इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सी डैक
CDAC

साइबर सुरक्षा जागरूकता

CYBER SAFETY & SECURITY

Supported by

certin
Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

my GOV
मेरी सरकार

CYBER DOST

I4C Indian Cyber Crime Coordination Centre
सहयोग करवाहे • Working Together With Vigour

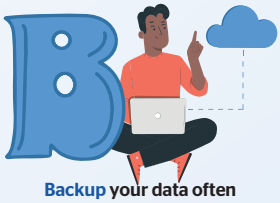
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

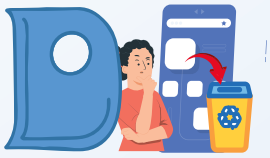
ABCs of Information Security

Antivirus should always be enabled with auto updates



Backup your data often

Clear cookies at the end of the online session



Diagnose for unwanted apps in your mobile device

Encrypt your Data

Firewalls protects your computer from unwanted traffic. Turn it On

Game Addiction is a kind of disorder. Protect your child from such disorders

HTTPS protects your credentials sniffing

Use Bluetooth in **Invisible** mode unless its required to connect with known device

Avoid **Jailbreaking** your mobile OS to protect it from possible threats

Keyloggers are used to steal sensitive information. Be Aware

Logout after you finish accessing your email account

Multi-Factor Authentication will add additional layer of security

Secure **Network Access Point** by enabling firewall and VPN

Optimize security settings of your social media account regularly

Passphrase is the best way to ensure strong password

Quarantine all unused apps

Respect the privacy of others

Search engine safety settings should be turned on Kids **Safe browsing**

Keep **Track** of Your Digital Footprint

Unknown sender emails are not to open or click

Prefer **Virtual Private Network** VPN while using public Wi-Fi

Watch out for online scams

eXamine the app permissions in your device regularly

Use **Yubikey** for enabling multi factor authentication

Not all mistakes can be undone with **ctrl Z** . Be Proactive to secure your information

Supported by

certin Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

my GOV मेरी सरकार

Indian Cyber Crime Coordination Centre

सी डैक CDAC

अभिस्वीकृति

एचआरडी विभाग
इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार

Acknowledgement

HRD Division
Ministry of Electronics and Information Technology
Government of India

आई.एस.ई.ए (ISEA) के बारे में

सूचना सुरक्षा के बढ़ते महत्व को एक महत्वपूर्ण क्षेत्र के रूप में पहचानते हुए, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) ने सूचना सुरक्षा शिक्षा और जागरूकता (ISEA) परियोजना तैयार की और भारत सरकार द्वारा इसे प्रारंभ /लॉन्च किया गया। इस कार्यक्रम के तहत एक गतिविधि यह है कि बच्चों, शिक्षकों, घरेलू उपयोगकर्ताओं, आईटी और गैर-आईटी पेशेवरों के बीच सूचना सुरक्षा जागरूकता फैलाना है, जो देश भर में हो रहा है।

भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) द्वारा इस परियोजना के कार्यान्वयन की जिम्मेदारी C-DAC हैदराबाद को सौंपी गई है। इस गतिविधि के अंतर्गत, C-DAC, हैदराबाद सूचना सुरक्षा जागरूकता सामग्री तैयार कर रहा है, भागीदार संस्थानों (पीआई) के साथ समन्वय कर रहा है, और विभिन्न सूचना सुरक्षा जागरूकता कार्यक्रमों का आयोजन कर रहा है।

दृष्टि :
भारतीय नागरिकों में सूचना सुरक्षा के लिए जागरूकता पैदा करना ताकि वे डिजिटल क्षेत्र में सुरक्षित रूप से भाग ले सकें।

सीडैक के बारे में

C-DAC ने वर्ष १९९९(1999) में हैदराबाद केंद्र की स्थापना की ताकि नवीनतम हार्डवेयर और सॉफ्टवेयर प्रौद्योगिकियों को अपनाते हुए अनुसंधान, विकास और प्रशिक्षण गतिविधियों में काम किया जा सके। यह केंद्र ज्ञान निर्माण, ज्ञान प्रसार और ज्ञान अनुप्रयोग के घटकों के साथ एक ज्ञान केंद्र है, जो अनुसंधान और विकास, प्रशिक्षण और व्यवसाय के क्षेत्रों में वृद्धि के लिए है। केंद्र के अनुसंधान और विकास के क्षेत्र हैं ई-सुरक्षा, एम्बेडेड सिस्टम, सर्वव्यापी कंप्यूटिंग, ई-लर्निंग और ग्रामीण विकास के लिए सूचना और संचार प्रौद्योगिकी(आई. सी. टी/ICT)। केंद्र ने समय के साथ कई उत्पाद और समाधान विकसित किए हैं और कई अत्याधुनिक तकनीकों में प्रयोगशालाएँ स्थापित की हैं। इन अनुसंधान और विकास की ताकतों के अनुसार, केंद्र स्नातकोत्तर स्तर के डिप्लोमा पाठ्यक्रम भी प्रदान करता है। केंद्र शिक्षकों के प्रशिक्षण कार्यक्रमों के आयोजन में भी सक्रिय रूप से संलग्न है। केंद्र नियमित रूप से कौशल आधारित प्रशिक्षण और सूचना सुरक्षा जागरूकता कार्यक्रम (आई.एस.ई.ए /ISEA)) आयोजित करता है।

About ISEA

The Ministry of Electronics & Information Technology (MeitY) has identified the growing importance of Information Security as a critical area, and in view of the same Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this program is to spread Information Security Awareness among children, teachers, home users, IT, and non-IT professionals throughout the country.

C-DAC Hyderabad has been assigned the responsibility of executing this project by the Ministry of Electronics & Information Technology (MeitY), Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events, etc.

Vision :
Generate Information Security Awareness among Indian citizens to enable them to participate safely in the digital space.

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development, and Training activities embracing the latest Hardware & Software Technologies. The center is a knowledge center with the components of Knowledge Creation, Knowledge Dissemination, and Knowledge Application to grow in the areas of Research & Development, Training, and Business respectively. The R & D areas of the center are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning, and ICT for Rural Development. The center has developed a number of products and solutions and has established a number of labs in cutting-edge technologies over a period of time. In line with these R & D strengths, the center also offers Post Graduate level diploma courses. The Centre is also actively involved in organizing faculty training programs. The center regularly conducts skill-based training and information security awareness programs (ISEA).

www.isea.gov.in

साइबर सुरक्षा आज के डिजिटल सिस्टम्स में कमजोरियों का फायदा उठाने वाले धोखेबाजों के कारण एक महत्वपूर्ण चिंता का विषय बन गई है। चूंकि संगठनों और व्यक्तियों की डिजिटल उपकरणों पर निर्भरता बढ़ती जा रही है, इन उभरते हुए खतरों और धोखाधड़ी को समझना और उन्हें कम करना डेटा, गोपनीयता और समग्र डिजिटल अखंडता की सुरक्षा के लिए आवश्यक है। यह पुस्तिका विभिन्न उभरते साइबर धोखाधड़ी को कवर करने का प्रयास करती है और डिजिटल युग में सुरक्षा बढ़ाने के लिए कदमों का वर्णन करती है।

Cybersecurity has become a critical concern as fraudsters exploit vulnerabilities in today's digital systems. As organizations and individuals rely heavily on digital tools, understanding and mitigating these emerging threats and frauds is essential to safeguard data, privacy, and overall digital integrity. The booklet attempts to cover various emerging cyber frauds and outlines steps to enhance security in the digital age.

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सूची | INDEX

CYBER HYGIENE PRACTICES

अपना सॉफ़्टवेयर अपडेट करें
UPDATE YOUR SOFTWARE

सॉफ्टवेयर अपडेट करने के पांच कारण
Five reasons to update software

1. पैच सुरक्षा खामियां
   Patch security flaws
2. नई सुविधाएँ प्राप्त करें
   Get new features
3. डेटा सुरक्षित रखें
   Protect data
4. प्रदर्शन में सुधार
   Improve performance
5. संगतता सुनिश्चित करें
   Ensure compatibility

Save your data with care backup to ensure it's always there

अपने डेटा को सावधानी से सहेजें, बैक अप लें ताकि वो हमेशा सुरक्षित रहै

पासवर्ड सुरक्षा

पासवर्ड अक्षरों की एक ऐसी श्रृंखला है जो उपयोगकर्ता को अपनी पहचान की पुष्टि करने और किसी सिस्टम या सेवा तक पहुंच हासिल करने के लिए प्रदान करना होता है। पासवर्ड्स सत्यापन की एक सामान्य विधि है, जिनका इस्तेमाल किसी उपयोगकर्ता की पहचान की पुष्टि करने के लिए किया जाता है।

पासवर्ड्स का उपयोग आमतौर पर अकाउंट्स, फ़ाइल्स और अन्य संवेदनशील जानकारी को सुरक्षित रखने के लिए किया जाता है। मजबूत और विशिष्ट पासवर्ड्स का उपयोग करना बेहद महत्वपूर्ण होता है, और अनेक अकाउंट्स के लिए एक ही पासवर्ड रखने से बचना भी महत्वपूर्ण है।

PASSWORD SECURITY

A password is typically a string of characters that a user must provide in order to confirm their identity and gain access to a system or service. Passwords are a common method of authentication, which are used to verify the identity of a user.

Passwords are commonly used to protect accounts, files, and other sensitive information. It is important to use strong and unique passwords, and to avoid reusing the same password across multiple accounts.

बहु -कारक प्रमाणीकरण (2FA) क्या है?
What is Two-factor authentication (2FA)?

बहु -कारक प्रमाणीकरण (2FA) उपयोगकर्ता की पहचान की पुष्टि करने की एक विधि है, जिसके लिए उन्हें दो अलग-अलग प्रकार के साक्ष्य प्रस्तुत करने की आवश्यकता होती है, आमतौर पर कुछ ऐसा जो वे जानते हैं (जैसे पासवर्ड) और कुछ ऐसा जो उनके पास है (जैसे पाठ संदेश के माध्यम से भेजे गए कोड वाला फोन)।

मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) उपयोगकर्ता की पहचान की पुष्टि करने की एक विधि है, जिसके लिए उन्हें कई प्रकार के साक्ष्य प्रस्तुत करने की आवश्यकता होती है। आमतौर पर, एमएफए को कम से कम तीन प्रकार के साक्ष्य की आवश्यकता होती है, जिन्हें श्रेणियों में बांटा जाता है जैसे कि उपयोगकर्ता कुछ जानता है (जैसे पासवर्ड), उपयोगकर्ता के पास कुछ है (जैसे मोबाइल फोन), और उपयोगकर्ता की अपनी पहचान (जैसे फिंगरप्रिंट या चेहरे की पहचान)।

Two-factor authentication (2FA) is a method of confirming a user's identity by requiring them to present two different forms of evidence, typically something they know (such as a password) and something they have (such as a phone with a code sent via text message).

Multi-factor authentication (MFA) is a method of confirming a user's identity by requiring them to present multiple forms of evidence. Typically, MFA requires at least three forms of evidence, which are grouped into categories such as something the user knows (e.g. password), something the user has (e.g. mobile phone), and something the user is (e.g. fingerprint or facial recognition).

एक मजबूत पासवर्ड सेट करने के लिए सर्वोत्तम अभ्यास
Best practices for setting a strong password

अद्वितीय, जटिल और लंबे पासवर्ड का उपयोग करें: एक मजबूत पासवर्ड कम से कम 12 वर्णों का होना चाहिए और इसमें अपरकेस और लोअरकेस अक्षरों, संख्याओं और विशेष वर्णों का मिश्रण शामिल होना चाहिए। अपने नाम, जन्मतिथि या सामान्य शब्दों जैसी आसानी से अनुमान लगाने वाली जानकारी का उपयोग करने से बचें।

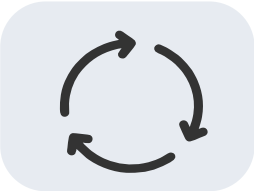
Use unique, complex, and long passwords:
A strong password should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information such as your name, birthdate, or common words.

पासवर्ड मैनेजर का उपयोग करें:
पासवर्ड प्रबंधक आपके लिए जटिल, अद्वितीय पासवर्ड बना और स्टोर कर सकता है। यह आपको अपने पासवर्ड का ट्रैक रखने और स्वचालित रूप से आपके खातों में लॉग इन करने में भी मदद कर सकता है।

Use a password manager:
A password manager can generate and store complex, unique passwords for you. It can also help you keep track of your passwords and automatically log you into your accounts.

दो-कारक प्रमाणीकरण (2FA) सक्षम करें:
दो-कारक प्रमाणीकरण आपके पासवर्ड के अलावा दूसरे प्रकार के सत्यापन की आवश्यकता के द्वारा सुरक्षा की एक अतिरिक्त परत जोड़ता है। यह एक फ़िंगरप्रिंट, आपके फ़ोन पर भेजा गया सुरक्षा कोड या सुरक्षा कुंजी हो सकता है।

Enable two-factor authentication (2FA):
Two-factor authentication adds an extra layer of security by requiring a second form of verification in addition to your password. This can be a fingerprint, a security code sent to your phone, or a security key.



