञापन समाचार पत्र में या रोजगार समाचार पत्र में प्रकाशित होते है।