PAN : AAMCT6464C | TAN : JDHT04845B
SECTION 8 LICENCE NUMBER : 177777
WEB : TECHLEGALAWARENESS.IN

DARPAN ID : RJ/2026/0949291

CIN : U88900RJ2026NPL110256
DIN : 11459970

TECH LEGAL AWARENESS FORUM

A NON-PROFIT SECTION 8 ORGANIZATION

SCAM FREE INDIA

CYBER ALERT

- **LEGAL ASSISTANCE**: DRAFTING COMPLAINTS, FIR GUIDANCE, RTI HELP, AND CONNECTING VICTIMS WITH VERIFIED ADVOCATES.
- **CYBER AWARENESS:** CAMPAIGNS ON OTP FRAUD, FAKE JOB SCAMS, CRYPTO & STOCK MARKET TRAPS, AND AI-BASED PHISHING.
- **TRAINING & EDUCATION**: DIGITAL WORKSHOPS, MOCK AWARENESS DRIVES, AND SCHOOL/COLLEGE EVENTS ON ONLINE SAFETY.
- **SOCIAL JUSTICE:** HELPING THE POOR AND DIGITALLY UNEDUCATED CITIZENS PROTECT THEIR RIGHTS IN THE MODERN ERA.

"To empower citizens with legal knowledge and digital awareness, and to support victims of cyber and financial crimes through education, guidance, and lawful action."

ADD : SH. NO.-3, NEAR SAMUDAYIK, BHAWAN, KUNHADI, GIRDHARPURA, KOTA- 324008, RAJASTHAN, INDIA

Present by :

TECH LEGAL AWARENESS FORUM

A SECTION 8 NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

साइबर अपराध जागरूकता

Stay Safe | Stay Smart

Cyber Alert

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

साइबर अपराध क्या है?

साइबर अपराध उन आपराधिक गतिविधियों को कहते हैं जिनमें कंप्यूटर, मोबाइल फोन, डिजिटल उपकरण या इंटरनेट का उपयोग होता है।

ये अपराध व्यक्ति, संस्था या सरकार को निशाना बना सकते हैं।

इनमें डेटा चोरी, धन की ठगी, सिस्टम हैकिंग और ऑनलाइन धोखाधड़ी शामिल है।

भारत में डिजिटल विकास के साथ साइबर अपराध तेज़ी से बढ़ रहे हैं।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

विभिन्न प्रकार के साइबर अपराध

- डिजिटल अरेस्ट
- इन्वेस्टमेंट स्कैम
- केवाईसी स्कैम
- साइबर गुलामी
- एपीके स्कैम
- ऑनलाइन जॉब स्कैम
- ऑनलाइन शॉपिंग फ्रॉड
- ऑनलाइन गेमिंग फ्रॉड
- सोशल मीडिया इम्पर्सोनेशन
- स्पैम / फिशिंग कॉल
- रैनसमवेयर
- डीपफेक साइबर क्राइम
- लॉटरी फ्रॉड
- डीपफेक साइबर क्राइम
- लॉटरी फ्रॉड

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA
CYBER ALERT

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते

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

डिजिटल अरेस्ट से सावधान

कैसे होता है यह अपराध ?

- फ़ोन कॉल के ज़रिए आपके नाम से नकली पार्सल में अवैध सामान या अन्य अवैध गतिविधियों में संलिप्त होने के नाम से डराया जाता है
- नकली पुलिस अधिकारी आपको वीडियो कॉल पर बने रहने के लिए बाध्य करते हैं।
- डराकर आपसे पैसे वसूले जाते हैं या प्रताड़ित किया जाता है।

वीडियो कॉल करने वाले ये लोग पुलिस, CBI, कस्टम अधिकारी या जज नहीं,

बल्कि साइबर अपराधी होते हैं

इनसे डरे नहीं, इनकी रिपोर्ट करें

1930 पर कॉल करें या

www.cybercrime.gov.in पर शिकायत दर्ज करें

रुको • सोचो • एक्शन लो

अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA CYBER ALERT

Top Cybersecurity Threats in 2026

स्लाइड 5 : डिजिटल अरेस्ट – क्या है?

वीडियो कॉल के ज़रिये गिरफ्तारी का झांसा देना खुद को पुलिस / CBI / जज बताना डर दिखाकर पैसे ऐंठना

Do’s (क्या करें)

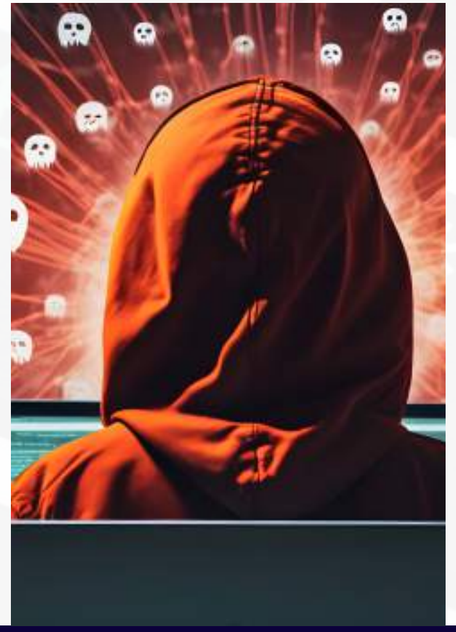
- तथ्यों को जानें : पुलिस या सरकारी अधिकारी कभी भी वीडियो कॉल के माध्यम से गिरफ्तारी या पूछताछ नहीं करते हैं।
- व्यक्तिगत जानकारी साझा न करें : कोई भी अधिकारी वीडियो कॉल के माध्यम से पैसे या व्यक्तिगत विवरण नहीं मांगता।
- कानून को समझें : भारत में डिजिटल गिरफ्तारी जैसी कोई कानूनी प्रक्रिया नहीं है।

