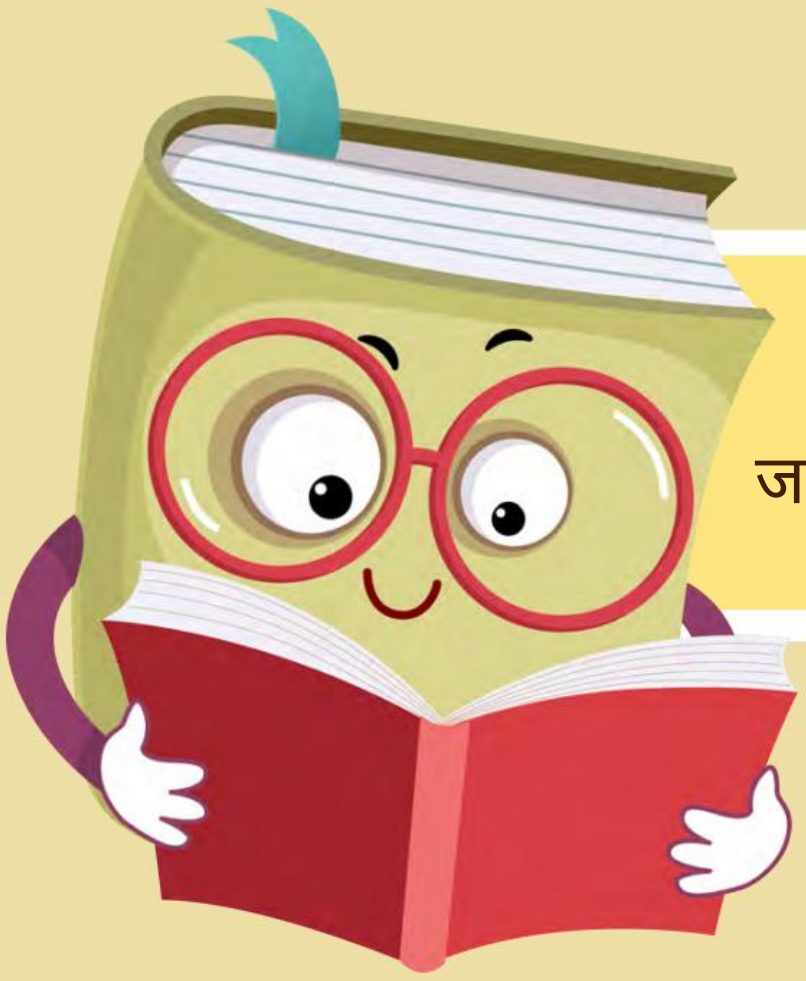
इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

आज़ादी का
अमृत महोत्सव



इंटरनेट सुरक्षा जनजागृती पुस्तिका

डिजिटल नागरीकांसाठी आणि
डिजिटल उपक्रम

द्वारे

भारतीय संगणक इमर्जन्सी रिस्पॉन्स टीम

certin
Enhancing Cyber Security in India

च्या प्रसंगी

सुरक्षित इंटरनेट दिवस (६ फेब्रुवारी २०२४)

"सुरक्षा ही आमची पहिली प्राथमिकता"

निर्देशांक

प्रस्तावना

इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) ही भारत सरकारच्या इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालयाच्या (MeitY), भारतीय सायबर स्पेस सुरक्षित करण्याच्या उद्देशाने स्थापन केलेली एक सरकारी संस्था आहे.