अपने पासवर्ड को नियमित रूप से अपडेट करें:
पासवर्ड को नियमित रूप से अपडेट किया जाना चाहिए, विशेष रूप से अगर उनके साथ छेड़छाड़ किए जाने का संदेह हो या अगर आपके द्वारा उपयोग की जाने वाली साइट्स में से किसी एक का डेटा उल्लंघन हुआ हो।

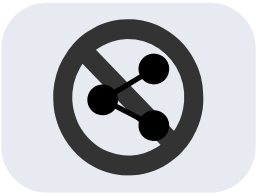
Regularly update your passwords:
Passwords should be updated regularly, especially if there is a suspicion of them being compromised or if there's been a data breach of one of the sites you use.

पासवर्ड का पुन: उपयोग न करें:
एकाधिक खातों में एक ही पासवर्ड का पुन: उपयोग करने से हमलावरों के लिए एकाधिक खातों तक पहुंच प्राप्त करना आसान हो जाता है अगर वे एक पासवर्ड को क्रैक करने में सक्षम होते हैं।

Do not reuse passwords:
Reusing the same password across multiple accounts makes it easier for attackers to gain access to multiple accounts if they are able to crack one password.

फ़िशिंग स्कैम और सोशल इंजीनियरिंग के बारे में खुद को और अपने सहयोगियों को शिक्षित करें: फ़िशिंग और सोशल इंजीनियरिंग हमले हमलावरों के लिए पासवर्ड चुराने के सामान्य तरीके हैं। इस प्रकार के हमलों के बारे में जागरूक होना और उनका पता लगाने का तरीका जानना आपके पासवर्ड को सुरक्षित रखने में मदद कर सकता है।

Educate yourself and your colleagues about phishing scams and social engineering: Phishing and social engineering attacks are common ways for attackers to steal passwords. Being aware of these types of attacks and knowing how to spot them can help protect your passwords.



पासवर्ड लिखने या शेयर करने से बचें: अपने पासवर्ड को निजी रखें, अपने पासवर्ड को किसी के साथ शेयर न करें, यहां तक कि अपने सहकर्मियों के साथ भी, और उन्हें ऐसी जगह पर न लिखें जहां वे आसानी से मिल सकें।

Avoid writing down or sharing passwords: Keep your passwords private, do not share your passwords with anyone, even your colleagues, and do not write them down in a place where they can be easily found.

सार्वजनिक वाई-फाई से सावधान रहें: हमलावर सार्वजनिक वाई-फाई नेटवर्क से आसानी से छेड़छाड कर सकते हैं। सार्वजनिक वाई-फाई नेटवर्क से कनेक्ट होने पर पासवर्ड जैसी संवेदनशील जानकारी दर्ज करने से बचें।

Be wary of public Wi-Fi: Public Wi-Fi networks can be easily compromised by attackers. Avoid entering sensitive information, such as passwords, while connected to a public Wi-Fi network.

अपने खातों की निगरानी करें: नियमित रूप से अपनी खाता गतिविधि की जांच करें और किसी भी संदिग्ध लॉगिन प्रयास या आपकी खाता जानकारी में किए गए बदलावों की निगरानी करें।

Monitor your accounts: Regularly check your account activity and look for any suspicious login attempts or changes made to your account information.

बहु -कारक प्रमाणीकरण के लाभ
Benefits of Multifactor Authentication (MFA)

- खातों तक अनधिकृत पहुंच को रोकता है
- कई स्तरित सुरक्षा प्रदान करता है
- पाशविक बल के हमलों से सुरक्षा
- सुरक्षा जोखिम/उल्लंघनों को कम करता है
- उपयोगकर्ताओं के लिए सुविधा

- Prevents unauthorized access to accounts
- Provides multiple layered protection
- Protection from brute force attacks
- Reduces security risks/breaches
- Convenience for the users

ONLINE SAFETY AND SECURITY

साइबर बुलिंग

साइबर बुलिंग ऑनलाइन लोगों को डराना है, जिसमें आपको धमकी भरे, अपमानजनक, शर्मनाक और परेशान करने वाले पोस्ट या कृत्यों के द्वारा ऑनलाइन एक सार्वजनिक मंच पर लक्षित किया जा सकता है।

इसे इलेक्ट्रॉनिक तकनीक के माध्यम से किया जा सकता है जिसमें डिवाइस और उपकरण जैसे सेल फोन, कंप्यूटर और टैबलेट के साथ-साथ संचार उपकरण शामिल हैं जिनमें सोशल मीडिया साइट्स, टेक्स्टमैसेज, ई-मेल, चैट रूम, चर्चा समूह और इंटरनेट में वेबसाइट्स शामिल हैं।

CYBER BULLYING

Cyber bullying is intimidating online behaviour, wherein you can be targeted on an online public platform with threatening, humiliating, embarrassing and harassing posts or acts.

It can be carried out through electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, e-mail, chat rooms, discussion groups and websites in Internet.

साइबरबुलिंग के उदाहरणों में टेक्स्ट मैसेज या ईमेल, ईमेल द्वारा भेजी गई अफवाहें या सोशल नेटवर्किंग साइट्स पर पोस्ट की गई अफवाहें और शर्मनाक तस्वीरें, वीडियो, वेबसाइट या नकली प्रोफाइल भेजना शामिल हैं।

Examples of Cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and sending embarrassing pictures, videos, websites, or fake profiles.

साइबर बुलिंग को रोकने के लिए सुरक्षा सुझाव और दिशानिर्देश

- सोशल मीडिया खातों पर सुरक्षा और गोपनीयता सुविधाओं को सक्षम करें
- बच्चों को साइबर बुलिंग या अनुचित सामग्री तक पहुँचने से बचने या रोकने के लिए पैरेंटल कंट्रोल बार, डेस्कटॉप फायरवॉल, ब्राउज़र फ़िल्टर का उपयोग करें।
- नकारात्मक पोस्ट मिलने पर चर्चा वाला पृष्ठ छोड़ दें और बुली को ब्लॉक करें।
- बुली की भड़काऊ टिप्पणियों पर कभी भी प्रतिकार न करें।
- समझें कि दूसरों की प्रतिक्रिया आपकी गलती नहीं है।
- सुनिश्चित करें कि आपके बच्चे के स्कूल में इंटरनेट सुरक्षा शिक्षा प्रोग्रामिंग है।
- कंप्यूटर लैब्स, इंटरनेट लैब्स के नियम बनाएं।
- साइबर बुलिंग के लिए स्कूल में इंटरनेट, कंप्यूटर और अन्य उपकरणों के उपयोग के संबंध में स्पष्ट नियम, दिशानिर्देश और नीतियां निर्दिष्ट करें।
- छात्रों को यह सब सिखाएं किकिसी भी प्रकार से किसी को डराना धमकाना अस्वीकार्य हैं और यह अनुशासनहीनताहै।
- छात्रों को सलाह देना और साथी के साथ निगरानी रखना।

Security tips and guidelines to prevent cyber bullying

- Enable Security and Privacy features on social media accounts
- Use Parental Control Bars, Desktop Firewalls, Browser Filters to avoid or preventing children from cyber bullying others or accessing inappropriate content.
- Leave the discussion page and block the bully, when you find negative posts.
- Never retaliate to the provocative comments of the bully.
- Understand that others reaction is not your fault.
- Make sure your child's school has Internet Safety education programming.
- Form the rules of computer Labs, Internet labs.
- Specify clear rules, Guidelines and policies regarding the use of the Internet, Computers and Other Devices at School for Cyber Bullying.
- Teach students that all; types of bullying are unacceptable and such behaviour is subject to discipline.
- Mentoring the students and establishment of peer Monitoring.

यदि आप किसी को साइबरबुलिंग का शिकार होते हुए या ऑनलाइन संदिग्ध गतिविधि देखते हैं, तो इसकी रिपोर्ट प्लेटफ़ॉर्म पर करें।

If you see someone being cyberbullied or suspicious activity happening online, Report it to the platform

यह करें / Do's

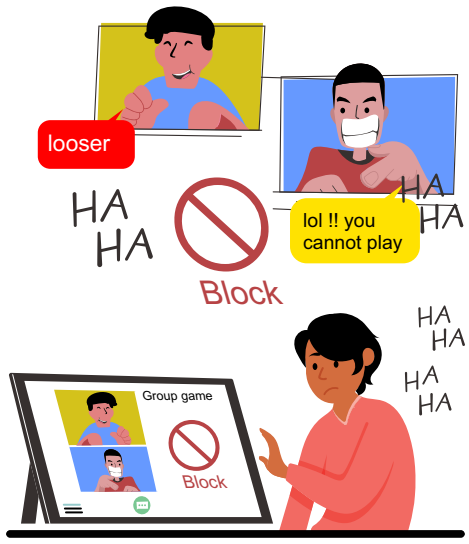
- तुरंत हस्तक्षेप करें। किसी दूसरे वयस्क की मदद लेना ठीक है।
- शामिल बच्चों को अलग करें।
- सुनिश्चित करें कि हर कोई सुरक्षित है।
- किसी भी तत्काल चिकित्सा या मानसिक स्वास्थ्य की जरूरतों को पूरा करें।
- शांत रहें। आसपास खड़े लोगों सहित शामिल बच्चों को आश्वस्त करें।
- जब आप बीच में हस्तक्षेप करें तो सम्मानजनक व्यवहार करें।

- Intervene immediately. It is ok to get another adult to help.
- Separate the kids involved.
- Make sure everyone is safe.
- Meet any immediate medical or mental health needs.
- Stay calm. Reassure the kids involved, including bystanders.
- Model respectful behavior when you intervene.

यह न करे / Don'ts

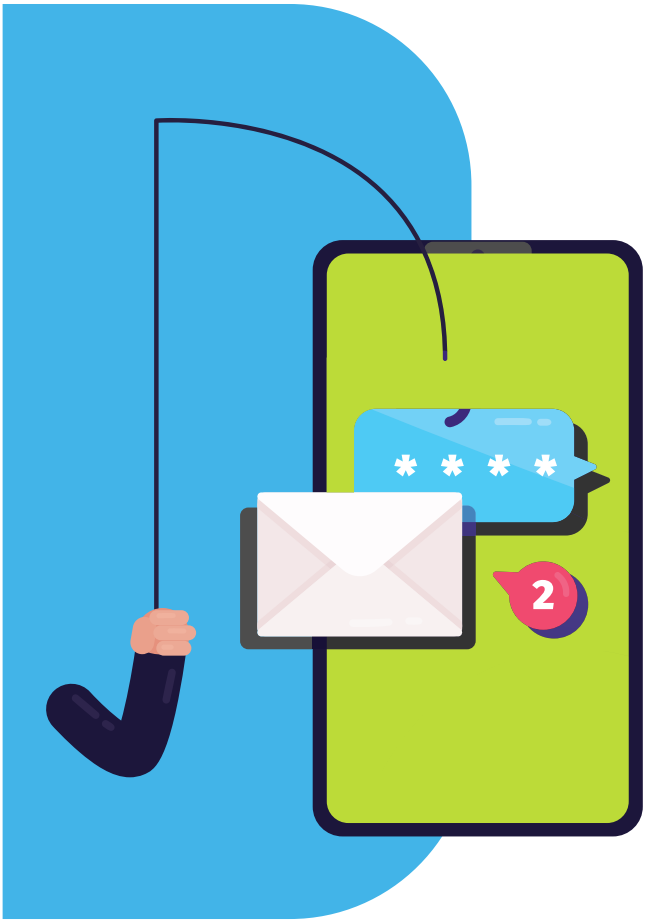
- इसे नज़रअंदाज़ न करें। ऐसा मत सोचो कि बच्चे वयस्कों की मदद के बिना इससे निपट पाएंगे।
- मामले को तुरंत सुलझाने का प्रयास न करें।
- अन्य बच्चों को सार्वजनिक रूप से कहने के लिए मजबूर न करें कि उन्होंने क्या देखा।
- दूसरे बच्चों के सामने शामिल बच्चों से सवाल न करें।
- शामिल बच्चों से एक साथ बात न करें, अलग से ही करें।
- बच्चों को शामिल न करें माफी मांगें या मौके पर ही मनमुटाव को ठीक कर लें।

- Don't ignore it. Don't think kids can work it out without adult help.
- Don't immediately try to sort out the facts.
- Don't force other kids to say publicly what they saw.
- Don't question the children involved in front of other kids.
- Don't talk to the kids involved together, only separately.
- Don't make the kids involved apologize or patch up relations on the spot.