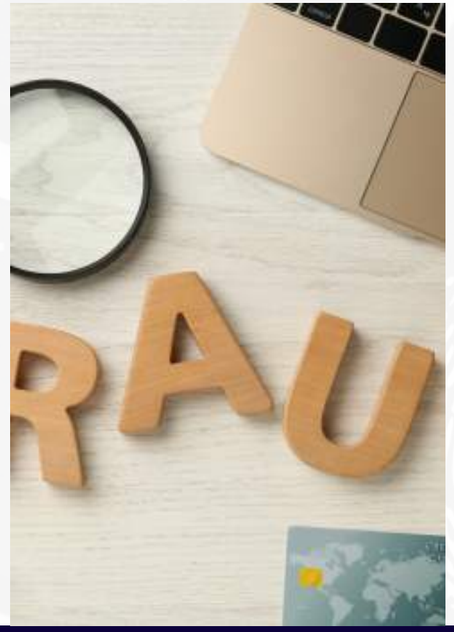
TECH LEGAL AWARENESS FORUM

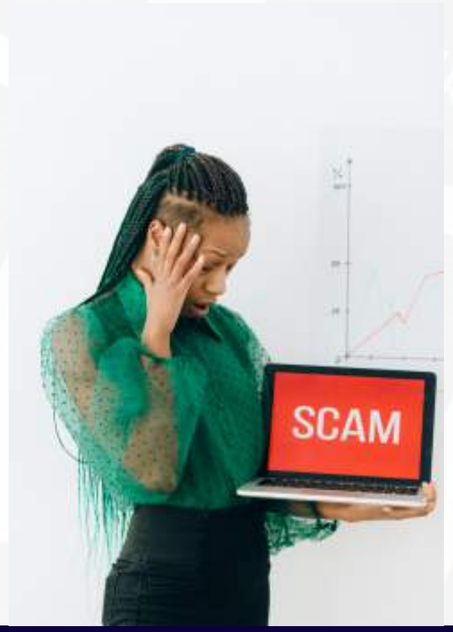
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA CYBER ALERT

Top Cybersecurity Threats in 2026







Don’ts (क्या न करें)

- धोखेबाजों के झांसे में न आएँ : यदि कोई वीडियो कॉल के जरिए आप पर दबाव डालता है, तो पैसे न भेजें।
- ज्यादा देर तक बातचीत न करें : संदिग्ध लगने वाले लंबे वीडियो कॉल में फँसने से बचें।
- बिना पुष्टि किए कॉल पर भरोसा न करें : सरकारी अधिकारी बनकर पैसे मांगने का दावा करने वाले किसी भी वीडियो कॉल को नज़रअंदाज़ करें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

आपका पैसा

ही उनका निशाना है!

जानने के लिए स्वाइप करें...

Follow @CyberDost for real cybercrime awareness tips

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

ILLUSION OF GUARANTEED PROFITS

www.cybercrime.gov.in

CALL 1930 FOR ANY CYBERCRIME

Follow @CyberDost for real cybercrime awareness tips

इन्वेस्टमेंट स्कैम – Investment Scam

इसमें धोखाधड़ी वाली योजनाएँ शामिल होती हैं, जो उच्च रिटर्न का वादा करती हैं।

ये योजनाएँ अक्सर सच होने से भी ज़्यादा आकर्षक दिखाई देती हैं।

Do’s (क्या करें)

• पंजीकृत संस्थाओं के साथ निवेश करें।

• निवेश उत्पादों की पुष्टि करें – योजना, कंपनी और दस्तावेज़ों की जाँच करें। • सूचित रहें : विनियमित संस्थाओं और वित्तीय उत्पादों से जुड़ी विश्वसनीय सूचना स्रोतों का पालन करें।

Don’ts (क्या न करें)

• घबराएँ नहीं : शांत रहें और किसी भी ऑफ़र की पहले पूरी पुष्टि करें।

• अविश्वसनीय और बिना किसी जोखिम वाले रिटर्न पर भरोसा न करें।

• संदिग्ध ट्रेडिंग ऐप्स या उनका प्रचार करने वाले सोशल मीडिया ग्रुप से दूर रहें।

• खतरे की घंटी को नज़रअंदाज़ न करें : यदि रिटर्न समय के साथ बहुत ज़्यादा या असामान्य लग रहा हो, तो सतर्क रहें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

एक दिन आया उसको अंजान कॉल, कहा KYC अपडेट करो नहीं तो अकाउंट होगा ब्लॉक

अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

केवाईसी स्कैम – KYC Scam

साइबर अपराधी पहचान सत्यापन (KYC) प्रक्रियाओं का दुरुपयोग करके व्यक्तिगत जानकारी चुराते हैं, पहचान की चोरी करते हैं या वित्तीय खातों तक अवैध रूप से पहुँच बना लेते हैं।

Do’s (क्या करें)

• अनुरोधों की पुष्टि करें : किसी भी KYC अपडेट अनुरोध की पुष्टि के लिए सीधे अपने बैंक या वित्तीय संस्था से संपर्क करें।

• घटनाओं की रिपोर्ट करें : यदि आपको किसी साइबर धोखाधड़ी का संदेह हो, तो तुरंत अपने बैंक या वित्तीय संस्था को सूचित करें।