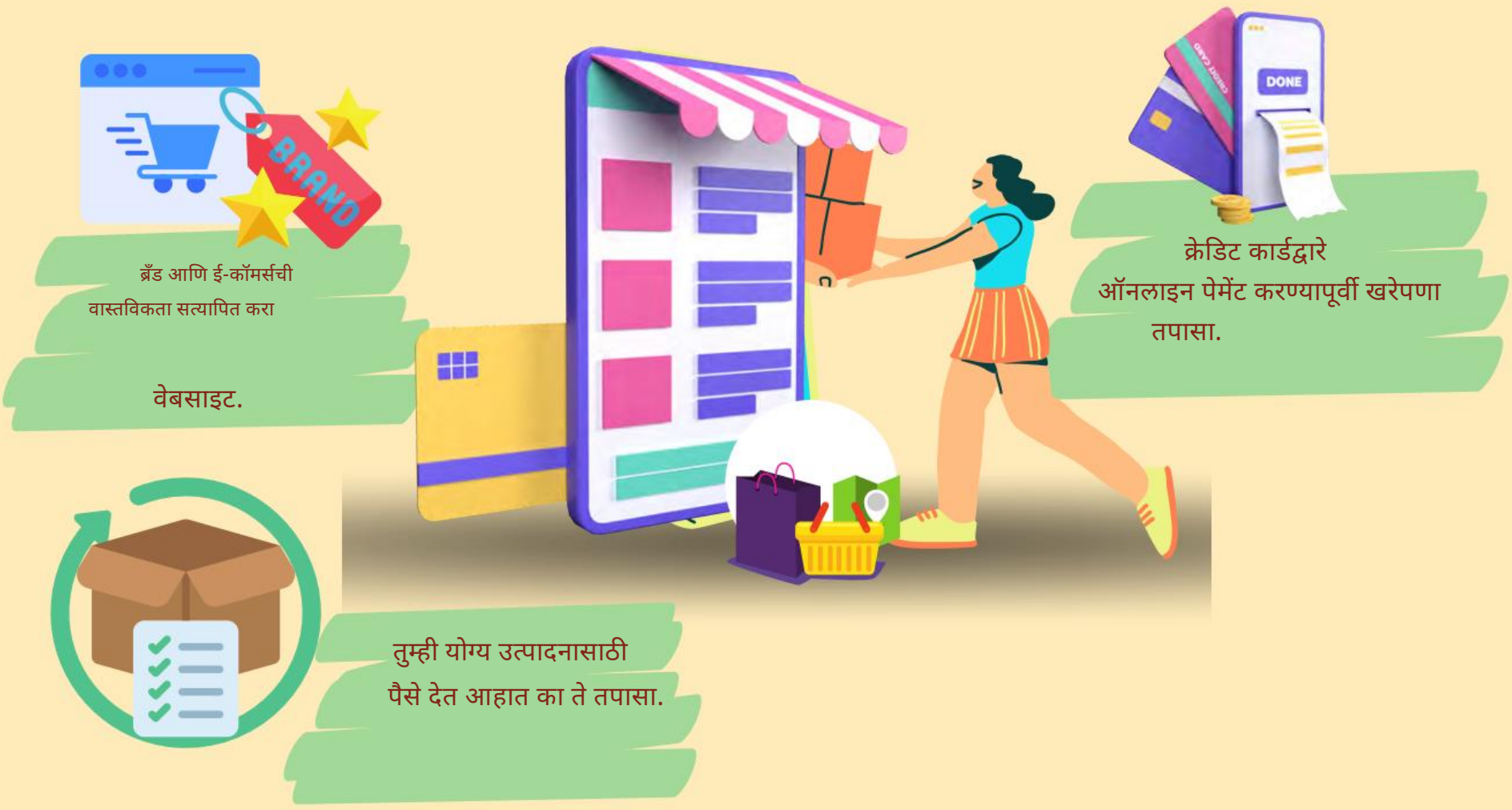
CERT-In घटना प्रतिबंध आणि प्रतिसाद सेवा तसेच सुरक्षा गुणवत्ता व्यवस्थापन सेवा प्रदान करते.

CERT-In ला माहिती तंत्रज्ञान कायदा, 2000 (सुधारणा 2008) च्या कलम 70B अंतर्गत घटना प्रतिसादासाठी राष्ट्रीय एजन्सी म्हणून नियुक्त करण्यात आले आहे. CERT-In च्या सेवांचा एक भाग म्हणून, सायबर सुरक्षेच्या क्षेत्रात जागरूकता निर्माण करण्यासाठी तसेच विविध भागधारकांच्या तांत्रिक ज्ञानाचे प्रशिक्षण/अपग्रेड करण्यासाठी, CERT-In 6 फेब्रुवारी 2024 रोजी सुरक्षित इंटरनेट दिन पाळत आहे.

डिजिटल नागरीक आणि डिजिटल एंटरप्रायझेससाठी ही इंटरनेट सुरक्षा जागरूकता पुस्तिका वापरकर्त्यांना सर्वोत्तम गोष्टींबद्दल शिक्षित करण्यासाठी CERT-In च्या जागरूकता उपक्रमांचा एक भाग म्हणून प्रसिद्ध करण्यात आली आहे.

सुरक्षित आणि सुरक्षित पद्धतीने इंटरनेट वापरण्यासाठी ज्या पद्धती पाळल्या पाहिजेत.

