साप्ताहिक परामर्श कार्यक्रम

सुचना प्रविधिमा साइबर सतर्कता

विपुल गौतम
प्रमुख, सुचना प्रविधि विभाग

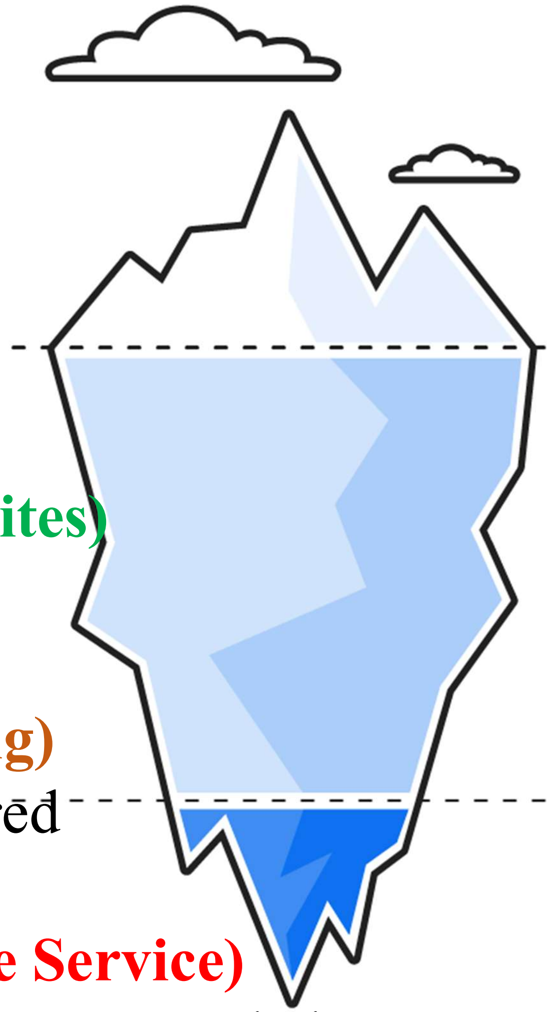
राष्ट्रिय सहकारी बैंक लिमिटेड
National Co-operative Bank Limited (NCBL)

Bhadra 5, 2083

Overview

- Word Wide Web
- Dark Web
- Cyber Security in a Cooperative
- सहकारीका कर्मचारीहरूका लागि साइबर सुरक्षा निर्देशिका
  - खाता र प्रमाणीकरण सुरक्षा (Account & Authentication Security)
  - डिजिटल ठगी र सामाजिक सञ्जाल सचेतना (Scams & Social Media Awareness)
  - उपकरण र नेटवर्क सुरक्षा (Device & Network Security)
  - गोपनीयता र संस्थागत आचरण (Privacy & Institutional Practices)
  - घटना व्यवस्थापन र सचेतना (Incident Response & Awareness)

Word Wide Web (www)



Surface Web (Public - News Sites)
No need of username/password

Deep Web (Secured - eBanking)
Username & Password is required

Dark Web (Hidden – Malware Service)
Special Browsers or Applications are needed

Surface web (5%–10%)

- Find information easily
- Connect on social media
- Shop online

Deep web (90%–95%)

- Send and receive emails
- Log into bank accounts
- Access subscriptions

Dark web (.01%)