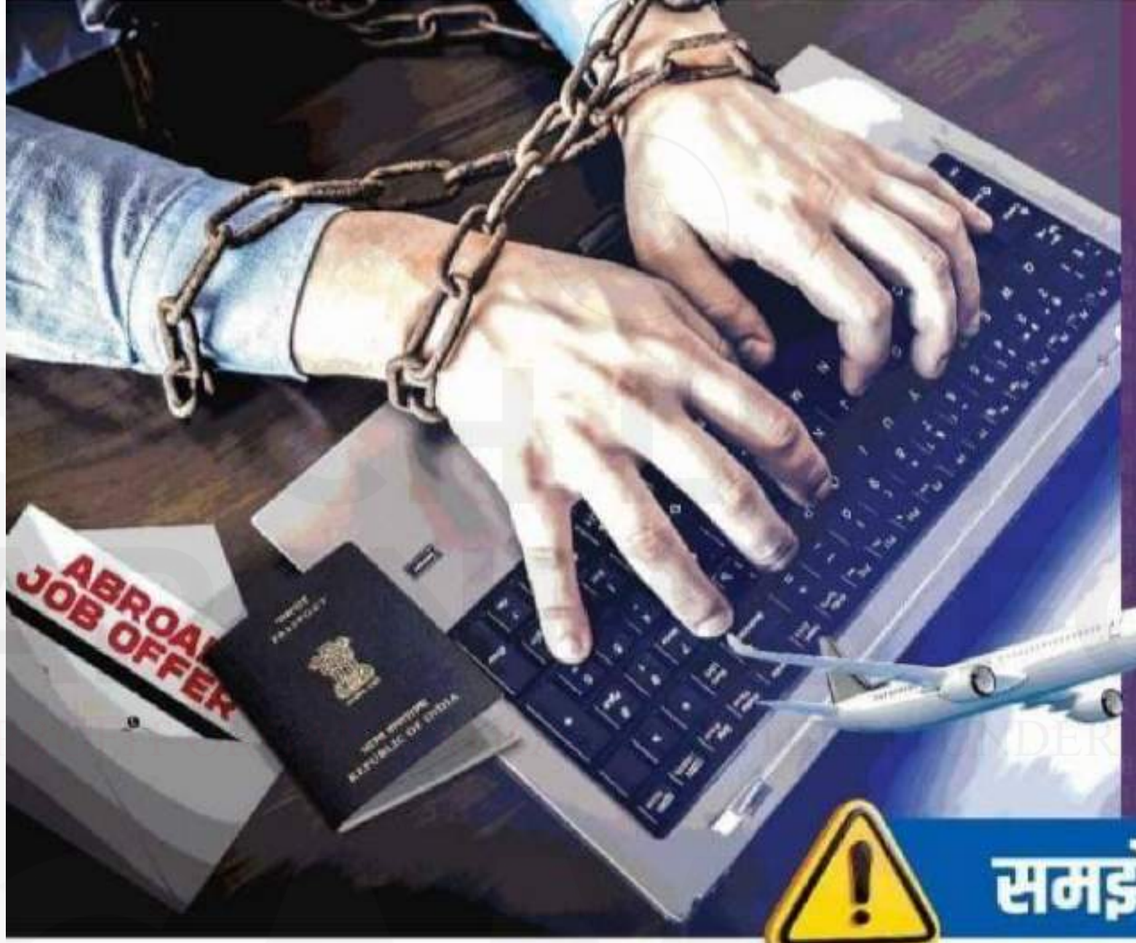
Don’ts (क्या न करें)

• क्रेडेंशियल्स की सुरक्षा करें : अपने खाते के लॉग-इन विवरण, कार्ड की जानकारी, PIN, पासवर्ड या OTP कभी भी किसी के साथ या अनधिकृत वेबसाइट/ऐप पर साझा न करें।

• संदिग्ध लिंक से बचें : मोबाइल या ई-मेल के माध्यम से प्राप्त संदिग्ध या असत्यापित लिंक पर क्लिक न करें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

दक्षिण-पूर्व एशियाई देशों से जॉब ऑफर हो सकता है

साइबर स्लेवरी का धोखा !

समझें कैसे होती है साइबर स्लेवरी:

धोखेबाज एजेंट झूठे वादे करते हैं और नौकरी एवं वीजा का लालच देते हैं।

पीड़ितों को दक्षिण-पूर्व एशियाई देशों में तस्करी करके ले जाया जाता है।

पीड़ितों को साइबर अपराध करने के लिए मजबूर किया जाता है, उनको अमानवीय परिस्थितियों में रख कर उनके साथ अत्याचार किया जाता है।

ध्यान रहें: जॉब ऑफर को ध्यान से जांचें। केवल सरकार द्वारा अधिकृत एजेंटों पर भरोसा करें।

रुको | सोचो | एक्शन लो

ऐसे ग्रुप्स या ईमेल की www.cybercrime.gov.in या **1930** पर कॉल करके रिपोर्ट करें।

अधिक जानकारी के लिए CyberDost को फॉलो करें।

CBC 19101/13/2022/6425

SCAM FREE INDIA
CYBER ALERT

साइबर गुलामी – Cyber Slavery

व्यक्तियों को विदेश में अच्छी नौकरी का झांसा देकर बंधक बनाया जाता है और वहाँ उन्हें साइबर अपराध करने के लिए मजबूर किया जाता है।

यह मुद्दा मानव तस्करी से भी जुड़ा हुआ है।

Do’s (क्या करें)

- सत्यापित एजेंटों के माध्यम से विदेश जाने हेतु आवेदन करें और नौकरी के प्रस्तावों की पुष्टि करें।
- “बहुत अच्छी” नौकरियों से सावधान रहें – जो ऑफर अवास्तविक लगें, उनकी जाँच करें।
- विदेश भेजने वाले नियोक्ताओं पर शोध करें – कंपनी, पता और दस्तावेज़ों की पुष्टि करें।

Don’ts (क्या न करें)

- झटपट मिलने वाले ऑफर से बचें।
- काम के लिए कभी भी टूरिस्ट वीज़ा का इस्तेमाल न करें।
- सोशल मीडिया पर अनजान लोगों या समूहों के विज्ञापनों या ऑफर पर भरोसा न करें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

झूठे ऐप्स के बारे में सतर्क रहें

शीघ्र उच्च रिटर्न/ लाभ की पेशकश करने वाले, धन कमाने वाले संदिग्ध ऐप्स इंस्टॉल करने और इनके जरिए निवेश करने से बचें