ऑनलाइन खरेदी सर्वोत्तम पद्धती



सर्वोत्तम पद्धती

- तुमची ऑनलाइन खरेदी करण्यासाठी नेहमी विश्वसनीय वेबसाइटला भेट द्या.
- तुमचे डिव्हाइस अँटीव्हायरस, अँटी-मालवेअर सोल्यूशन्ससह सुरक्षित ठेवा.

- तुमच्या डिजिटल पेमेंटचा मागोवा ठेवा.
- वेबसाइटच्या सुरक्षिततेच्या बाबी तपासा, जसे की साइट https//: किंवा ब्राउझर ॲड्रेस बारवर पॅडलॉकसह सुरक्षित आहे का.

- तुमची वैयक्तिक माहिती आणि खाते तपशील विचारणाऱ्या ईमेलला कधीही प्रतिसाद देऊ नका.
- तुमचे पासवर्ड वारंवार बदला.
- नेहमी सुरक्षित इंटरनेट कनेक्शन वापरा.
- आर्थिक व्यवहार करण्यासाठी सार्वजनिक वाय-फाय वापरणे टाळा.
- सवलत किंवा बक्षिसे ऑफर करणाऱ्या संशयास्पद लिंकवर क्लिक करू नका जे खरे असायला खूप चांगले वाटतात.

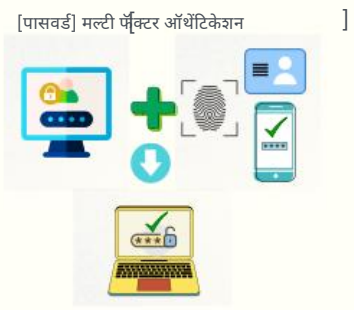
ई-मेल
सर्वोत्तम पद्धती

ई-मेल सुरक्षिततेसाठी टिपा

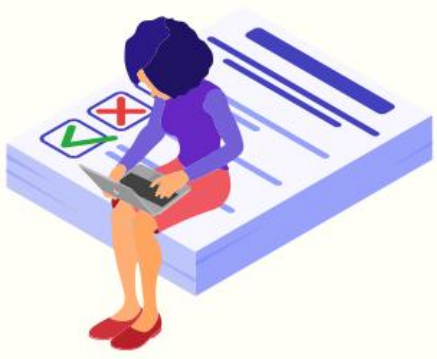
स्पॅम टाळण्यासाठी नेहमी ई-मेल फिल्टरिंग सॉफ्टवेअर वापरा जेणेकरून केवळ अधिकृत वापरकर्त्यांचे संदेश प्राप्त होतील.

अज्ञात स्त्रोतांकडून दुवे/संलग्नक उघडणे टाळा कारण ते दुर्भावनापूर्ण असू शकतात.

अद्ययावत अँटीव्हायरस आणि अँटी-मालवेअर सॉफ्टवेअरसह तुमची प्रणाली नियमितपणे स्कॅन करा.