ऑनलाइन गेम मनोरंजन के लिए हैं, वे आपको परिभाषित नहीं करते हैं। सुरक्षित रहें और किसी बदमाश को अपने साथ खिलवाड़ न करने दें।

Online games are for fun, they do not define you Play safe and don't let a bully mess with you



फिशिंग हमले

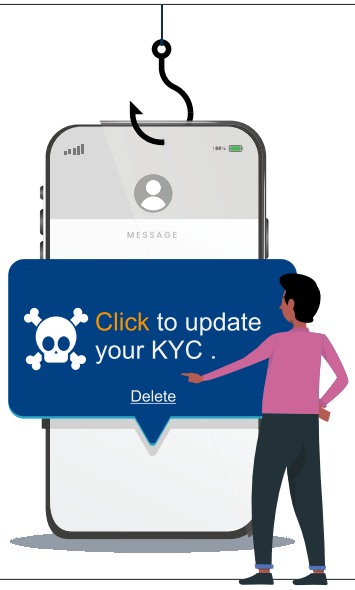
फ़िशिंग ई-मेल जैसे इलेक्ट्रॉनिक संचार माध्यमों के माध्यम से एक भरोसेमंद उपयोगकर्ता विवरण के रूप में उपयोगकर्ता नाम, पासवर्ड, पिन, बैंक खाता, क्रेडिट कार्ड विवरण जैसी जानकारी प्राप्त करने का प्रयास करने का एक तरीका है।

फ़िशिंग आमतौर पर ई-मेल स्पूफिंग या त्वरित संदेश द्वारा किया जाता है और यह अक्सर उपयोगकर्ताओं को एक नकली वेबसाइट पर विवरण दर्ज करने का निर्देश देता है जिसका रूप और अनुभव लगभग वैध के समान होता है। फ़िशिंग उपयोगकर्ताओं को धोखा देने के लिए उपयोग की जाने वाली सोशल इंजीनियरिंग तकनीकों का एक उदाहरण है।

PHISHING ATTACKS

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN,bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

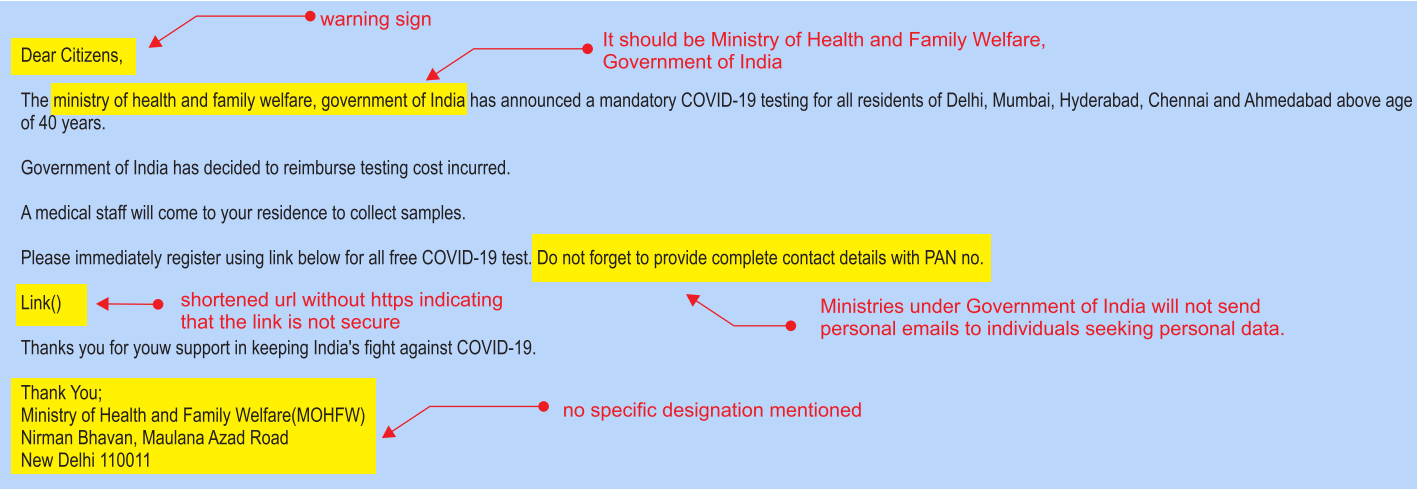
Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.



सतर्क रहें, विशिंग प्रक्रिया में न फंसें

Stay cautious don't get caught in the Vishing process

एक फ़िशिंग ईमेल संदेश कैसा दिखता है? विस्तार से :।
How does a phishing email message look like? In detail ....



- वर्तनी और अशुद्घ व्याकरण की जाँच करें।
- दी गयी लिंक्स आपको .exe फ़ाइलों तक भी ले जा सकता हैं। इस प्रकार की फ़ाइल दुर्भावनापूर्ण सॉफ़्टवेयर को फैलाने के लिए जानी जाती है।

- Check for Spelling and bad grammar.
- Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

धमकियां

कभीकभी आपको ऐसा धमकी भरा मेल मिल सकता है कि यदि आप ईमेल संदेश का जवाब नहीं देते हैं तो आपका वेबमेल अकाउंट बंद हो जाएगा। ऊपर दिखाया गया ईमेल संदेश उसी तरह की चाल का एक उदाहरण है। साइबर क्रिमिनल तकनीकों का प्रयोग अक्सर लोगों को यह विश्वास दिलाने के लिए करते हैं कि उनकी सुरक्षा से समझौता किया गया है।

Threats

Sometimes you may receive a threat mail saying that your webmail account would be closed if you do not respond to an e-mail message. The e-mail message shown above is an example of the same trick. Cybercriminals often use techniques to make one believe that security has been compromised.

लोकप्रिय वेबसाइटों या कंपनियों को स्पूफ़ करना।

- स्कैम में निपुण लोग ईमेल में ऐसे ग्राफिक्स का उपयोग करते हैं जो वैध वेबसाइटों के समान दिखते हैं, लेकिन वास्तव में आपको घोटाले की जाली साइट्स या वैध दिखने वाली पॉपअप विंडो पर ले जाते हैं।
- साइबर क्रिमिनल्स ऐसे वेब एड्रेसेस का भी इस्तेमाल करते हैं जो नामी कंपनियों के नाम से मिलते जुलते लेकिन थोड़े बदले हुए होते हैं
- साइबर क्रिमिनल्स आपको फोन पर कॉल कर सकते हैं और आपकी कंप्यूटर सम्बन्धी समस्याओं को हल करने में मदद करने या आपको एक सॉफ़्टवेयर लाइसेंस बेचने की पेशकश कर सकते हैं।

Spoofing popular websites or companies.

- Scam artists use graphics in email that look identical to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered
- Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license.

याद रखने योग्य स्टेप्स (चरण) / Steps to remember

चरण 1 :

ब्राउजर में url को क्रॉस चेक करें

- संख्याओं से शुरू होने वाली वेबसाइटों में अपनी जानकारी दर्ज न करें

चरण 2

गलत वर्तनी url की हमेशा जाँच करें

- इसलिए एड्रेस बार में url हमेशा टाइप करें और कॉपीपेस्ट न करें

चरण 3

- हमेशा सुरक्षित चैनल में ही ऑनलाइन बैंकिंग करें अर्थात् सुरक्षित बैंकिंग के लिए पैडलॉक और सुरक्षित चैनल होने का ध्यान रखें
- हमेशा वेबसाइट के विश्वसनीय होने की जांच करें, जिसमें रॉज और पैडलॉक हों

चरण 4

- हमेशा वित्तीय या अन्य व्यागित जानकारी के लिए किसी भी, और विशेष रूप से तत्काल अनुरोध के ईमेल को संदेह से देखें। जब संदेह हो, तो संदिग्ध ईमेल का उत्तर न दें या संदिग्ध वेबसाइटों पर जानकारी दर्ज न करें। आपके द्वारा प्राप्त संचार की वैधता की पुष्टि करने के लिए आप कथित प्रेषक से संपर्क भी कर सकते हैं।
- फ़िशिंग साइट का एक उदाहरण, पंजाब नेशनल बैंक की साइट की तरह दिख एवं प्रतीत हो रही है।

चरण 4

- कभी भी उन ईमेल्स का उत्तर न दें जो आपकी व्यागित जानकारी जैसे क्रेडिट कार्ड / डेबिट कार्ड / बैंक का विवरण मांगते हैं।

Step 1

Cross check the URL in the brows

- Don't enter your information in the websites that start with numbers

Step 2

Always check for the misspelled URL

- So Always key in the URL in the address bar yourself don't copy and paste

Step 3

- Always perform online banking in secure channel i.e check for the Padlock and secure channel for secure banking
- Always check for the trusted website which has https and padlock

Step 4

- Always view any email request for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not respond to questionable email or enter information on questionable websites. You may also contact the alleged sender to confirm the legitimacy of communications you've received.
- An Example of Phishing site, the look and feel of the Punjab national bank is same.

Step 5

- Never respond to the emails that ask for your personal information like creditcard /debit card/bank information.

सावधानियां / Precautions

ई-मेल के मूल स्रोत की पुष्टि किए बिना स्पैम मेल का जवाब न दें।

Don't respond to spam mails without verification of the e-mail origin.

जब तक उम्मीदवार का कंपनी द्वारा व्यक्तिगत रूप से साक्षात्कार न लिया जाए तब तक पैसा जमा न करें।

Don't deposit money unless the candidate is interviewed personally by the company.

पैसे देकर पिछले दरवाजे से नौकरी पाने की कोशिश न करें जो रोजगार प्रदान करने का वादा करता है, और जो उपयोगकर्ताओं को धोखा देगा।

Don't try to get job through back door methods by paying money which promises to provide employment, which will cheat users.

आगे बढ़ने से पहले किसी भी नौकरी की पेशकश के लिए मूल कंपनी की वेबसाइट की जांच करें।

Check with original company website for any job offers before proceeding.

खाते में साइन इन करने के लिए दो चरणीय सत्यापन कोड बनाए रखें (मोबाइल अलर्ट)।

Maintain two step verification code to sign into account (Mobile alert).

जब भी जालसाजी का पता चले तो तुरंत मूल कंपनी को सूचित करें।

Whenever the fraud is noticed immediately inform the original company.

अपने खाते में पैसा जमा करने से पहले यह सुनिश्चित करने के लिए कंपनी से फोन पर बात करें कि क्या पिछले खाते के विवरण और कंपनी के नाम में कोई बदलाव हुआ है।

Talk over phone with the company to ascertain, before depositing the money in their account, whether there is change of previous a/c details and name of the company.

मोर्फिंग

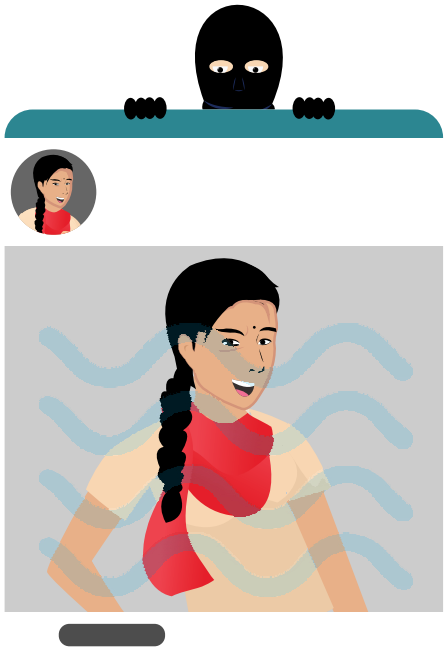
मॉर्फिंग ऑनलाइन उपलब्ध मॉर्फिंग टूल का उपयोग करके व्यक्ति की तस्वीरों को बिगाड़ना या बदलना है। युवा लड़कियां और महिलाएं आमतौर पर ऑनलाइन अपराधियों के हाथों शिकार हो जाती हैं, जो ऑनलाइन पोस्ट की गई अपनी तस्वीरों का उपयोग करते हैं और तस्वीरों को बदलकर इन बदली हुई तस्वीरों का प्रयोग करते हैं।

बदली हुई तस्वीरों का इस्तेमाल अपराधी आपको ब्लैकमेल करने, नकली ऑनलाइन प्रोफाइल बनाने, सेक्सटिंग, सेक्स चैट, अश्लील सामग्री, नग्न तस्वीरें आदि बनाने के लिए करते हैं।

MORPHING

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by changing the pictures.

The altered pictures are then used by perpetrators for blackmailing you, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc.,



ऑनलाइन तस्वीरें साझा करते समय हमेशा वॉटरमार्क का उपयोग करें। खुद को मॉर्फिंग से बचाने का सरल लेकिन प्रभावी तरीका है।

Always use watermark while sharing pictures online Simple yet effective way to safeguard yourself from MORPHING

सावधानियां / Precautions

सोशल मीडिया खातों पर अपनी सुरक्षा और गोपनीयता सुविधाओं को सक्षम करें

Enable your security and privacy features on social media accounts

कभी भी अपनी व्यक्तिगत तस्वीरों को सोशल मीडिया अकाउंट्स पर सार्वजनिक रूप से ऑनलाइन साझा न करें

Never share your personal pictures online publicly on social media accounts

चित्र साझा करते समय वॉटरमार्क का प्रयोग करें

Use watermark while sharing pictures

अपने सोशल मीडिया अकाउंट के लिए मजबूत पासवर्ड के साथ टू फैक्टर ऑथेंटिकेशन का इस्तेमाल करें।

Use two factor authentication with strong passwords for your social media accounts.

बाद में घटना का उल्लेख करने के लिए सबूत और स्क्रीन शॉट सहेजें।

Save the evidence and the screen shots for referring to the incident later

अगर आप समस्या में फंस गए हैं तो चुपचाप रहकर पीड़ित न हों बल्कि परिवार और दोस्तों की मदद लें

Don’t suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.

अगर आप सोशल मीडिया पर अपनी फेक प्रोफाइल या ऐसी कोई आपत्तिजनक पोस्ट देखते हैं तो इसकी सूचना सोशल मीडिया सहायता केंद्र पर दें।

If you observe your fake profile or any such objectionable post on social media, report on the social media help centre about it.