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Indian Cyber Crime Coordination Centre

Don't Download

"Jio internet speed 5G network connection.apk" file

It can APK hack your phone

FOR MORE INFO, FOLLOW CYBERDOST ON

एपीके स्कैम – Mobile Application APK Scam

असली ऐप से मिलते-जुलते फर्जी ऐप थर्ड-पार्टी ऐप स्टोर या फिशिंग लिंक जैसे अनधिकृत माध्यमों से वितरित किए जाते हैं। एक बार इंस्टॉल हो जाने पर ये ऐप आपके बैंकिंग क्रेडेंशियल और व्यक्तिगत डेटा चुरा लेते हैं।

Do's (क्या करें)

• आधिकारिक स्टोर से डाउनलोड करें : ऐप हमेशा Google Play Store / Apple App Store या बैंक की आधिकारिक वेबसाइट जैसे विश्वसनीय स्रोतों से ही डाउनलोड करें।

• फोन का ऑपरेटिंग सिस्टम सॉफ़्टवेयर अपडेट रखें।

• दो-कारक प्रमाणीकरण (2FA) सक्षम रखें।

Don'ts (क्या न करें)

• अनधिकृत लिंक से ऐप डाउनलोड न करें।

• अज्ञात ऐप में संवेदनशील / बैंकिंग जानकारी दर्ज न करें।

• अपने डिवाइस को रूट / जेलब्रेक न करें।

• क्रेडेंशियल साझा न करें : अपना बैंकिंग PIN या OTP कभी भी किसी के साथ साझा न करें, भले ही वे सहायक कर्मचारी होने का दावा करें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Indian Cyber Crime Coordination Centre

डरो नहीं रिपोर्ट करो

संकेत

बिना आवेदन किए
नौकरी का ऑफर आना

कंपनी की
ऑनलाइन जानकारी न होना

अनुभव के बिना
अधिक वेतन मिलना

सुरक्षित रहें

जवाब देने से पहले
जांच करें

नौकरी पाने के लिए
कभी पैसे न दें

स्कैम हो जाए तो **1930** या
cybercrime.gov.in पर रिपोर्ट करें

SCAM FREE INDIA
CYBER ALERT

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

ऑनलाइन जॉब स्कैम – Online Job Scam

नौकरी की तलाश कर रहे लोगों को ठगा जाता है। साइबर अपराधी वेबसाइटों, सोशल मीडिया या ई-मेल के माध्यम से नकली नौकरियों के विज्ञापन देते हैं और ज़्यादा वेतन व आसान काम का लालच देते हैं।

Do's (क्या करें)

• विश्वसनीय स्रोतों का उपयोग करें : प्रमाणिक निजी और सरकारी नौकरी लिस्टिंग के लिए समाचार पत्रों, जॉब पोर्टल्स या सरकारी पोर्टल्स का संदर्भ लें।

• ई-मेल सत्यापित करें : ऐसे ई-मेल पतों पर ध्यान दें जो वास्तविक कंपनियों की नकल करते हों।

Don'ts (क्या न करें)

• क्रेडेंशियल्स की सुरक्षा करें : अपने खाते के लॉग-इन विवरण, कार्ड की जानकारी, PIN, पासवर्ड या OTP कभी भी किसी के साथ या अनधिकृत वेबसाइट/ऐप पर साझा न करें।

• संदिग्ध लिंक से बचें : मोबाइल या ई-मेल के माध्यम से प्राप्त संदिग्ध या असत्यापित लिंक पर क्लिक न करें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

इस नवरात्रि शॉपिंग,

ध्यान रखें इन बातों का..

- खरीदारी करने से पहले साइट की स्पेलिंग और URL देखें।
- "Too good to be true" ऑफ़र्स अक्सर धोखा होते हैं।
- सिर्फ़ सुरक्षित और भरोसेमंद पेमेंट गेटवे/UPI ऐप का इस्तेमाल करें।
- किसी भी लिंक पर बिना जांचे-परखे क्लिक न करें।

Follow @CyberDost for real cybercrime awareness tips

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

ऑनलाइन सामानों की खरीद - बिक्री में धोखाधड़ी से सावधान रहें!

याद रहे, हमेशा पूरी जानकारी एकत्र करें, विक्रेताओं से व्यक्तिगत रूप से मिलें, और किसी भी लेन-देन से पहले उत्पाद की जाँच करें। ऑनलाइन धोखाधड़ी से सुरक्षित रहें!

1. QR कोड धोखाधड़ी
2. अग्रिम भुगतान
3. नकली पहचान
4. नकली उत्पाद

FOR ANY CYBER CRIME COMPLAINT REPORT TO : https://cybercrime.gov.in

In case of online financial fraud DIAL 1930

FOLLOW US ON :

ऑनलाइन शॉपिंग फ्रॉड – Online Shopping Fraud

साइबर अपराधी पीड़ितों को अवैध खरीदारी करने के लिए धोखा देते हैं। वे नकली वेबसाइट बनाते हैं या वैध प्लेटफॉर्म पर हैकिंग/हेरफेर करते हैं, ऐसे सौदे पेश करते हैं जो सच होने से बहुत दूर होते हैं और व्यक्तिगत व वित्तीय जानकारी चुरा लेते हैं।

Do's (क्या करें)

- कीमतों की तुलना करें : विभिन्न ई-कॉमर्स वेबसाइटों पर कीमतों की तुलना करें।
- संदेह होने पर कैश-ऑन-डिलीवरी चुनें : यदि कोई वेबसाइट संदिग्ध लगे, तो कैश-ऑन-डिलीवरी भुगतान विधि चुनें।
- विश्वसनीय विक्रेताओं से खरीदारी करें : ई-कॉमर्स वेबसाइटों पर सत्यापित या भरोसेमंद विक्रेताओं से ही खरीदारी करना पसंद करें।