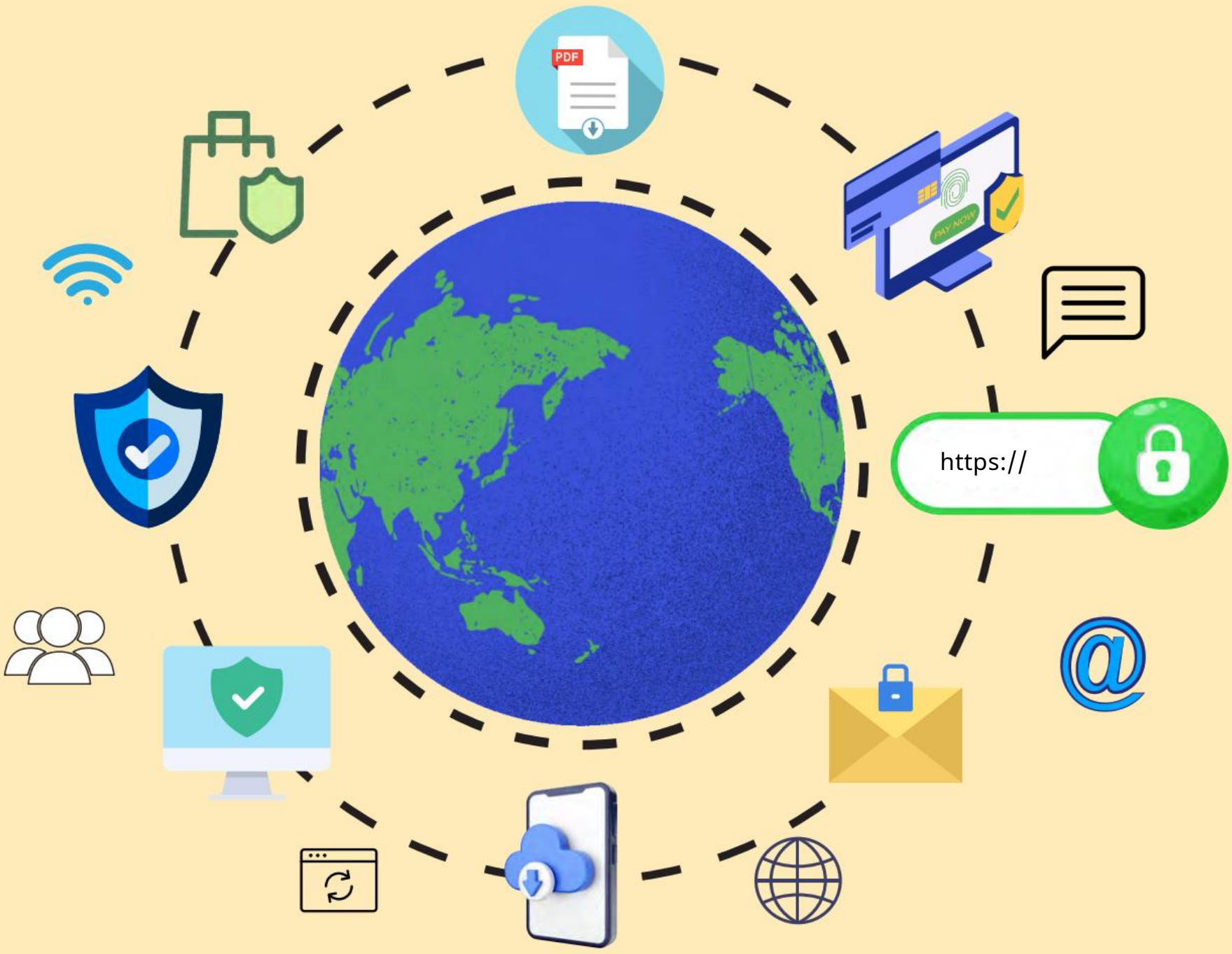
मल्टी-फॅक्टर सक्षम करा प्रमाणीकरण



अवांछित ईमेलद्वारे येणारे फॉर्म भरणे किंवा अविश्वासू स्त्रोतांकडून प्राप्त झालेल्या ईमेलमधील लिंकवर क्लिक करणे टाळा.

निकडीची भावना निर्माण करणारे ईमेल किंवा संदेश एक चेतावणी आहे!