सामाजिक नेटवर्किंग सुरक्षा

सोशल मीडिया इंटरैक्टिव टेक्नोलॉजीस हैं जो जानकारी,विचारों, रूचियों, और अन्य प्रकार की अभिव्यक्ति को वर्चुअल कम्यूनिटीज और नेटवर्क के माध्यम से क्रिएट करने और शेयर करने की सुविधा प्रदान करता है। सोशल मीडिया प्लेटफॉर्म्स डिजिटल यूजर्स को एक दूसरे के साथ संचार करने बातचीत करने, जानकारी को साझा करने और कॉन्टेंट को क्रिएट करने की अनुमति देता है।

SOCIAL NETWORKING SECURITY

Social media are interactive technologies that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks. The social media platforms allow the digital users to communicate with each other have conversations, share information and create content.

सर्वोत्तम व्यवहार / Best practices

अपनी व्यक्तिगत जानकारी जैसे पता, मोबाइल नंबर, पर्सनल मेल आईडी और अन्य संवेदनशील पहचान संबंधी जानकारी को सोशल मीडिया पर शेयर करने से बचें।		Avoid sharing your personal information like address, mobile number, personal mail id and other sensitive identity related information on social media.
अपनी व्यक्तिगत तस्वीरों को सोशल मीडिया अकाउंट पर सार्वजनिक रूप से शेयर न करें		Do not share your personal pictures online publicly on social media accounts
उचित सत्यापन के बिना कभी भी फ्रेंड रिक्वेस्ट को स्वीकार न करें		Never accept friend requests without appropriate verification
जब तक आप स्रोत की प्रामाणिकता की पुष्टि नहीं कर लेते, तब तक कभी भी संदिग्ध लिंक पर क्लिक न करें या कुछ भी डाउनलोड न करें।		Never click on suspicious links or download anything until you verify the authenticity of the source.

अलग-अलग सोशल मीडिया अकाउंट और ईमेल्स के लिए अलग-अलग पासवर्ड का इस्तेमाल करें।

Use different passwords for different social media accounts and emails.

सिक्योरिटी और प्राइवेसी फीचर्स से परिचित रहें और सोशल मीडिया अकाउंट्ससपर उन्हे इनेबल करें।

Be aware of security and privacy features and enable them on the social media accounts

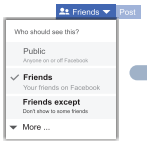
सोशल मीडिया प्लेटफॉर्म का इस्तेमाल करते समय सतर्क रहें, अगर आपको लगता है कि किसी अज्ञात/गुमनाम व्यक्ति द्वारा कमेंट्स भेजे जा रही हैं तो उन्हें तुरंत ब्लॉक कर दें।

Be alert while using social media platforms, if you feel that the comments are being sent from an unknown/anonymous person immediately block them.

स्पैलिंग और ग्रामर की गलतियों, इग्ज़ैजरैशन, एक्टिंग एनटाइटल जैसे कुछ पॉइंट्स/विशेषताओं के साथ ट्रोल को पहचानें और उन्हें ब्लॉक करें।

Identify the troll with few points/ traits like spelling & grammar mistakes, exaggeration, acting entitled and block them.

बाद में घटना का उल्लेख करने के लिए सबूत और स्क्रीन शॉट सहेजें।



Ensure to share personal videos privately and restrict privacy settings to friends only

अगर आप समस्या में फंस गए हैं तो चुपचाप रहकर पीड़ित न हों बल्कि परिवार और दोस्तों की मदद लें

Never share any compromising images, posts, videos of yourself to anyone, no matter who they are

अगर आप सोशल मीडिया पर अपनी फेक प्रोफाइल या ऐसी कोई आपत्तिजनक पोस्ट देखते हैं तो इसकी सूचना सोशल मीडिया सहायता केंद्र पर दें।

Turn off your electronic devices and web cameras when you are not using them.

अनजान लोगों से ऑनलाइन बातचीत करते समय बहुत सतर्क रहें, अपने फ्रेंड सर्कल के माध्यम से उस व्यक्ति की पहचान की पुष्टि करें।

Be very cautious when interacting with unknown people online, confirm the identity of the person through your friends circle.

ऑनलाइन बैंकिंग सुरक्षा

र्तमान डिजिटल समय में, ऑनलाइन/इंटरनेट/वेब बैंकिंग एक ऐसी सेवा है जो ग्राहकों को एक बटन के क्लिक पर बैंकिंग सेवाओं तक पहुंच प्रदान करती है। यह ग्राहकों को किसी भी समय कहीं से भी अपनी सुविधानुसार आराम से वित्तीय लेनदेन की एक विस्तृत श्रृंखला करने में सक्षम बनाता है।

फ़ायदे

वर्तमान डिजिटल समय में, ऑनलाइन/इंटरनेट/वेब बैंकिंग एक ऐसी सेवा है जो ग्राहकों को एक बटन के क्लिक पर बैंकिंग सेवाओं तक पहुंच प्रदान करती है।
इसके कई फायदे हैं जैसे -

- चौबीसों घंटे आसान पहुँच, सुविधा प्रदान करता है और समय बचाता है।
- मोबाइल बैंकिंग ऐप सेवा के माध्यम से चलते-फिरते बैंकिंग सेवाएं प्रदान करता है।
- खातों की निगरानी करें, बिलों का भुगतान करें, धनराशि स्थानांतरित करें, विवरण देखें और डाउनलोड करें आदि।

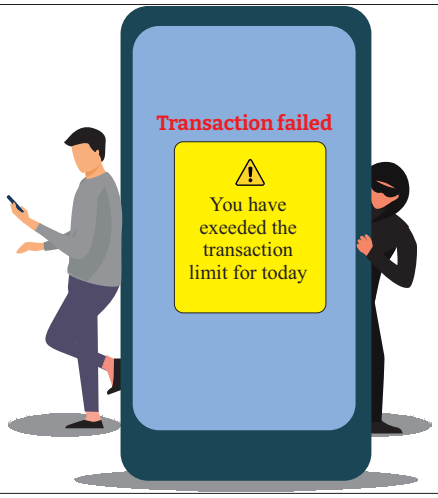
ONLINE BANKING SECURITY

In current digital times, online/internet/web banking is a service that offers customers access to banking services at the click of a button. It facilitates and enables customers to perform a wide range of financial transactions comfortably at their convenience from anywhere at any time.

Benefits

In current digital times, online/internet/web banking is a service that offers customers access to banking services at the click of a button.
It has many benefits like-

- Offers easy access round the clock, convenience and saves time.
- Offers banking services on the go through mobile banking app service.
- Monitor accounts, pay bills, transfer funds, view and download statements etc.,



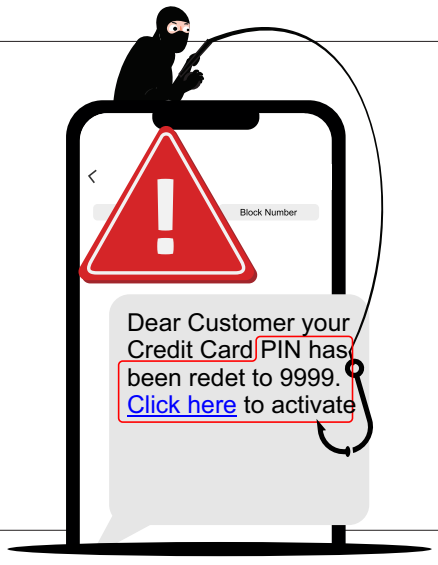
ऑनलाइन लेन-देन तीव्र हो सकता है जोखिम से बचने के लिए सीमा निर्धारित करें।

Online transactions can be quick Set limits to avoid risk

यह करें / Do's

- आपको प्राप्त होने वाले किसी भी अटैचमेंट को खोलने या डाउनलोड करने में सतर्क रहें, भले ही उन्हें किसने भी भेजा हो।
- कोई भी व्यक्तिगत जानकारी दर्ज करने/देने से पहले प्रेषक की ईमेल आईडी देखें।
- अपडेट एंटीवायरस, एंटीस्पाइवेयर और फ़ायरवॉल सॉफ़्टवेयर का उपयोग करें।
- वेब ब्राउज़र को हमेशा अपडेट करें और फ़िशिंग फ़िल्टर एनेबल करें।
- किसी भी संदिग्ध ईमेल की प्राप्ति के मामले में, यह पुष्टि करने के लिए कंपनी को कॉल करें कि यह वैध है या नहीं।
- ऑनलाइन शॉपिंग, व्यक्तिगत आदि जैसी चीज़ों के लिए एक अलग ईमेल खाते का उपयोग करें।
- अज्ञात स्रोतों से संदेशों के माध्यम से प्राप्त लिंक पर कभी भी क्लिक न करें।
- संदेह की स्थिति में, टोल फ्री नंबर या बैंक द्वारा उपलब्ध कराए गए किसी अन्य संपर्क से संपर्क करने का प्रयास करें।
- ग्राहक सेवा अधिकारियों या सेवा प्रदाताओं से संपर्क करने के लिए संस्थानों की अधिकृत वेबसाइटों पर उपलब्ध संपर्क नंबरों का उपयोग करें।
- कोई भी व्यक्तिगत जानकारी दर्ज करने/देने से पहले प्रेषक की ईमेल आईडी देखें।

- Be cautious about opening any attachment or downloading files you receive regardless of who sent them
- Look for the sender's email ID before you enter/give away any personal information.
- Use updated antivirus, antispyware and firewall software.
- Always update the web browser and enable phishing filters.
- In case of receipt of any suspicious email, do call the company to confirm if it is legitimate or not.
- Use a separate email account for things like shopping online, personal etc.,
- Never click on links received through messages from unknown sources.
- In case of doubt, try to contact the toll free number or any other contact provided by the bank.
- Use the contact numbers available on authorized websites of the institutes for contacting customer care executives or service providers.
- Look for the sender's email ID before you enter/give away any personal information.



आपका बैंक आपको आपका पिन मैसेज नहीं करेगा। यह एक फिशिंग का कांटा है।

Your bank won't text you your PIN. That's a Phish hook

यह न करे / Don'ts/

- कभी भी ओटीपी, पिन, सीवीवी, डेबिट/क्रेडिट कार्ड की जानकारी किसी के साथ साझा न करें।
- ऐसे ईमेल या पॉप-अप संदेश का उत्तर न दें जो व्यक्तिगत या वित्तीय जानकारी मांगता हो।
- व्यक्तिगत या वित्तीय जानकारी यानी क्रेडिट कार्ड या अन्य संवेदनशील जानकारी ईमेल के माध्यम से साझा न करें।
- वैधता के बारे में संदेह होने पर ईमेल या संदेश न खोलें।
- अप्रत्याशित ईमेल के अटैचमेंट न खोलें, विशेषकर ज़िप फ़ाइलें और कभी भी .exe फ़ाइलें न चलाएँ।
- व्यक्तिगत संचार के लिए कंपनी के ईमेल पते का उपयोग न करें।
- किसी भी स्पैम ईमेल से अटैचमेंट न खोलें/डाउनलोड न करें।
- सोशल नेटवर्किंग साइटों पर संदिग्ध वीडियो या फ़ोटो न खोलें क्योंकि सोशल नेटवर्किंग साइटें फ़िशिंग का मुख्य लक्ष्य होती हैं।
- बैंक से संबंधित विवरण मांगने वाले फोन कॉल का जवाब कभी न दें। यह विशिंग (वॉयस फ़िशिंग) हो सकता है।
- गूगल सर्च से अचानक मिले सेवा प्रदाताओं के नंबरों पर कॉल न करें क्योंकि वे फर्जी नंबर हो सकते हैं।
- किसी भी संदेश (एसएमएस) का जवाब न दें जिसमें "चोरी" या "खो गई" खाते की जानकारी की पुष्टि करने या प्रकट करने के लिए प्रोत्साहित करने के लिए कहा गया हो।
- ऐसे ईमेल या पॉप-अप संदेश का उत्तर न दें जो व्यक्तिगत या वित्तीय जानकारी मांगता हो।

- Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
- Don't reply to an email or pop-up message that asks for personal or financial information.
- Don't share personal or financial information i.e credit card or other sensitive information via email.
- Don't open email or message, in case of suspicion about legitimacy.
- Don't open attachments of unexpected emails, especially ZIP files and NEVER run .exe files.
- Don't use company email addresses for personal communication.
- Don't open/download attachments from any spam email.
- Don't open suspicious videos or images on social networking sites since social they are the prime target of phishing.
- Never respond to phone calls asking for bank related details. It might be vishing (voice phishing).
- Do not call the numbers of service providers randomly found by Google search as they can be fake numbers.
- Don't respond to any message (sms) asking to confirm account information that has been "stolen" or "lost" or encouraging to reveal
- Don't reply to an email or pop-up message that asks for personal or financial information.