Don'ts (क्या न करें)

- सार्वजनिक नेटवर्क से बचें : सार्वजनिक कंप्यूटर या नेटवर्क का उपयोग करके ई-शॉपिंग लेनदेन न करें।
- अपनी जानकारी सुरक्षित रखें : अपने कार्ड का विवरण, जन्मतिथि, फोन नंबर आदि अविश्वसनीय ई-शॉपिंग वेबसाइटों पर सेव न करें।
- ऑफ़र और विक्रेताओं का सत्यापन करें : बहुत ज़्यादा सस्ते या अवास्तविक ऑफ़र देने वाले विक्रेताओं से सावधान रहें।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

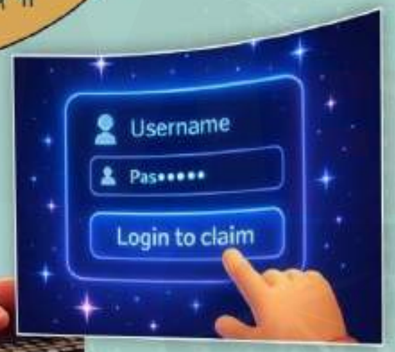
#CYBER SAFESUMMER

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

खुल गई एक चमकदार वेबसाइट

LOGIN करो और अपना **REWARD** लो!

मन्नू ने तुरंत अपना **USERNAME** और **PASSWORD** डाल दिया



अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

#CYBER SAFESUMMER

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

कभी भी अनजान लिंक पर

क्लिक न करें

अपनी गेम ID/पासवर्ड किसी से

साझा न करें

केवल ऑफिशियल वेबसाइट या ऐप से

ही लॉगिन करें

अगर स्कैम हो जाए, तो

1930 पर कॉल करें या

cybercrime.gov.in पर रिपोर्ट करें

अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

ऑनलाइन गेमिंग फ्रॉड – Online Gaming Fraud

साइबर अपराधी गेमिंग प्लेटफॉर्म की कमियों का फायदा उठाते हैं और फिशिंग स्कैम, मैलवेयर और सोशल इंजीनियरिंग के ज़रिए खिलाड़ियों को निशाना बनाते हैं।

Do's (क्या करें)

- यदि आप अभिभावक हैं, तो बच्चों की ऑनलाइन गेम्स तक पहुँच निगरानी में ही प्रदान करें।
- कई गेमिंग ऐप्स धोखाधड़ी वाले हो सकते हैं – सतर्क रहें और संदिग्ध लगने वाले ऐप्स से बचें।
- ऐप अनुमतियों का विवेकपूर्ण उपयोग करें : किसी ऐप को संपर्क, संग्रहण और स्थान जैसी अनुमतियाँ देने से पहले सावधानी बरतें।

Don'ts (क्या न करें)

- संदिग्ध या अविश्वसनीय स्रोतों से गेमिंग ऐप डाउनलोड न करें।
- सुनिश्चित रिटर्न या जीत का वादा करने वाले गेमिंग ऐप्स से सावधान रहें।
- अनजान साथी खिलाड़ियों के साथ गोपनीय या व्यक्तिगत जानकारी साझा न करें।
- सोशल मीडिया पर शेयरिंग सीमित रखें : अपनी गेमिंग उपलब्धियों को सोशल मीडिया पर अत्यधिक साझा करने से बचें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

सावधान! Video Call के जरिए लोगों को निशाना बना रहे हैं स्कैमर्स।

स्कैमर्स वीडियो कॉल के माध्यम से लोगों की आपतिजनक प्रतिक्रिया को रिकॉर्ड करके ब्लैकमैल करते हैं और फिर उस वीडियो को सोशल मीडिया पर पोस्ट करने की धमकी देकर वक्ति से मोटी रकम वसूल लेते है।

FOR ANY CYBER CRIME COMPLAINT REPORT TO : https://cybercrime.gov.in

In case of online financial fraud DIAL 1930

FOLLOW US ON :

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

सोशल मीडिया पर फर्जी पहचान – Social Media Impersonation

किसी वास्तविक व्यक्ति या संगठन की पहचान की नकल करके चोरी, वित्तीय धोखाधड़ी, प्रतिष्ठा को नुकसान पहुँचाया जाता है और झूठी/भ्रामक जानकारी का प्रसार किया जाता है।

Do's (क्या करें)

• खातों को सत्यापित करें : प्रामाणिकता की पुष्टि के लिए नीला चेकमार्क, एक-जैसे उपयोगकर्ता नाम और परिचित प्रोफ़ाइल चित्र देखें।

• सावधान रहें : अनचाहे संदेशों से बचें और कभी भी व्यक्तिगत जानकारी साझा न करें या संदिग्ध लिंक पर क्लिक न करें।

• प्रतिरूपण (Impersonation) की रिपोर्ट करें : संबंधित प्लेटफ़ॉर्म और उस वास्तविक व्यक्ति/संगठन को सूचित करें जिसकी पहचान की नकल की जा रही है।

Don'ts (क्या न करें)

• धन अनुरोधों की पुष्टि करें : फोन कॉल या व्यक्तिगत रूप से मिलकर दोस्तों/रिश्तेदारों से धन अनुरोधों की पुष्टि किए बिना भुगतान न करें।

• भुगतान न करें : अज्ञात व्यक्तियों या अविश्वसनीय/असत्यापित चैरिटी को ऑनलाइन भुगतान करने से बचें।

• जानकारी निजी रखें : सोशल मीडिया पर कभी भी व्यक्तिगत या गोपनीय जानकारी साझा न करें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

स्पैम / फिशिंग कॉल – Spam / Phishing Calls

• साइबर अपराधी सोशल इंजीनियरिंग का इस्तेमाल करके पीड़ितों से व्यक्तिगत या वित्तीय जानकारी जैसी संवेदनशील जानकारी निकलवाते हैं।