ब्राउझर सर्वोत्तम पद्धती

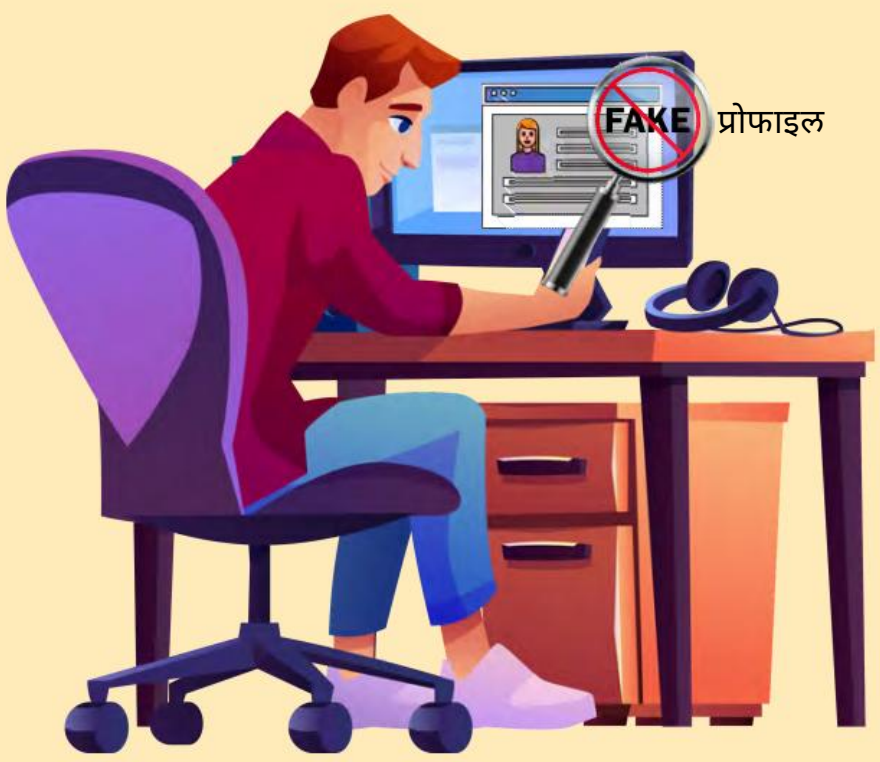


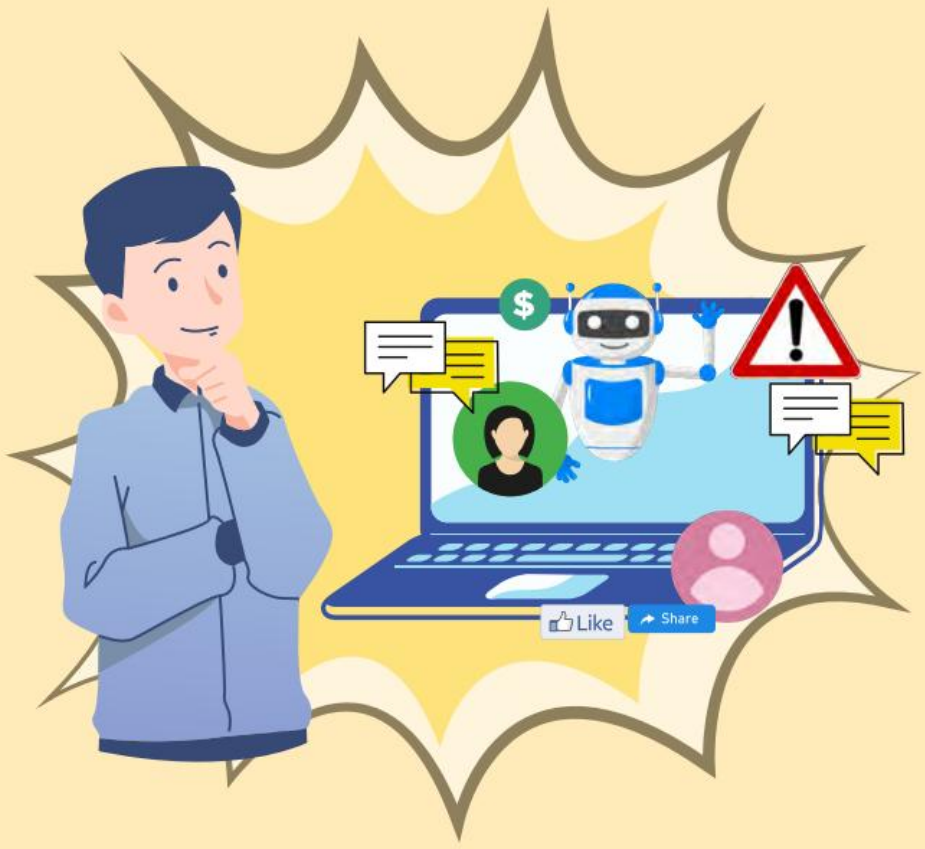
सर्वोत्तम पद्धती

- तुमचा वेब ब्राउझर नेहमी नवीनतम पॅचसह अपडेट करा.
- तुमच्या ब्राउझरमध्ये पॉप-अप विंडो अक्षम करा.
- ब्राउझर कुकीज आणि कॅशे नियमितपणे हटवा.
- खाजगी ब्राउझिंग किंवा गुप्त मोड सक्षम करा.
- तुम्ही भेट देत असलेल्या वेबसाइट/लिंकबाबत सावधगिरी बाळगा.
- लहान URL विस्तृत करा आणि क्लिक करण्यापूर्वी त्यांची पडताळणी करा.
- ब्राउझरमध्ये अंतर्निहित गोपनीयता किंवा सुरक्षा सेटिंग्ज वापरा.

- लॉगिन आणि पासवर्ड लक्षात ठेवा पर्याय अक्षम करा.
- वेबसाइट जेव्हा विस्तार किंवा थीम स्थापित करण्याचा प्रयत्न करतात तेव्हा वापरकर्ता चेतावणी पर्याय सक्षम करा.
- शोध इंजिनमध्ये "सुरक्षित शोध" चालू करा.