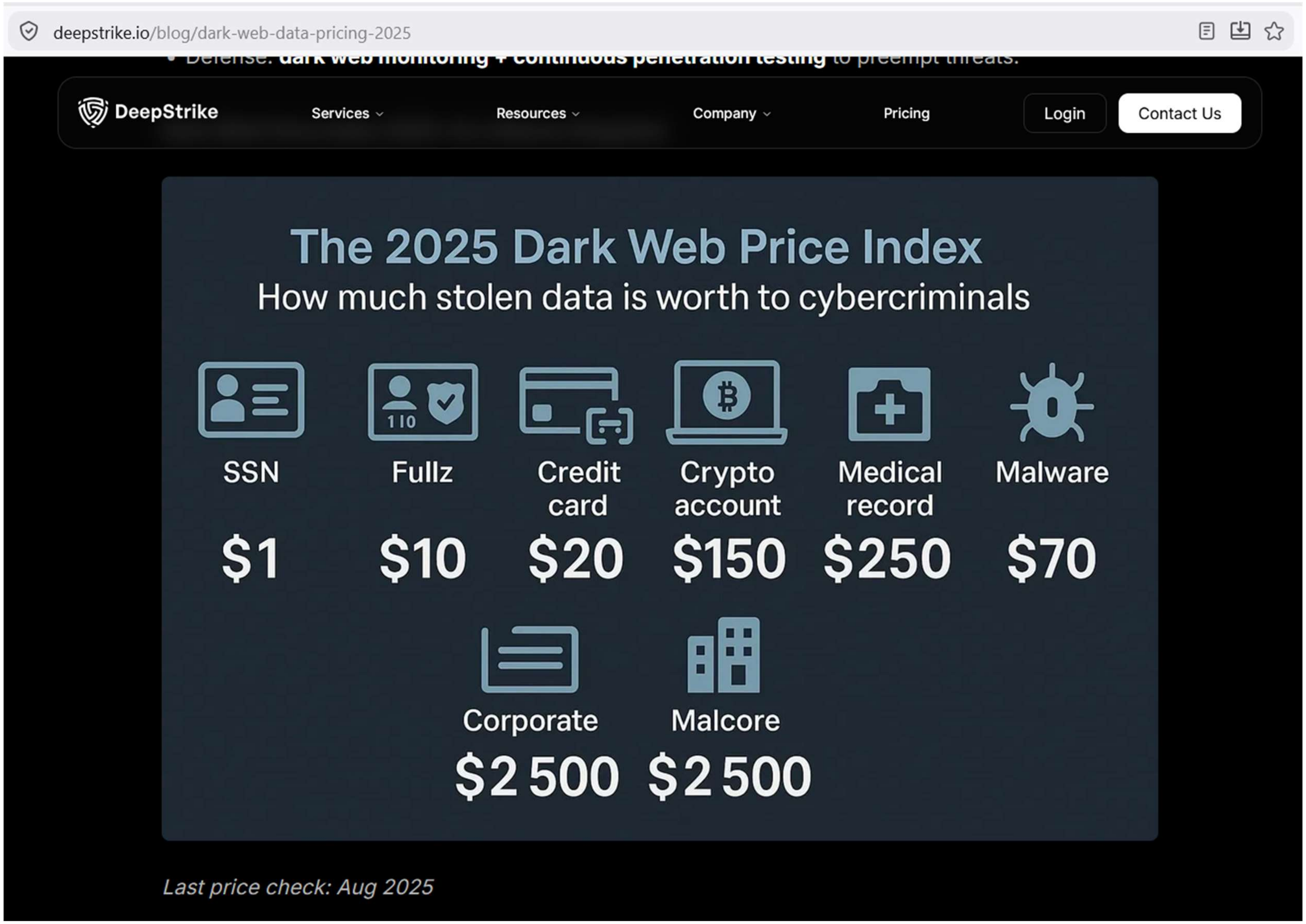
- Access censored news
- Communicate anonymously
- Consume niche or illegal content

Source: https://us.norton.com/blog/privacy-tips/deep-web-vs-dark-web

Dark Web

- डार्क वेब (Dark Web) इन्टरनेटको **एउटा यस्तो लुकेको भाग हो** जसलाई Google, Bing वा Yahoo जस्ता **साधारण सर्च इन्जिनहरूले फेला पार्न सक्दैनन्**।
- यसलाई खोल्नका लागि विशेष सफ्टवेयर वा प्रविधिको आवश्यकता पर्दछ र यसले प्रयोगकर्ताको पहिचान र लोकेसनलाई पूर्ण रूपमा गोप्य राख्छ।
- डार्क वेबको एक्सेस सजिलो त छैन, तर केही गरी चलाउन पुगियो भने उक्त एक्सेस धेरै कारणले प्रत्युत्पादक (counterproductive) वा खतरनाक हुन सक्छ।
- **What do we get in a Dark Web?**
  - Black Market Place (कालो बजारी),
  - Whistle Blowing Sites (गोप्य सूचना बाहिर ल्याउने साइटहरू)
  - Counterfeit Document in Sale (नक्कली कागजात बिक्रीमा)
  - Counterfeit Money in Sale (नक्कली नोट बिक्रीमा)
  - Stolen Data in Sale (चोरिएका डाटा बिक्रीमा) [like PII, passwords, credit card details]
  - Illegal Drugs & Human Trafficking (अवैध लागुऔषध र मानव बेचबिखन)
  - Malware-As-A-Service (मालवेयर-एक-सेवाको-रूपमा)
  - Hacking Forums with Data Theft Details (डाटा चोरीका विवरणहरू भएका ह्याकिङ फोरमहरू)