अपने कार्ड को सुरक्षित रखने के लिए RFID (रेडियो फ्रीक्वेंसी आइडेंटिफिकेशन) ब्लॉकिंग स्लीव का उपयोग करें।

Use an RFID (Radio frequency identification) blocking sleeve To keep your card safe and relieve

SCAMS AND SECURITY MEASURES


Home / Companies / News / Digital arrest and Rs 7 crore heist: How Vardhman Group head was tricked

Digital arrest and Rs 7 crore heist: How Vardhman Group head was tricked

The fraudsters used fake court orders and impersonated the Chief Justice of India to convince Oswal he was part of a money laundering investigation

Ref. https://www.business-standard.com/companies/news/digital-arrest-and-rs-7-crore-heist-how-vardhman-group-head-was-tricked-124100100832_1.html

फेडएक्स (FEDEX) कूरियर घोटाला / डिजिटल गिरफ्तारी घोटाले

फेडएक्स कूरियर घोटाला बाजार में एक नया और तेजी उभरता हुआ घोटाला है, जहाँ ठग कूरियर कंपनी के कर्मचारियों, कस्टम अधिकारियों या पुलिस अधिकारियों के रूप में प्रस्तुत होते हैं और लोगों को कॉल करके कहते हैं कि उनके नाम पर एक कूरियर भेजा गया है जिसमें अवैध वस्तुएं हैं। वे इस बहाने धोखाधड़ी करने के लिए डराने-धमकाने की रणनीति का उपयोग करते हैं।

"हाल के समय में/दिनों में, भारत ने 'डिजिटल गिरफ्तारी' घोटालों में वृद्धि देखी है। साइबर अपराधी सी बी आई (CBI) या स्थानीय पुलिस जैसी प्रतिष्ठित एजेंसियों के अधिकारियों के रूप में प्रस्तुत होते हैं। वे फोन कॉल के माध्यम से पीड़ितों को निशाना बनाते हैं और आरोप लगाते हैं कि वे संदिग्ध गतिविधियों में शामिल हैं – अक्सर ऐसे पार्सल के इर्द-गिर्द, जिनमें अवैध वस्तुएं होती हैं। ठग डराने-धमकाने की रणनीति अपनाते हैं और दावा करते हैं कि पीड़ित 'डिजिटल गिरफ्तारी' में हैं और अपना नाम साफ़ करने के लिए उनके निर्देशों का पालन करना होगा। ये निर्देश आमतौर पर पैसे स्थानांतरित करने या संवेदनशील वित्तीय जानकारी साझा करने से संबंधित होते हैं।

डिजिटल गिरफ्तारी घोटाले हाल के समय में तेजी से बढ़ रहे हैं, खासकर भारत में। कई मामले सामने आए हैं, जहां लोग ठगों द्वारा धोखा खाकर बड़ी रकम खो चुके हैं।

FEDEX COURIER SCAMS / DIGITAL ARREST SCAMS

The Fedex courier scam is a new thriving scam in the market where fraudsters impersonating as courier company employees, customs officials or as police officials and call a people and say that there is a courier that is sent in their names which has illegal items in it and use fear tactics to commit fraud.

In recent times, India has witnessed a surge in the "digital arrest" scams. Cybercriminals impersonate officials from esteemed agencies like the CBI or local police. They target victims with phone calls, alleging involvement in suspicious activities – often centered around parcels containing illegal items. The scammers use scare tactics, claiming the victim is under "digital arrest" and must clear their name by following their instructions. These instructions typically involve transferring money or sharing sensitive financial data.

Digital arrest scams have been on the rise in recent times, particularly in India. There have been several cases reported, where people lost large sums of money after being fooled by scammers.

कार्यप्रणाली / Modus Operandi

कूरियर कंपनी/अधिकारी/पुलिस के रूप में फोन कॉल (अक्सर नकली कॉलर आईडी का उपयोग करते हुए)।

Calls posing as a courier company/official/police (often using fake caller ID).

आपके नाम पर एक पैकेज जिसमें अवैध वस्तुएं (जैसे ड्रग्स, क्रेडिट कार्ड) हैं और जिसे आपके आधार (पहचान दस्तावेज़) से जोड़ा जाता है।

A package in your name containing illegal items (drugs, credit cards) linked to your Aadhaar (identity document).

आधिकारिक शब्दों का उपयोग करना और संभवतः आपको जांच के लिए एक नकली 'उच्च अधिकारी' से जोड़ना।

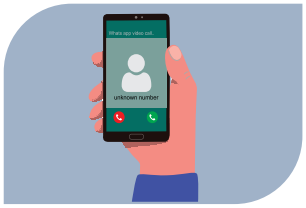
Using official terms and potentially transferring you to a fake "higher authority" for "investigation."

पीड़ित के पैसे को मनी लॉन्ड्रिंग में शामिल होने की जांच के लिए आरबीआई (RBI) के सॉफ्टवेयर द्वारा 'जांच' करने की आवश्यकता बताना और 'सत्यापन' के लिए पैसे स्थानांतरित करने का अनुरोध करना। यह पूरी तरह से आपके पैसे चुराने के उद्देश्य से होता है।"

Victim's money needs to be "checked" by an RBI software for involvement in money laundering and request transfers for "verification". This is purely to steal your money.

आपको सहायता मांगने या जानकारी सत्यापित करने से रोकना।

Preventing you from seeking help or verifying the information.



वीडियो कॉल के माध्यम से कानूनी परिणामों की धमकी देकर डर बढ़ाना।

Threating legal consequences to heighten fear using video calls.

सुरक्षा उपाय / Security Tips

- कॉल करने वाले की प्रामाणिकता की जाँच करें।
- व्यक्तिगत जानकारी साझा न करें।
- अवांछित कॉल और संदेशों के प्रति सतर्क रहें।
- अधिकारियों से परामर्श करें।
- अपने एंटीवायरस और एंटीमालवेयर सॉफ़्टवेयर को अपडेट रखें।
- संवेदनशील समूहों के बीच जागरूकता फैलाएं और उन्हें शिक्षित करें।

- Verify authenticity of the caller
- Do not share personal information
- Stay skeptical / cautious of unsolicited calls and messages
- Consult authorities
- Keep your antivirus and anti malware software updated
- Spread awareness and educate vulnerable groups

याद रखें : कानून प्रवर्तन प्राधिकारीहमेशा उचित प्रक्रियाओं का पालन करते हैं और डिजिटल गिरफ्तारी जैसे तरीकों का सहारा नहीं लेते हैं।
Remember: Law enforcement will always follow proper procedures and will not resort to such practices like digital arrest.

निवेश घाटालें

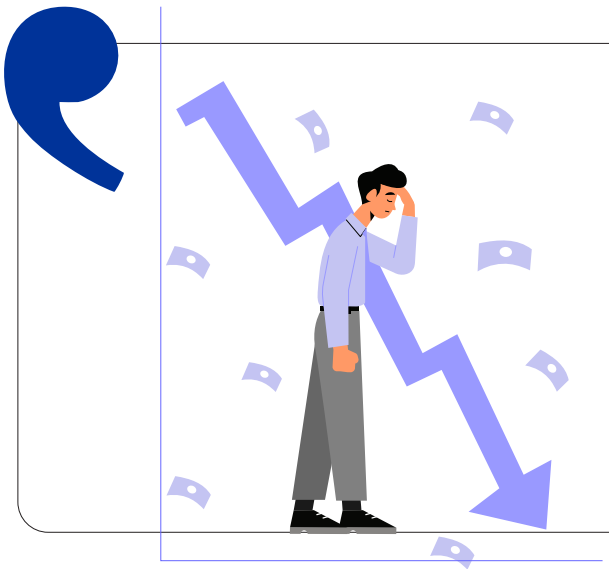
निवेश घोटाले कपटपूर्ण या भ्रामक योजनाएं हैं, जो धोखेबाजों द्वारा व्यक्तियों को धोखा देने और उन्हें ऐसे निवेश करने के लिए प्रेरित करने के लिए डिज़ाइन की जाती हैं जो या तो होते नहीं हैं या गलत तरीके से प्रस्तुत किए गए हैं। इन घोटालों का अक्सर वे लोगों शिकार होते हैं जो अपने धन में वृद्धि या अपने निवेश पर अधिक रिटर्न अर्जित करना चाहते हैं।

ये निवेश घोटाले आम तौर पर धन और कम समय में अच्छा रिटर्न अर्जित करने वाले व्यक्ति की इच्छा का दुरुपयोग करते हैं। ऐसे घोटालों को अंजाम देने वाले धोखेबाज अक्सर लोगों को उनकी मेहनत की कमाई लगाने के लिए लुभाने वाले उच्च रिटर्न, विशेष सौदे या अंदरूनी जानकारी का वादा करते हैं। धोखेबाज़ अपने ऑफ़र को उचित और आकर्षक दिखाने के लिए नकली क्रेडेंशियल, उपहार या वित्तीय रिपोर्ट पेश करने जैसी प्रेरक रणनीति अपनाते हैं।

INVESTMENT SCAMS

Investment scams are fraudulent or deceptive schemes, that are designed by fraudsters to deceive individuals and trick them into making investments that either do not exist or are misrepresented. These scams often prey on people's desire to grow their wealth or earn high returns on their investments.

These investment scams usually misuse the individual's desire for wealth and earn good returns in a short time. The fraudsters operating such scams often promise high returns, exclusive deals, or insider information to entice individuals into parting with their hard-earned money. The fraudsters employ persuasive tactics, such as presenting fake credentials, testimonials, or financial reports, to make their offers seem legitimate and appealing.



Invest online with care as scams are not rare. Look for trusted online ventures and guard your treasures

ऑनलाइन निवेश सावधानी से करें क्योंकि घोटाले दुर्लभ नहीं हैं । विश्वसनीय ऑनलाइन उद्यमों की तलाश करें और अपने खजाने की रक्षा करें ।

सुरक्षा उपाय / Security Measures

कोई भी निवेश करने से पहले, व्यापक शोध और उचित परिश्रम करें।

Before making any investment, conduct comprehensive research and due diligence.

केवल उन निवेश पेशेवरों, ब्रोकर्स या सलाहकारों से जुड़ें जो पंजीकृत और लाइसेंस प्राप्त हैं।

Only engage with investment professionals, brokers, or advisors who are registered and licensed

असाधारण रूप से उच्च रिटर्न या गारंटीकृत लाभ का वादा करने वाले निवेश के अवसरों को स्वीकार करते समय सावधानी बरतें।

Exercise caution when encountering investment opportunities that promise exceptionally high returns or guaranteed profits

ऐसे किसी भी व्यक्ति से सावधान रहें जो आप पर तत्काल निवेश का निर्णय लेने के लिए दबाव डालता है या अत्यावश्यकता की भावना पैदा करता है।

Beware of anyone who pressures you into making immediate investment decisions or creates a sense of urgency.

अनपेक्षित निवेश का प्रस्ताव, विशेष रूप से कोल्ड कॉल, ईमेल या सोशल मीडिया पर मैसेज के माध्यम से प्राप्त करते समय संदेह का एक स्वस्थ स्तर बनाए रखें।

Be cautious when you receive unsolicited investment offers, particularly through cold calls, emails, or messages on social media

असत्यापित व्यक्तियों या कंपनियों के साथ बैंक खाता संख्या या सोशल सिक्योरिटी नंबर जैसे संवेदनशील विवरणों को साझा करने से दूर रहकर अपनी व्यक्तिगत और वित्तीय जानकारी सुरक्षित रखें।

Safeguard your personal and financial information by refraining from sharing sensitive details with unverified individuals or companies

अपने निवेश विवरण, ट्रांजेक्शन हिस्ट्री और खाते की शेष राशि की नियमित रूप से समीक्षा करें। संभावित मुद्दों के समाधान के लिए किसी भी विसंगति या संदिग्ध गतिविधियों की तुरंत अपने निवेश प्रदाता या वित्तीय संस्थान को रिपोर्ट करें।

Promptly report any suspicious activities to your investment provider or financial institution to address potential issues.