सोशल मीडिया सर्वोत्तम पद्धती





सर्वोत्तम पद्धती

- तुमची वैयक्तिक माहिती जसे की पत्ता, मोबाइल नंबर, वैयक्तिक मेल आयडी आणि इतर संवेदनशील ओळख संबंधित माहिती सोशल मीडियावर शेअर करणे टाळा.
- तुमची वैयक्तिक छायाचित्रे सोशल मीडिया अकाउंटवर सार्वजनिकपणे ऑनलाइन शेअर करू नका.
- योग्य पडताळणी आणि पुष्टीकरणाशिवाय कधीही मित्र विनंत्या स्वीकारू नका.
- संशयास्पद लिंक्सवर कधीही क्लिक करू नका किंवा संदेशांद्वारे प्राप्त झालेले कोणतेही ॲप डाउनलोड करू नका जोपर्यंत तुम्ही याची सत्यता पडताळत नाही.
स्रोत
- वेगवेगळ्या सोशल मीडिया खाती आणि ईमेलसाठी वेगवेगळे पासवर्ड वापरा.
- सोशल मीडिया खात्यांसाठी बहु-घटक प्रमाणीकरण सक्षम करा.
- सार्वजनिक शोधांमधून प्रोफाइल दृश्यमानता अक्षम करा.
- प्रत्येक सत्रानंतर लॉग आउट करा.
- सोशल मीडिया क्रेडेन्शियल्स कधीही कोणाशीही शेअर करू नका.
- सोशल मीडिया प्रोफाइलची गोपनीयता सेटिंग्ज अत्यंत प्रतिबंधित स्तरावर ठेवा, विशेषतः सार्वजनिक पाहण्यासाठी.
- छायाचित्रे, व्हिडिओ, स्टेटस, टिप्पण्या इत्यादी शेअर करताना जास्तीत जास्त सावधगिरी बाळगा. गुन्हेगार वापरकर्त्यांच्या पोस्ट आणि प्रोफाइलमधून वापरकर्त्यांबद्दल पुरेशी माहिती गोळा करू शकतात.