• विश्वास जीतने और जानकारी चुराने के लिए कॉलर आईडी स्पूफिंग और तत्कालता (Urgency) जैसी रणनीतियों का उपयोग करते हैं।

Do's (क्या करें)

• स्पैम कॉल्स की रिपोर्ट करें।

• सावधान रहें : अनजान नंबरों से आने वाली कॉल्स का जवाब देते समय सावधानी बरतें।

• जागरूकता फैलाएँ : आम फोन स्कैम के बारे में दूसरों को शिक्षित करें।

• सुरक्षा सक्षम करें : अतिरिक्त सुरक्षा के लिए वॉइसमेल पासवर्ड का उपयोग करें।

Don'ts (क्या न करें)

• निजी जानकारी साझा न करें : अनजान कॉल करने वालों को कभी भी अपनी निजी या वित्तीय जानकारी न दें।

• अनजान नंबरों से बचें : अपरिचित या अंतरराष्ट्रीय नंबरों से आने वाली कॉल का जवाब न दें।

• अपना डेटा सुरक्षित रखें : असली संस्थान कभी भी यूज़रनेम, पासवर्ड या OTP जैसी संवेदनशील जानकारी नहीं मांगते— इन्हें कभी भी साझा न करें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Indian Cyber Crime Coordination Centre

#RansomAware

रैंसमवेयर अटैक

कैसे होता है?

फर्जी ईमेल
फिशिंग लिंक/अटैचमेंट से डेटा चोरी

इन्फेक्टेड वेबसाइट्स
बिना बताए मैलवेयर डाउनलोड

कमज़ोर सर्वर
हैकर्स आसानी से
आपके सिस्टम में घुस सकते हैं

ऑनलाइन विज्ञापन
भरोसेमंद वेबसाइट्स पर भी छिपे
मैलिशियस कोड से हमला हो सकता है

अनजान लिंक पर क्लिक न करें

रैंसमवेयर अटैक को तुरंत रिपोर्ट करें: 1930 या cybercrime.gov.in पर

अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

रैनसमवेयर – Ransomware

यह एक प्रकार का दुर्भावनापूर्ण सॉफ़्टवेयर है, जो पीड़ित की फ़ाइलों को लॉक कर देता है और उन्हें एक्सेस करना असंभव बना देता है। इसके बाद हमलावर फ़ाइलों को अनलॉक करने की कुंजी के बदले फिरौती की मांग करते हैं।

Do's (क्या करें)

- डेटा की हानि से बचने के लिए नियमित रूप से बैकअप लें।
- सामग्री (फ़ाइल/ई-मेल) स्कैनिंग का उपयोग करें।
- सुरक्षा खामियों को दूर करने के लिए सिस्टम और सॉफ़्टवेयर अपडेट रखें।
- कर्मचारियों/उपयोगकर्ताओं को प्रशिक्षित करें ताकि वे फिशिंग प्रयासों और अन्य दुर्भावनापूर्ण गतिविधियों को पहचान सकें और उनसे बच सकें।

Don'ts (क्या न करें)

- फिरौती देने से बचें।
- व्यक्तिगत जानकारी सुरक्षित रखें : अपरिचित स्रोतों को कभी भी व्यक्तिगत जानकारी न दें।
- हमले को फैलने से रोकें : प्रभावित सिस्टम को तुरंत अलग (आइसोलेट) करें।
- हमले के दौरान बैकअप न चलाएँ : हमले के समय बैकअप न चलाएँ, क्योंकि वे भी लॉक हो सकते हैं।

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

डीपफेक साइबर क्राइम – Deepfake Cybercrime

आर्टिफिशियल इंटेलिजेंस (AI) का उपयोग करके वास्तविक फ़ुटेज या रिकॉर्डिंग में हेरफेर कर नकली वीडियो या ऑडियो क्लिप तैयार की जाती हैं, जिन्हें सोशल मीडिया, मैसेजिंग ऐप्स और ई-मेल के माध्यम से फैलाया जाता है।
अक्सर यह अपराध सार्वजनिक हस्तियों, मशहूर व्यक्तियों या उच्च पदस्थ लोगों को निशाना बनाकर किया जाता है।

Do's (क्या करें)

- सूचित रहें : डीपफेक तकनीक और उससे जुड़े जोखिमों के बारे में जानकारी रखें।
- सामग्री की पुष्टि करें : किसी भी मीडिया सामग्री को साझा करने या उस पर विश्वास करने से पहले उसकी प्रामाणिकता की जाँच अवश्य करें।
- विश्वसनीय स्रोतों का उपयोग करें : समाचारों और अपडेट के लिए प्रतिष्ठित व भरोसेमंद प्लेटफॉर्म पर ही भरोसा करें।
- संदिग्ध सामग्री की रिपोर्ट करें : यदि आपको संभावित डीपफेक सामग्री मिले, तो संबंधित प्लेटफॉर्म या अधिकारियों को सूचित करें।

Don'ts (क्या न करें)

- असत्यापित मीडिया साझा न करें : सत्यता की जाँच किए बिना किसी भी सामग्री को प्रसारित करने से बचें।
- संदिग्ध स्रोतों पर भरोसा न करें : ऐसे अविश्वसनीय स्रोतों से दूर रहें जो डीपफेक सामग्री साझा कर सकते हैं।
- आँख मूँदकर भरोसा न करें : अत्यधिक भावनात्मक या सनसनीखेज लगने वाली सामग्री से सावधान रहें।
- गोपनीयता की अनदेखी न करें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

ऑनलाइन लॉटरी फ़्राड

जालसाज फर्जी संदेश/ईमेल भेजते हैं जिसमें दावा किया जाता है कि पीड़ित ने बड़ी रकम की लॉटरी जीती है। पीड़ित के आश्वस्त होने के बाद, जालसाज लॉटरी को प्रोसैस करने के लिए पैसे मांगता है।

सुरक्षा टिप्स

- फर्जी लॉटरी जीतने से संबंधित कॉल/एसएमएस/ईमेल का कभी भी जवाब न दें
- व्यक्तिगत जानकारी साझा न करें
- उच्च रिटर्न की आशा में कभी भी अज्ञात व्यक्तियों या संस्थाओं को फंड ट्रांसफर न करें।

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

तुरंत कमाई का लालच देने वाले ऐसे ऐप्स से सावधान!