सामान्य निवेश घोटालों और धोखाधड़ी की तकनीकों से अपडेट रहें।

Stay updated on common investment scams and fraud techniques

यदि आपके सामने कोई निवेश घोटाला आता है या आपको संदेह है, तो तुरंत अपनी स्थानीय कानून प्रवर्तन एजेंसी और वित्तीय नियामक अधिकारियों को इसकी रिपोर्ट करें।

If you come across or suspect an investment scam, promptly report it to your local law enforcement agency and financial regulatory authorities

भारतीय डाक के नाम पर धोखाधड़ी

इंडिया पोस्ट

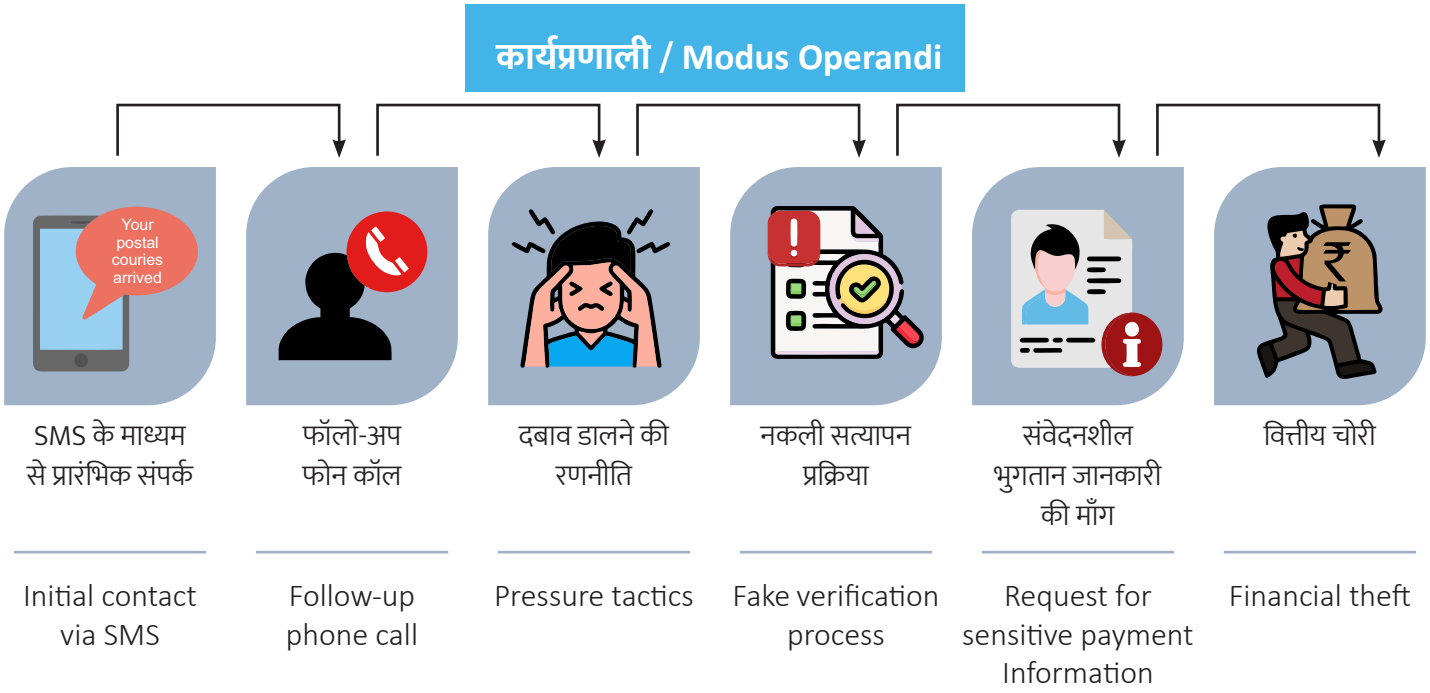
धोखाधड़ी यह देखा गया है कि साइबर ठग कमजोर समूहों जैसे महिलाओं और वरिष्ठ नागरिकों को निशाना बना रहे हैं, क्योंकि उन्हें जटिल डिजिटल धोखाधड़ी से अपरिचित समझा जाता है। अब साइबर अपराधी इंडिया पोस्ट का उपयोग करके निर्दोष व्यक्तियों को ठगने की कोशिश कर रहे हैं। हाल ही में एक मामले में, एक सेवानिवृत्त सरकारी कर्मचारी को 23.26 लाख रुपये की धोखाधड़ी का सामना करना पड़ा। हालाँकि अब तक केवल कुछ ही मामले सामने आए हैं, विशेषज्ञों का मानना है कि यह एक चिंताजनक प्रवृत्ति बन सकती है।

Ref.: https://economictimes.indiatimes.com/news/how-to/beware-cybercriminals-are-now-using-india-post-for-online-fraud/articleshow/113412935.cms

FRAUDS IN THE NAME OF INDIA POST

India Post fraud

It has been observed that cyber fraudsters are targeting vulnerable groups like women and senior citizens, due to their perceived lack of familiarity with complex digital scams. Cyber criminals are now using India Post to scam unsuspecting individuals. A recent case involved a retired government employee losing 23.26 lakh. Though only few cases have been reported so far, this can become a worrying trend, caution experts.



ई-मेल के माध्यम से प्राप्त जॉब ऑफर से सावधान रहें

- बहुत से छात्र नौकरियों के लिए ऑनलाइन आवेदन करते हैं। जालसाजी करने वाले व्यक्ति वेबसाइट्स पर पोस्ट किए गए विवरण एकत्र करते हैं और फ़िशिंग ई-मेल भेजते हैं।
- फर्जी मेल साइट के माध्यम से प्राप्त ई-मेल वास्तविक कंपनी के मेल की तरह दिखता है और साक्षात्कार भी आयोजित करता है।
- जालसाज (फ्रौड़स्टर) फर्जी मेल सेवा का उपयोग करके ऑफर लेटर भेज सकते हैं, एमएनसी के नाम पर स्पूफ कॉल कर सकते हैं और ऑफर लेटर भेज सकते हैं।
- इस प्रकार विक्टिम को एक फर्जी नौकरी का प्रस्ताव पत्र प्राप्त होता है। बदले में वह फ्रौड़स्टर सुरक्षा राशि के रूप में कुछ राशि जमा करने को कहता है।
- फ्रौडस्टर विभिन्न स्थानों / बैंक खातों / ई-वॉलेट में राशि जमा करवाता है और विक्टिम को धोखा देकर राशि तुरन्त निकाल लेता है

BE AWARE OF JOB OFFERS THROUGH E-MAILS

- Many of the students apply online for jobs. The accused collect the details posted in the websites and send phishing e-mails.
- The e-mail looks like a mail from genuine companies through fake mailer sites and also conducts interviews.
- Fraudster may send the offer letter using fake mailing service, make spoofed calls in the name of MNC and send the offer letters.
- Thus the victim receives a fake job offer letter. In return this fraudster asks to deposit some amount as a security deposit.
- The fraudster gets the amount deposited in the various places/Bank accounts/e-Wallets and immediately withdraw the amounts by cheating the victim

सावधानियां / Precautions

- ई-मेल के स्रोत के सत्यापन के बिना स्पैम मेल का जवाब न दें।
- अवैध तरीके से नौकरी पाने की कोशिश न करें। पैसे लेकर आपको जो रोजगार देने का वादा करता है, वह आपको धोखा दे सकता है।
- किसी भी नौकरी के ऑफर के लिए आवेदन करने से पहले सम्बन्धित कंपनी की मूल वेबसाइट देखें

- Don't respond to spam mails without verification of the e-mail origin.
- Don't try to get job through back door methods by paying money which promises to provide employment, which may cheat you.
- Check with original company website for any job offers before proceeding

जॉब स्कैमर्स के पास अपना कीमती समय न गवाँए, असली जॉब ऑफर मे पैसे कभी नहीं माँगते ।

Don't let job scammers take your timeGenuine job offers don't ask for a dime!

ऑनलाइन धोके (चीटिंग) / शॉपिंग के बारे में अवगत रहें

ऑनलाइन शॉपिंग घर बैठे सभी चीजों को खरीदने के लिए बहुत लोकप्रिय हो गई है, और यह इलेक्ट्रॉनिक उपकरणों, फर्नीचर, सौंदर्य प्रसाधन, और कई अन्य चीजों को खरीदने का एक सुविधाजनक तरीका है। स्टोर खुलने के लिए प्रतीक्षा करने के बजाय हम किसी भी विशेष समय कभी भी मनचाही वस्तु खरीद सकते हैं। इन सभी लाभों के बावजूद , चूंकि इंटरनेट के कुछ ख़ास जोखिम हैं, इसलिए ऑनलाइन खरीदारी करने से पहले कुछ सुरक्षा उपाय करना अति आवश्यक है।

- यदि आप नियमित उपयोगकर्ता नहीं हैं, तो ऑनलाइन खरीदारी के जानकार मित्रों / परिवार के सदस्यों से सहायता लें
- हमेशा सुरक्षित वेबसाइट्स से ऑनलाइन खरीदारी करें।
- एसएमएस, व्हाट्सएप, इंस्टाग्राम आदि के माध्यम से फ़िशिंग ई-मेल / लिंक का जवाब न दें क्योंकि वे क्रेडिट / डेबिट कार्ड के बारे में महत्वपूर्ण जानकारी का दुरूपयोग करने के लिए उसे संग्रहित कर सकते हैं।

BE AWARE OF ONLINE CHEATING/SHOPPING

Online shopping has become very popular to purchase all things without leaving your home, and it is a convenient way to buy things like electronic appliances, furniture, cosmetics, and many more. There is no particular time to buy things we can buy at anytime instead of waiting for the store to open. Apart from all these advantages, as there are unique internet risks, it is very important to take some safety measures before you go for online shopping.

- Take support from known friends / family members who is familiar with online shopping if you are not a regular user
- Always perform online shopping from secured websites.
- Don’t respond to phishing e-mails / links through SMS, WhatsApp, Instagram etc as they may collect vital information about the credit/debit cards and will misuse.

सुरक्षित साइटें सुखद खरीदारी सुनिश्चित करती हैंसतर्क रहें, समझदारी से खरीदारी करें और सुरक्षित रहें

Secure sites ensure happy buys Stay vigilant, Shop smart and stay safe

सुरक्षित ऑनलाइन शॉपिंग के लिए युक्तियाँ / Tips for safe online shopping

- ऑनलाइन खरीदारी आरम्भ करने से पहले यह सुनिश्चित करें कि आपका पीसी / मोबाइल सभी बुनियादी सुरक्षा जैसे एंटीवायरस, एंटी-स्पाइवेयर, फ़ायरवॉल, सिस्टम के साथ अपडेट किया गया है और उच्च स्तर की सुरक्षा युक्त हो तथा विश्वसनीय साइट्स के लिए वेब ब्राउज़र की सुरक्षा की गयी हो।
- ऑनलाइन खरीदारी करने से पहले, वैधता को लेकर वेबसाइट के बारे में जाँच-पड़ताल और समीक्षा करें। विक्रेता के विवरण जैसे टेलीफोन नंबर, उनकी प्रामाणिकता के लिए भौतिक पता भी नोट करें।
- उत्पाद की कीमतों में भारी विविधताओं की स्थिति में अलग-अलग वेबसाइट्स पर सर्च और तुलना करें,क्योंकि ऐसी विविधताएं नकली उत्पाद / वेबसाइट / मोबाइल ऐप के कारण हो सकती हैं।
- उपभोक्ताओं और विक्रेताओं की रिव्यु/कमेंट्स की जाँच करें।
- यदि आप ऑनलाइन कुछ खरीदने के लिए तैयार हैं, तो यह जांच लें कि क्या साइट सुरक्षित रूप से https का उपयोग करके संचार कर रही है और ब्राउज़र एड्रेस बार पर URL से पहले पैडलॉक है; उसके बाद वित्तीय लेनदेन के लिए आगे बढ़ें।
- लेन-देन पूरा करने के बाद लेन-देन के रिकॉर्ड का प्रिंट या स्क्रीनशॉट लें और उत्पाद का जैसे विवरण जैसे कीमत, पुष्टिकरण की रसीद, बिक्री की शर्तें और नियम आदि का विवरण भी लें।
- जैसे ही आप समाप्त कर लें तो क्रेडिट कार्ड / डेबिट कार्ड / ई-वॉलेट / खाता विवरणों की तुरंत जांच करें और आपके द्वारा भुगतान किए गए चार्जेज के बारे में पता करें और यदि आप इसमें कोई बदलाव पाते हैं तो तुरंत संबंधित अधिकारियों को रिपोर्ट करें।
- "कृपया अपने भुगतान, खरीदारी और उत्पाद के लिए खाता विवरण की पुष्टि करें"जैसे ई-मेल्स से सावधान रहें। याद रखें कि वैध ऑनलाइन शॉपिंग वेबसाइट / मोबाइल ऐप कभी भी ऐसे ई-मेल नहीं भेजते हैं। यदि आपको ऐसे ई-मेल प्राप्त होते हैं, तो तुरंत सम्वन्धित व्यापारी को कॉल कर सूचित करें।
- अपनी ऑनलाइन खरीदारी समाप्त करने के बाद सभी वेब ब्राउज़र कुकीज़ को हटा दें और अपना पीसी को बंद करें / ऐप बंद करें
- ऑनलाइन लेन-देन करते समय हमेशा सभी एप्लीकेशन्स को बंद करें
- ऑनलाइन शॉपिंग में, जहां उपलब्ध हो, हमेशा कैश ऑन डिलीवरी आप्शन को चुनें।

- Before you go for online shopping make sure your PC / Mobile is secured with all basic protections like an antivirus, anti-spyware, firewall, system updated with all patches and web browser security with the trusted sites and security level at high.
- Before shopping online, research and review the website for the legitimacy. Also make the note of the vendor details like telephone number, physical address for their authenticity.
- Search and compare the prices of the product in different websites for huge price variations, which may be due to fake product /website/ mobile app.
- Check the reviews of consumers and vendors.
- If you are ready to buy something online check whether the site is securely communicating using https and observe padlock before the URL on the browser address bar and then proceed with financial transactions.
- After finishing the transaction take a print or screenshot of the transaction records and details of product like price, confirmation receipt, terms and conditions of the sale.
- Immediately check the Credit card /Debit card / e-Wallet / Account statements as soon as you finish and get to know about the charges you paid were same, and if you find any changes immediately report to concerned authorities.
- Beware of the e-Mails like "please confirm of your payment, purchase and account detail for the product." Remember that legitimate online shopping website /Mobile apps never send such e-Mails. If you receive such e-Mails immediately call the merchant and inform the same.
- After finishing your online shopping clear all the web browser cookies and turn off your PC / close the app