मोबाईल फोन सर्वोत्तम पद्धती

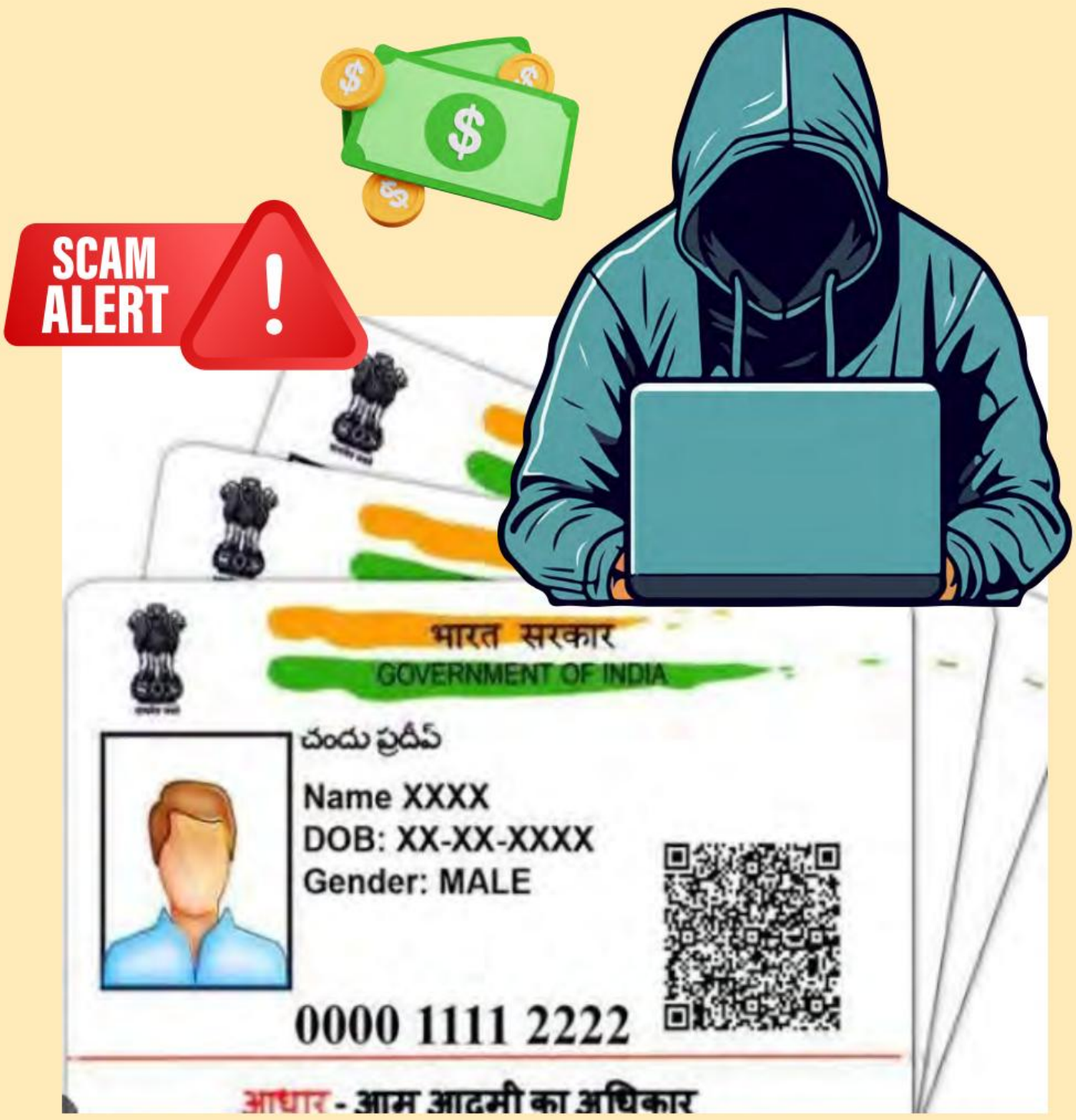
सर्वोत्तम पद्धती

- अपडेटेड अँटीव्हायरस आणि अँटी-मालवेअर सॉफ्टवेअर वापरा.
- अद्ययावत ऑपरेटिंग सिस्टम वापरा.
- प्लेस्टोअर किंवा ॲपस्टोअरवरून नेहमी ॲप्स डाउनलोड करा.
- तृतीय पक्षाच्या वेबसाइटवरून किंवा मेसेज किंवा चॅटद्वारे मिळालेल्या लिंकवरून ॲप्स डाउनलोड करू नका.
- ॲप्ससाठी फक्त आवश्यक परवानग्या सक्षम करा.
- अनोळखी व्यक्तींकडून मिळालेल्या कोणत्याही संशयास्पद लिंकवर क्लिक करू नका.
- कोणत्याही अर्जासाठी मिळालेला तुमचा OTP कोणाशीही शेअर करू नका.

- जेव्हा शक्य असेल तेव्हा मल्टी-फॅक्टर ऑथेंटिकेशन सक्षम करा.
- तुमचा फोन वापरात नसल्यास नेहमी लॉक ठेवा.
- सार्वजनिक ठिकाणी यूएसबी चार्जिंग टाळा.

आधार

सर्वोत्तम पद्धती



सर्वोत्तम पद्धती

- तुमच्या खात्याच्या तपशीलांमध्ये अनधिकृत प्रवेश टाळण्यासाठी m-Aadhaar ॲप/ UIDAI पोर्टलद्वारे तुमचे बायोमेट्रिक्स लॉक करा.
- आधार क्रमांकाचा खुलासा टाळण्यासाठी व्हर्च्युअल आयडी (व्हीआयडी) किंवा मास्क केलेले आधार वापरा.
- कोणत्याही गतिविधीची सूचना मिळवण्यासाठी तुमचा आधार डेटा तुमच्या मोबाइल नंबरशी लिंक करा.
- तुमच्या डिजिटल आधारच्या प्रती सुरक्षित ठेवा.
- तुमचा आधार तपशील, OTP अनोळखी व्यक्तींना शेअर करू नका.
- सार्वजनिक संगणकांमध्ये तुमचा डिजिटल आधार जतन करणे टाळा.
- तुमचे काम पूर्ण झाल्यावर सार्वजनिक संगणकावरून आधार माहिती/प्रत हटवा.

डेस्कटॉप
सर्वोत्तम पद्धती

सर्वोत्तम पद्धती

- अस्सल ऑपरेटिंग सिस्टम आणि सॉफ्टवेअर वापरा.
- तुमची ऑपरेटिंग सिस्टम अपडेट ठेवा.
- अँटी-व्हायरस आणि अँटी-मालवेअर सोल्यूशन्स स्थापित करा.
- तुमचे अँटीव्हायरस आणि अँटी-मालवेअर सोल्यूशन्स अपडेट ठेवा.
- मजबूत लॉगिन पासवर्ड वापरा आणि वेळोवेळी बदला.