लॉटरी फ्रॉड – Lottery Fraud

साइबर अपराधी लोगों को यह विश्वास दिलाकर धोखा देते हैं कि उन्होंने कोई इनाम/लॉटरी जीत ली है, और फिर उनसे पैसे भेजने या अपनी निजी जानकारी साझा करने के लिए उकसाते हैं।

Do's (क्या करें)

- शुल्क न दें : धोखेबाज़ अक्सर नकली इनामों के लिए टैक्स, शिपिंग शुल्क या हैंडलिंग शुल्क की मांग करते हैं। किसी भी लॉटरी के लिए कभी भी पैसे न भेजें।
- अनचाहे दावों पर सवाल उठाएँ : अप्रत्याशित लॉटरी जीत के संदेशों या कॉल से सावधान रहें।
- धोखाधड़ी की रिपोर्ट करें : यदि आपको लॉटरी घोटाले का संदेह हो, तो अधिकारियों को सूचित करें।
- संदेह में रहें : याद रखें, कोई भी मुफ्त में बड़ी रकम नहीं देता।

Don'ts (क्या न करें)

- क्रेडेंशियल साझा न करें : लॉटरी के दावों के लिए कभी भी सुरक्षित/निजी विवरण न दें और भुगतान न करें।
- नकली संदेशों पर ध्यान न दें : पुरस्कार राशि, सरकारी सहायता या पुरस्कार से जुड़े KYC अपडेट का वादा करने वाले प्रस्तावों का जवाब देने से बचें।

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

साइबर सुरक्षा के लिए सामान्य सुझाव

Do's (क्या करें)

- किसी भी लेन–देन के लिए सत्यापित और आधिकारिक वेबसाइटों का ही उपयोग करें।
- बैंक या कंपनी से होने का दावा करने वाले अज्ञात कॉलर्स की पहले जाँच करें।
- केवल आधिकारिक स्टोर (Google Play Store / Apple App Store) से ही ऐप इंस्टॉल करें।
- महत्वपूर्ण डेटा का नियमित बैकअप रखें।
- परिवार के सदस्यों, खासकर बुजुर्गों और बच्चों को साइबर सुरक्षा के बारे में शिक्षित करें।

Don'ts (क्या न करें)

- OTP, PIN या पासवर्ड किसी के साथ साझा न करें।
- संदिग्ध लिंक पर क्लिक न करें या अनजान अटैचमेंट डाउनलोड न करें।
- अनजान कॉल करने वालों को रिमोट एक्सेस न दें।
- कॉल के दौरान आपात स्थिति या आकर्षक ऑफ़र का दावा किए जाने पर भावुक निर्णय न लें।
- बिना सत्यापन के किसी भी ऑनलाइन प्रोफ़ाइल या ई-मेल को असली न मानें।

SCAM FREE INDIA CYBER ALERT

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

JALDBAAZI, LALACH AUR DARR

AAPKO SCAM KARNE KA CYBER CRIMINALS KA UNIVERSAL FORMULA

To report cyber crimes,
1930 or visit cybercrime.gov.in

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

DIAL 1930 to report cyber crime

Call this helpline number to report cyber crimes to National Cyber Crime Reporting Portal.

अगर आप पीड़ित हैं तो क्या करें

- तुरंत 1930 (साइबर हेल्पलाइन) पर सूचना दें।
- www.cybercrime.gov.in पर शिकायत दर्ज करें।

व्हाट्सऐप हेल्पलाइन:

9256001930 / 9257510100

- अपने बैंक को तुरंत सूचित करें और संदिग्ध लेन–देन रोकने के लिए कहें।
- स्क्रीनशॉट या अन्य सबूत न मिटाएँ, उन्हें सुरक्षित रखें।

SCAM FREE INDIA CYBER ALERT

TECH LEGAL AWARENESS FORUM
A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते

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

SCAM FREE INDIA
CYBER ALERT

रुको . सोचो . एक्शन लो

STOP . THINK . TAKE ACTION

1930

www.cybercrime.gov.in

For Latest Updates Follow CyberDost

CIN: U88900RJ2026NPL110256

PAN: AAMCT6464C
TAN: JDHT04845B

TECH LEGAL AWARENESS FORUM

A SECTION 8 - NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

टेक लीगल अवोयरनेस फोरम

1. **Legal Awareness Promotion**
   कानूनी अधिकारों और कानूनों के पान जानरूप्यान
2. **Digital Literacy & Cyber Safety Education**
   डिजिटल साक्षरत बढ़ाना और साइबर सुरक्षा से संबंधित शिक्षा देना।
3. **Socio-Economic Empowerment**
   वोग और जमरूकता के सागजिक एवं आधिक सम्किकरण
4. **Training, Workshops & Awareness Programs**
   ट्रेनिंग श्रोग्राम, वर्केशॉय, सेथिनार और जामरूकता आम्मेयानों का आयोजना
5. **Research & Community Outreach**
   रिसर्च, सर्वे और कम्यूनिटो आउटरोच गविधियों सचशिकरण
6. **Focus on Vulnerable Groups**
   डिथेटल सर्वे और सानकार्यट्टें और जागरूकता और सादाल्सन
7. **Prevention of Online Frauds**
   डिजिटल आरोगी अेकथाम हेतु जागरूकता थमरिस्का करनी।
8. **Access to Justice & Legal Rights Awareness**
   तकनीक के ज़िम्मेदार और येतिक उपयोग (Capacity Building) में सहयोग।
9. **Support to Victims of Digital Crimes**
   डिजिटल अपराध के पीड़ितों को सहायता, मार्गदर्शन और समर्थन।
10. **Responsible & Ethical Use of Technology**
    तकनीक के ज़िम्मेदार और येतिक उपयोग को बढ़ावा देना।