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

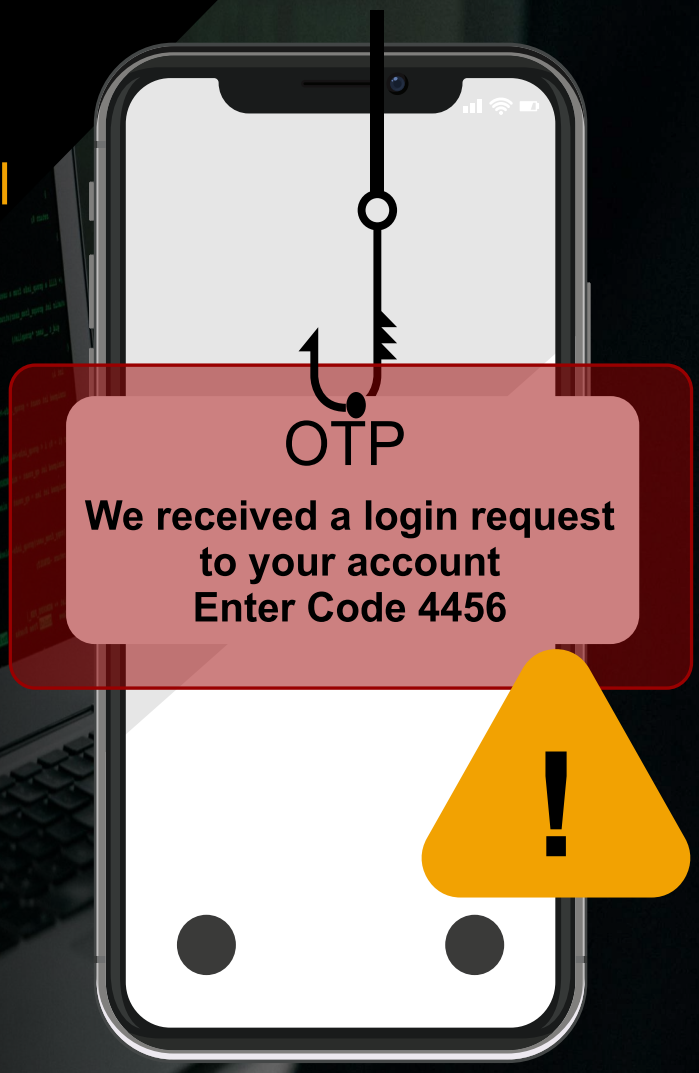
www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सी डैक CDAC

फ़िशिंग स्कैम
आपको अपने
मल्टी-फ़ैक्टर कोड
देने के लिए धोखा दे सकते हैं।
इन कोड को कभी
भी किसी के साथ
साझा न करें।

Phishing scams
can trick you
into giving your
multi-factor codes.
Never share these
codes with anyone



 # Online Safety

Supported by

certin Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

mygov मेरी सरकार

CYBER DOST

Indian Cyber Crime Coordination Centre
सहयोग करवाहै • Working Together With Vigour

साइबर स्पेस में जोखिम और कुछ निवारक उपाय

- **आप कहाँ है, इस तरह के व्यक्तिगत विवरण न दें:** अपनी विशिष्ट व्यक्तिगत जानकारी ऑनलाइन पोस्ट न करें, जैसे कि यात्रा की तारीख, स्थान और जो फिल्म आप देखना चाहते हैं उसका समय, शाम की कक्षा का विवरण आदि।

- **मित्र:**
  अजनबियों से मित्रता अनुरोध प्राप्त होने पर बेहतर है कि मित्रता के अनुरोध को स्वीकार न करें।

- सामने वाला व्यक्ति चाहे पुरुष हो या स्त्री, उससे **अपनी व्यक्तिगत जानकारी और प्रोफ़ाइल की जानकारी** साझा न करें क्योंकि उसके साथ आपके सम्बन्ध तनावपूर्ण होने की स्थिति में वह अपमानजनक/अभद्र संदेश पोस्ट कर सकता/सकती हैं।

RISKS AND FEW PREVENTIVE MEASURE IN CYBER SPACE

- **Don't give your personal details of where abouts :**
  Don't post specific personal information online, such as travel dates, location and time of the movie you plan to watch, evening classes that you take etc.,

- **Friends:**
  Better avoid strangers as friends when requests are received.

- **Don't share your personal information** and profile information Irrespective of gender as they may post abusive/indecent messages when the relations are strained with them.

निम्नलिखित जोखिमों से अवगत रहें / Be aware of following risks

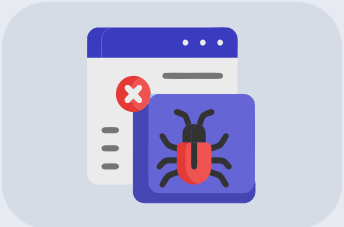
स्पैम:
जैसा कि हम सभी जानते हैं कि स्पैम आमतौर पर ई-मेल की सूची या ई-मेल पते के समूह को उत्पाद के विज्ञापन के बारे में भेजे जाने वाले अवांछित ई-मेल विज्ञापन होते हैं। इसी तरह से स्पैमर्स सोशल नेटवर्किंग साइट्स के अरबों उपयोगकर्ताओं को ऐसे अवांछित मेल या संदेश भेज रहे हैं जो मुफ़्त हैं।

Spam:
As we all know that spam is usually unwanted e-mail advertising about a product sent to list of e-mails or group of e-mail addresses. Similarly spammers are sending the unwanted mails or messages to the billions of users of social networking sites which are free.

स्कैमस (घोटाले) :
ऑनलाइन स्कैमर आमतौर पर उपयोगकर्ता को एक लिंक के साथ ऐसा ईमेल या संदेश भेजते हैं जिस पर प्रोफ़ाइल की जानकारी माँगी जाती है और उपयोगकर्ता को बताया जाता है कि नए फोलोअर्स को जोड़ दिया जाएगा। उपयोगकर्ता को भेजे गए ये लिंक एप्लिकेशन, गेम आदि के समान होंगे। इसलिए जब भी उपयोगकर्ता लिंक में अपना विवरण पोस्ट करेगा तो वह विवरण स्कैमर्स को प्राप्त होगा और जानकारी का दुरुपयोग किया जाएगा।

Scams:
Online scammers generally send an email or message with a link to the user which ask for the profile information and tell the user that it would add new followers. These links sent to the user would be similar to applications, games etc. So whenever the user post his details in the link then the details will be received by scammers and information would be misused.

दुर्भावनापूर्ण एप्लिकेशन:
सॉफ़्टवेयर का उपयोग करते या इंस्टॉल करते समय अथवा सोशल नेटवर्किंग संदेशों आदि पर क्लिक करते समय दुर्भावनापूर्ण एप्लिकेशन आ सकती है। एप्लिकेशन इंस्टॉलेशन प्रक्रिया शुरू कर सकती है या फोटो, वीडियो आदि देखने के लिए या लिंक दे सकती है। अपने इच्छित ऑपरेशन को अंजाम देने के लिए एप्लीकेशन उपयोगकर्ता से मेरी बुनियादी जानकारी तक पहुंच, मेरी वॉल पर अपडेट, मेरी वॉल पर पोस्ट करें आदि, जैसे कुछ उन्नत विशेषाधिकार के लिए आवेदन अनुरोध कर सकती है, जो दुर्भावनापूर्ण व्यवहार हैं।



Malicious application:
Malicious application might come through different application while using or installing software or by clicking on the social networking messages etc. The application may start the installation process or link to view the photo, video etc. In order to fulfil its intended operation the application requests for some elevated privileges from the user like access to my basic information, update on my wall, post on my wall, etc which are malicious behaviour.

क्लिकजैकिंग:

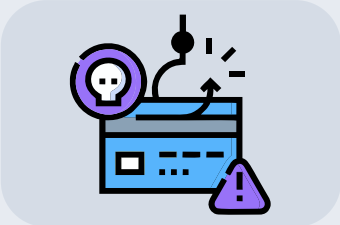
क्लिकजैकिंग वेब उपयोगकर्ताओं अहानिकर ऑब्जेक्ट्स, वेब पेजेस पर क्लिक करते समय उनकी गोपनीय जानकारी प्रकट करने या उनके कंप्यूटर को नियंत्रण में लेने के लिए एक दुर्भावनापूर्ण तकनीक है। विभिन्न ब्राउज़रों और प्लेटफ़ॉर्मों पर भेद्यता के कारण क्लिकजैकिंग, एक एम्बेडेड कोड या स्क्रिप्ट का रूप लेती है जो उपयोगकर्ता की जानकारी के बिना चल सकती है। सोशल नेटवर्किंग डोमेन में इसका अनुसरण किया जाता है। इस तरह के हमले के पीछे उद्देश्य यह होता है कि उपयोगकर्ताओं को लिंक, आइकन, बटन आदि पर क्लिक करने के लिए उकसाया जा सकता है, जिससे उपयोगकर्ता की जानकारी के बिना पृष्ठभूमि में प्रक्रियाओं का चलन हो सकता है।

Clickjacking:

Clickjacking is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous objects, Web pages. Vulnera-bility across a variety of browsers and platforms, a clickjacking takes the form of embedded code or script that can run without the user's knowl-edge. The same is followed in the social networking domain. The objective behind such an attack is that users can be tricked into clicking in the links, icons, buttons etc., which could trigger running of processes at the background without the knowledge of the user.

फ़िशिंग:

जैसा कि हम सभी जानते हैं कि फ़िशिंग अटैक/हमला मूल साइट के समान ही नकली साइट का निर्माण है। इसी तरह इन दिनों फिशिंग बैंकों और लोकप्रिय ट्रेडिंग वेबसाइट्स पर फ़िशिंग हमलों की तरह ही सोशल नेटवर्किंग पर भी अलग-अलग रूप में आ गई है। सोशल नेटवर्किंग फ़िशिंग कुछ विशेष विषयों की पेशकश, प्रोफ़ाइल को अपडेट करने, सुरक्षा एप्लिकेशन / सुविधाओं को अपडेट करने आदि जैसे नकली मेल्स और संदेशों के साथ होती है। अपडेट्स देखने के लिए उपयोगकर्ता को एक लिंक को फ़ॉलो करने और लॉग -इन करने की आवश्यकता होती है, जिसके माध्यम से हमलावर द्वारा क्रेडेंशियल्स लिए जाते हैं। लिंक किया गया पेज मूल लॉगइन पेज की एक नकली प्रति होती है, जो उपयोगकर्ता के खाते के क्रेडेंशियल्स चुराने पर केंद्रित होती है।



Phishing:

As we all know the phishing attack is creation of fake site just similar to original site. Similarly these days even social networking phishing has come in different flavours just like phishing attacks on banks and popular trading websites. Social networking phishing has come up with fake mails and messages like offering some specialized themes, updating the profile, updating the security application/features etc. In order to see the updates the user needs to follow a link and log in, through which the credentials are taken by the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials.

क्या आपको लॉटरी के ई-मेल / एसएमएस मिल रहे हैं?

ARE YOU GETTING LOTTERY E-MAILS/SMS ?

- लॉटरी ईमेल / एसएमएस में अपराधी ई-मेल भेजता है या पीड़ित को कॉल करता है या सार्वजनिक रूप से यह बताते हुए एसएमएस भेजता है कि व्यक्तियों के सेल फोन नंबर लाखों रुपये की लॉटरी जीत गए हैं और एक ई-मेल आईडी देकर उन व्यक्तियों को सभी विवरण प्रस्तुत करने के लिए कहता है तथा हर व्यक्ति को अलग से सूचित कर कहता है कि वह इस मामले को किसी के सामने प्रकट न करें ।
- विक्टिम (शिकार हुआ व्यक्ति) सोचता है कि उसने लॉटरी के माध्यम से बड़ी राशि जीत ली और ई-मेल के माध्यम से सभी विवरण प्रस्तुत कर देता है ।
- जालसाज़ व्यक्ति पीड़ित के नाम पर जाली चेक / प्रमाण पत्र की स्कैन की हुई कॉपी भेजता है क्योंकि वह भेजने के लिए तैयार रखी होती है। कलप्रिट एक बैंक खाता संख्या प्रस्तुत करके पंजीकरण शुल्क के रूप में कुछ राशि जमा करने के लिए व्यक्ति को फिर से सूचित करता है।
- विक्टिम (पीड़ित) व्यक्ति भरोसा कर लेता है और कलप्रिट (अपराधी)द्वारा बताये गए विभिन्न बैंक खातों में पैसा जमा कर देता है और कभी-कभी पीड़ित व्यक्ति अलग अलग संख्याओं में लाखों रुपयों से अधिक राशि जमा कर सकता है।
- बाद में बड़ी मात्रा में धन खो देने के बाद पीड़ित व्यक्ति को पता चलता है कि उसे अलग-अलग नामों पर लॉटरी जैसे कि कौनबनेगा करोडपति, एयरटेल लॉटरी, आईसीसी लॉटरी, स्टार स्पोर्ट्स लॉटरी आदि, के नाम पर धोखा दिया गया है ।