- तुमच्या महत्त्वाच्या फाइल्स आणि डेटाचा नियमितपणे बॅकअप घ्या.
- हार्डवेअर अयशस्वी होणे किंवा सायबर हल्ल्यांसारख्या घटनांच्या बाबतीत, बॅकअप घेणे तुम्हाला महत्त्वाची माहिती पुनर्संचयित करण्यात मदत करू शकते.

- आपत्तींच्या बाबतीत नुकसान टाळण्यासाठी वेगवेगळ्या ठिकाणी गंभीर डेटाच्या अनेक प्रती ठेवा.
- आवश्यकतेनुसार पुनर्संचयित करण्यासाठी त्यांचा वापर केला जाऊ शकतो याची खात्री करण्यासाठी वेळोवेळी चाचणी आणि पडताळणी करा.

जागरूकता साहित्य

मार्गदर्शक तत्त्वे:

सरकारी संस्थांसाठी माहिती सुरक्षा पद्धतींवरील मार्गदर्शक तत्त्वे भेट द्या: https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf सुरक्षित अनुप्रयोग डिझाइन, विकास, अंमलबजावणी आणि ऑपरेशन्ससाठी मार्गदर्शक तत्त्वे भेट द्या: https://www.cert- in.org.in/PDF/

Application_Security_Guidelines.pdf

सल्ला:

भेट द्या: https://www.cert-in.org.in CERT-In Advisory CIAD-2024-0006 : सुरक्षित करणे सोशल मीडिया अकाउंट्स CERT-In Advisory CIAD-2022-0003 : सुरक्षित करणे ट्विटर अकाउंट्स CERT-In Advisory CIAD-2022- 0026 : पासवर्ड व्यवस्थापन आणि सुरक्षा

जनजागृती पुस्तिका:

भेट द्या: https://www.cert-in.org.in/PDF/CSA_Booklet.pdf

सायबरस्वच्छतकेंद्र

सुरक्षा साधने

फ्री बॉट रिमूव्हल टूल- मायक्रोसॉफ्ट विंडोजसाठी

- eScan अँटीव्हायरस
- K7 सुरक्षा
- जलद बरे

मोफत बॉट रिमूव्हल टूल - Android साठी

- eScan अँटीव्हायरस

मोफत मोबाइल सुरक्षा अनुप्रयोग - Android साठी

- म-कवच २

इतर संबंधित साधने:

- यूएसबी प्रतिरोध
- AppSamvid
- ब्राउझर JSGuard

मला स्कॅन करा

सायबर सुरक्षेचा अहवाल द्या सीईआरटी-इनची घटना

CERT-In ला सायबर सुरक्षा घटनांचा अहवाल देण्यासाठी: वेबसाइटला भेट द्या: https://www.cert-in.org.in

ईमेल: घटना@cert-in.org.in टोल फ्री फोन: +91-1800-11-4949 फोन:

+91-11-24368551

माहिती डेस्क

टोल फ्री फॅक्स: +91-1800-11-6969

फॅक्स: +91-11-24368546

I4C ला सायबर फसवणूक आणि गुन्ह्याची तक्रार करण्यासाठी: वेबसाइटला भेट द्या: https://www.cybercrime.gov.in कॉल: 1930

सायबर सुरक्षेच्या क्षेत्रात CERT-In सह असुरक्षा आणि सहयोगाची तक्रार करण्यासाठी: वेबसाइटला भेट द्या: https://www.cert-in.org.in ईमेल: vdisclose@cert-in.org.in (असुरक्षा प्रकटीकरण) collaboration@cert-in.org.in (सहयोग)

फोन: +11-22902600 विस्तार: 1012, +91-11-24368572

प्रशिक्षण/जागृती कार्यक्रमांसाठी: ईमेल: training@cert-in.org.in

@IndianCERT चे अधिकृत सोशल मीडिया हँडल

https://www.facebook.com/IndianCERT/

https://twitter.com/IndianCERT

https://www.kooapp.com/profile/IndianCERT

https://www.pixstory.com/user/indiancert/9280 https://www.instagram.com/cert_india/

मला स्कॅन करा

www.cert-in.org.in

मला स्कॅन करा

www.csk.gov.in