Registered Office: Sh. No-3, Near Samudayik Bhawan, Kunhadi, Kota, Rajasthan -324009

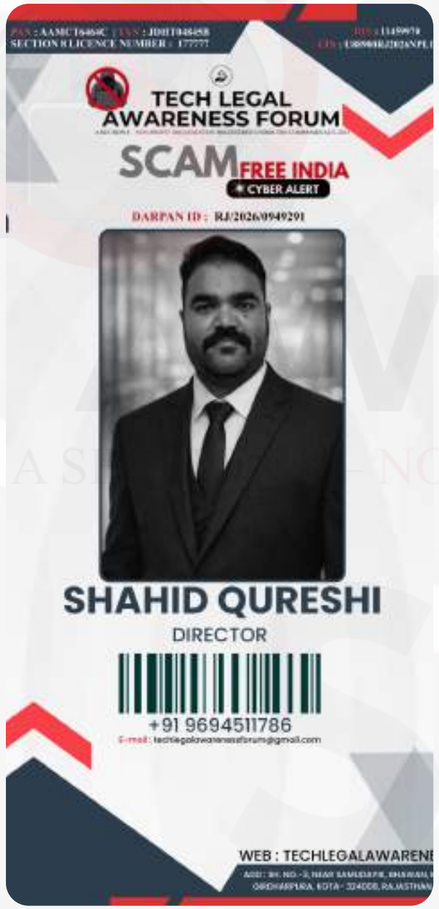
Email: techlegalawarenessforum@gmail.com

+91 9694511786 | +91 8005940528

Board of Directors
Abdul Shahid Qureshi
Director | DIN:11459970

TECH LEGAL AWARENESS FORUM

Our team



SHAHID QURESHI

DIRECTOR

SOMITRA JAIN

DIRECTOR

ABHISHEK MEENA

COORDINATOR

MOHD KASIM PATHAN

COORDINATOR

MAYANK KHANDELWAL

COORDINATOR

TECH LEGAL AWARENESS FORUM

A SECTION 8 – NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

“One step at a time.
You’ll get there.”
@reallygreatsite

TECH LEGAL AWARENESS FORUM

A SECTION 8 – NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2019

Presented by Borcelle

Thank You for your Attention

Staying Ahead of the Curve

The Cybersecurity Threat Landscape refers to the constantly evolving environment of potential and known cyber threats that can affect individuals, organizations, or specific industries.

सत्यमेव जयते

GOVERNMENT OF INDIA
MINISTRY OF CORPORATE AFFAIRS

Central Registration Centre

Certificate of Incorporation

[Pursuant to sub-section (2) of section 7 and sub-section (1) of section 8 of the Companies Act, 2013 (18 of 2013) and rule 18 of the Companies (Incorporation) Rules, 2014]

I hereby certify that TECH LEGAL AWARENESS FORUM is incorporated on this FIRST day of JANUARY TWO THOUSAND TWENTY SIX under the Companies Act, 2013 (18 of 2013) and that the company is Company limited by guarantee

The Corporate Identity Number of the company is **U88900RJ2026NPL110256**

The Permanent Account Number (PAN) of the company is **AAMCT6464C***

The Tax Deduction and Collection Account Number (TAN) of the company is **JDHT04845B***

Given under my hand at Manesar this FIRST day of JANUARY TWO THOUSAND TWENTY SIX

Document certified by DS MINISTRY OF CORPORATE AFFAIRS , CRC MANESAR 2 <RC.CRC@MCA.GOV.IN>

Digitally signed by
DS MINISTRY OF CORPORATE
AFFAIRS , CRC MANESAR 2
Date: 2026.01.01 14:53:05 IST

Shourya Chak

Assistant Registrar of Companies/ Deputy Registrar of Companies/ Registrar of Companies

For and on behalf of the Jurisdictional Registrar of Companies

Registrar of Companies

Central Registration Centre

Disclaimer: This certificate only evidences incorporation of the company on the basis of documents and declarations of the applicant(s). This certificate is neither a license nor permission to conduct business or solicit deposits or funds from public. Permission of sector regulator is necessary wherever required. Registration status and other details of the company can be verified on mca.gov.in

Mailing Address as per record available in Registrar of Companies office:

TECH LEGAL AWARENESS FORUM

Sh. No.-3, Near Samudayik, Bhawan, Kunhadi, Girdharpura, Kota, Kota- 324008, Rajasthan

*as issued by Income tax Department

CERTIFICATE

TRUSTED

आयकर विभाग
INCOME TAX DEPARTMENT

भारत सरकार
GOVT. OF INDIA

स्थायी लेखा संख्या कार्ड
Permanent Account Number Card

AAMCT6464C

नाम / Name
TECH LEGAL AWARENESS FORUM

निगमन / गठन की तारीख
Date of Incorporation/Formation
01/01/2026

PAN : AAMCT6464C | TAN : JDHT04845B

TECH LEGAL AWARENESS FORUM

A SECTION 8 – NON-PROFIT ORGANIZATION REGISTERED UNDER THE COMPANIES ACT, 2013

SCAM FREE INDIA

CYBER ALERT

DIN : 11459970

CIN : U88900RJ2026NPL110256

ADD : SH. NO.-3, NEAR SAMUDAYIK, BHAWAN, KUNHADI, GIRDHARPURA, KOTA- 324008, RAJASTHAN, INDIA

WEB : TECHLEGALAWARENESS.IN