- In the lottery emails/SMS the culprit sends e-mail or calls the victim or sends SMSs to public stating that the cell phone numbers of the individuals has won lottery in lakhs and furnishes an e-mail id and asks the individuals to furnish all details through e-mail and informs the individuals that he should not reveal the matter to anyone.
- Victim thinks that he won big amount through lottery and furnishes all the details through e-mail.
- The fraudster sends a scanned copy of forged cheque/certificate on the victim name as it is ready for dispatch. The culprit again informs the individual to deposit certain amount as registration fee by furnishing a fake bank account number.
- Victim believes and deposits money in different bank accounts as asked by culprit & victim may sometimes deposit more than lakhs in different amount numbers.
- Later after losing large amount of money the individual realize that he has been cheated on the name of lottery on different names KaunBanegaCrorepathi, Airtel Lottery, ICC Lottery, Star Sports lottery etc.,

लॉटरी घोटाला

कभी-कभी आपको इस तरह का एक ईमेल प्राप्त होता है कि "आपने 10 लाख डॉलर की लॉटरी जीती है"; इस तरह के मेल प्राप्त करना बहुत अच्छी बात है, और वास्तव में यह सबसे खुशी की बात है। इस तरह के मेल का जवाब देने से भारी मात्रा में धन की हानि हो जायेगी। क्योंकि ऐसे मेल झूठे होते हैं, ज़ाहिर है कि घोटालेबाज आपको पैसे प्राप्त करने के लिए बेवकूफ बनाने और फंसाने की कोशिश करते हैं

Lottery scam

Sometimes you receive an email like "you won a lottery of million dollars" receiving such a kind of mails is a great thing, and really it's a happiest thing. By responding to such a kind of mails huge amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money

इस तरह के ईमेल स्कैम – बधाई! आपने वेब कैमरा, डिजिटल कैमरा आदि जीता है।

कभी-कभी आपको इस तरह के संदेश के साथ एक ई-मेल मिलता है कि - आपने डिजिटल कैमरा, वेब कैमरा जैसे कुछ विशेष जीता है, बस आपको नीचे दिए गए लिंक पर क्लिक करके हमारी वेब साइट पर जाना होगा और डाक द्वारा भेजने तथा प्रबंधन के खर्च की पूर्ति के लिए अपना डेबिट या क्रेडिट कार्ड विवरण प्रदान करना होगा। हालांकि आइटम कभी नहीं आता है, लेकिन कुछ दिनों के बाद आपके बैंक खाते पर शुल्क दिखाए जाएंगे, और आप पैसे खो देंगे।

Email Scam Like -Congratulations you have won Webcam, Digital Camera, etc.

Sometimes you receive an email like "you won a lottery of million dollars" receiving such a kind of mails is a great thing, and really it's a happiest thing. By responding to such a kind of mails huge amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money

सावधानियां / Precautions

- ऑनलाइन लॉटरी या त्योहार पर भारी छूट के संबंध में अजनबियों से ई-मेल या मोबाइल पर एसएमएस प्राप्त होने पर कभी भी जवाब न दें।
- उचित पुष्टि के बिना अज्ञात खातों में कोई पैसा जमा न करें।
- जीती गयी लॉटरी की राशि की धोखाधड़ी किसी ऐसे बैंक खाता धारक की सुविधा के साथ की जाती है जिसे कमीशन दिया जाता है और जिसका धोखेबाज के साथ कोई संबंध नहीं होता है।
- स्कैमर्स और इस विषय के ई-मेल के चक्कर में न फंसें कि आपने $ 1000 जीते हैं। ज़रा यह सोचें कि आपकी भागीदारी के बिना ही केवल आपको ईमेल क्यों मिला।
- सीजनल सेल अवधि के दौरान रियायती मूल्य पर मिलने वाले उत्पादों के बारे में जागरूक रहें। विश्वसनीय वेबसाइट से ऑफ़र की पुष्टि करें। मेल / एसएमएस के माध्यम से भेजी गए ऐसे लिंक पर क्लिक न करें जो फ़िशिंग अटैक(हमले) का कारण बन सकती है।

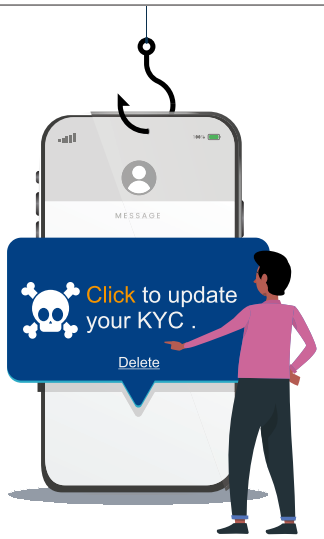
- Never respond to e-mail or SMS on mobile from strangers regarding online lottery or bumper festival bonanza.
- Don't deposit any money in unknown accounts without proper confirmation.
- The winning lottery amount is a fraud committed with convenience of a bank account holder who is paid commission and has no link with fraudster.
- Don't get trapped by scammers and e-Mails with a subject line you won some $10000 just think why only you received the email without your participation.
- Be aware about the products you get for a discounted price during seasonal sale period. Verify the offer from trusted website. Don't click on links send via mails/SMS which can cause phishing attack.

शिकायत कैसे करें

- संबंधित बैंक से पिछले छह महीने के बैंक स्टेटमेंट प्राप्त करें ।
- कथित लेनदेन से संबंधित प्राप्त एसएमएस की एक प्रति बनाएँ।
- बैंक रिकॉर्ड में दिखाए अनुसार अपने आईडी प्रूफ और एड्रेस प्रूफ की कॉपी लगाएं।
- अपने नजदीकी पुलिस स्टेशन में शिकायत दर्ज करें, जिसमें उपरोक्त दस्तावेजों के साथ पूरी घटना का स्पष्ट विवरण किया गया हो।

How to make a compliant

- Collect Bank statement from the concerned bank of last six months.
- Make a copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.
- Lodge a complaint in your nearest Police Station explaining complete incident along with the above mentioned documents.



सतर्क रहें, विशिंग प्रक्रिया में न फंसें

Stay cautious don't get caught in the Vishing process

अपने डेटा को सावधानी से सहेजें, बैक अप लें ताकि वो हमेशा सुरक्षित रहै

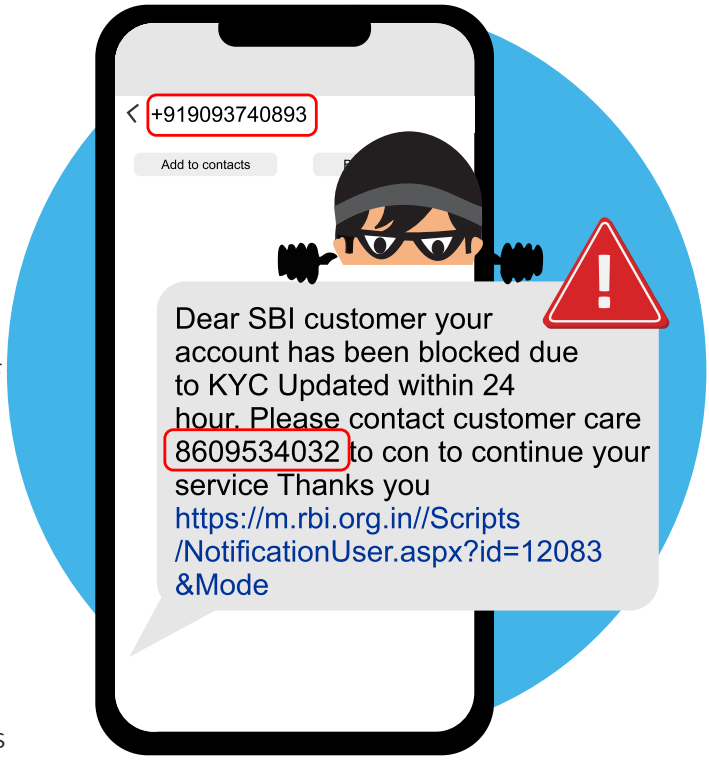
Save your data with care backup to ensure it's always there

अपने ग्राहक को जानें (KYC) धोखाधड़ी

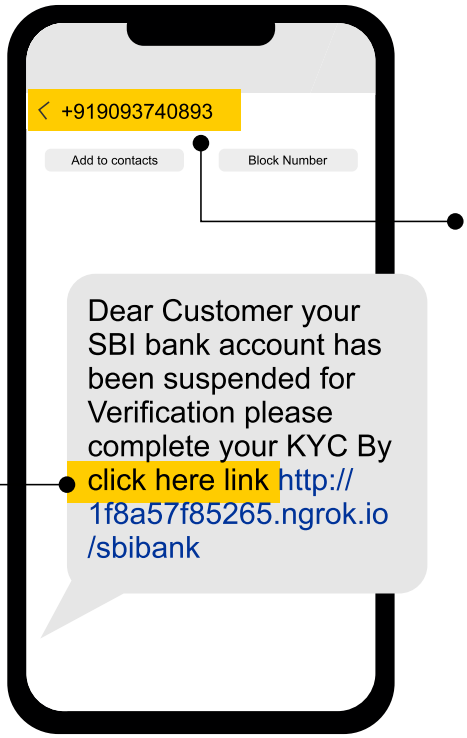
बैंकिंग ग्राहकों को जाली एसएमएस परिचालित किए जा रहे हैं जिनमें उन्हें केवाईसी नवीनीकरण/अद्यतन लंबित होने के कारण खाता निलंबन/ब्लॉक के बारे में संचारित किया जा रहा है। जालसाज वित्तीय घोटाला करने के लिए केवाईसी नवीनीकरण/अपडेट के लिए संदेश में फिशिंग लिंक या नकली संपर्क नंबर प्रदान करते हैं।

KNOW YOUR CUSTOMER (KYC) FRAUDS

Fake SMS(s) are being circulated, to the banking customers alerting them about the account suspension/ block due to pending KYC renewal/update. The fraudsters provide phishing link or fake contact numbers in the message for KYC renewal/update to commit financial scam.



चेतावनी के संकेत / Warning Signs



प्राप्त संदेश में खराब व्याकरण, विराम चिह्न और शब्दों का अवांछित कैपिटलाइजेशन।

Poor grammar, unctuation and unwanted capitalization of words in the message received.

अधिकृत बैंकिंग कस्टमर केयर/ सर्विस नंबर के बजाय मोबाइल नंबर से भेजा गया संदेश।

Message sent from a mobile number instead of the authorized banking customer care / service number.

सुरक्षा उपाय / Security Measures

अनजान स्रोत लिंक या असत्यापित से प्राप्त लिंक पर कभी क्लिक न करें ।

Never click on unknown links or links received from unverified sources

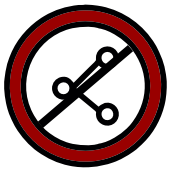
हमेशा याद रखें - कोई बैंक केवाईसी अपडेट करने के लिए अपने ग्राहकों को कभी कोई लिंक नहीं भेजता है ।

Always remember that a bank never sends any links to its customers, for updating KYC

एक वैध कस्टमर केयर नंबर कभी भी 10 अंकों का मोबाइल नंबर नहीं हो सकता है जैसा कि आमतौर पर नकली संदेश में दिया जाता है।

A valid customer care number can never be a 10 digit mobile number as generally given in the fake message.

अपना मोबाइल संख्या, खाता संख्या, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय विवरण किसी के साथ कभी साझा न करें ।



Never share your mobile number, account number, password, OTP, PIN or any other confidential details with anyone

कोई भी अधिकृत बैंक या ग्राहक सेवा कभी भी अपने ग्राहकों से कोई गोपनीय जानकारी साझा करने के लिए नहीं कहती है

Any authorized bank or customer service never asks its customers to share any confidential information

Google खोज पर प्रदान की गई ग्राहक सेवा/संपर्क नंबरों से संपर्क करने से बचें। केवल मूल बैंकिंग वेबसाइटों में दिए गए अधिकृत नंबरों से संपर्क करें।

Avoid contacting the customer service/contact numbers provided on Google search. Only contact the authorized numbers provided in original banking websites.

किसी भी समस्या के मामले में तुरंत संबंधित बैंक अधिकारियों को तुरंत रिपोर्ट करें।

In case of any such issues immediately report to the specific bank authorities immediately.

ऐसी किसी भी धोखाधड़ी के बारे में सरकारी पोर्टल पर ऑनलाइन शिकायत दर्ज करें www.cybercrime.gov.in

File an online complaint regarding any such frauds on the government portal www.cybercrime.gov.in

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सी-डैक CDAC

जॉब स्कैमर्स के पास अपना कीमती समय न गवाँए , असली जॉब ऑफर मे पैसे कभी नहीं माँगते ।

Don't let job scammers take your time Genuine job offers don't ask for a dime!

Supported by

certin Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

mygov मेरी सरकार

CYBER DOST

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

सत्यमेव जयते
Ministry of Electronics & Information Technology, Government of India

Information Security Education & Awareness
www.isea.gov.in
www.staysafeonline.in

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Join our WhatsApp and Telegram Channel at

ISEA - Digital Naagrik

To Share Tips / Latest News, mail us to

isea@cdac.in

Social Media Presence

National Cybercrime Helpline No. 1930

www.cybercrime.gov.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)

www.cdac.in