  - Dark Web Data Pricing
- Nepali Banks' Data Found in Dark Web


deepstrike.io/blog/dark-web-data-pricing-2025
• Defense: dark web monitoring + continuous penetration testing to preempt threats.
DeepStrike
Services
Resources
Company
Pricing
Login
Contact Us
The 2025 Dark Web Price Index
How much stolen data is worth to cybercriminals
SSN
$1
Fullz
$10
Credit card
$20
Crypto account
$150
Medical record
$250
Malware
$70
Corporate
$2 500
Malcore
$2 500
Last price check: Aug 2025

Cyber Security in a Cooperative

- **Firewall** Devices
  - Antivirus, Web Filtering, **Intrusion Prevention**, Virtual Private Network (**VPN**), etc.
- **End Point Protection** (like Antivirus for PC/Laptop/Servers)
- Network Vulnerability Assessment & Penetration Testing (VAPT)
- Application VAPT
- Information System (IS) Audit
- Regular Testing **Backups** by Restoring
- Security Information & Event Management (SIEM)
- Network Operation Center (NOC) & Security Operations Center (SOC)
- Business Continuity Planning (BCP)
  - **Data Center (DC)** & Disaster Recovery (DR) Site
  - **Redundancy** (Links & Devices) & DR Drill
- Awareness & **Trainings** to Staff, and as well as to Members.
- **Regulatory Compliance**

सहकारीका कर्मचारीहरूका लागि साइबर सुरक्षा निर्देशिका

सहकारीको वित्तीय कारोबार र सदस्यहरूको व्यक्तिगत विवरण (KYM) लाई सुरक्षित राख्दै सम्भावित साइबर जोखिम र डिजिटल ठगीबाट बच्नका लागि सबै कर्मचारीहरूले पालना गर्नुपर्ने मुख्य साइबर सुरक्षाका मापदण्डहरू यस प्रकार छन्:

१. खाता र प्रमाणीकरण सुरक्षा (Account & Authentication Security)

२. डिजिटल ठगी र सामाजिक सञ्जाल सचेतना (Scams & Social Media Awareness)

३. उपकरण र नेटवर्क सुरक्षा (Device & Network Security)

४. गोपनीयता र संस्थागत आचरण (Privacy & Institutional Practices)

५. घटना व्यवस्थापन र सचेतना (Incident Response & Awareness)

१. खाता र प्रमाणीकरण सुरक्षा (Account & Authentication Security)

- **बलियो पासवर्ड (Strong Password or Passphrase):**
  - आफ्ना सबै वित्तीय र प्रशासनिक खाताहरूमा कडा पासवर्ड (अक्षर, अंक, र विशेष चिन्हहरू मिश्रित) प्रयोग गर्ने र समय-समयमा अनिवार्य रूपमा परिवर्तन गर्ने ।
- **दुई-चरणको प्रमाणीकरण (Two Factor Authentication - 2FA):**
  - सहकारीको कोर बैंकिङ प्रणाली, इमेल वा अन्य कुनै पनि संवेदनशील सफ्टवेयर लगइन गर्दा अनिवार्य रूपमा पासकोड र ओटीपी (OTP) प्रणाली सुचारु गर्ने ।
- **ओटीपी (One Time Password) सुरक्षा:**
  - बैंकिङ कारोबार वा कुनै पनि संवेदनशील सेवा प्रयोग गर्दा मोबाइल वा इमेलमा प्राप्त हुने ओटीपी कसैसँग, कुनै पनि बहानामा सेयर नगर्ने ।
- **कम्प्युटर वा मोबाइल स्क्रिन लक (Device Locking):**
  - आफ्नो कम्प्युटर वा मोबाइल छोडेर आफ्नो सिट वा कार्यकक्षबाट बाहिर जाँदा अनिवार्य रूपमा स्क्रिन लक (Windows + L) गर्ने बानी बसाल्ने ।

१. खाता र प्रमाणीकरण सुरक्षा (Account & Authentication Security)

- **वेब ब्राउजरमा पासवर्ड सुरक्षित नगर्ने (No Password Saving in Browsers):**
  - सहकारीको वित्तीय प्रणाली वा अन्य प्रशासनिक खाताहरू लगइन गर्दा वेब ब्राउजर (जस्तै: Chrome, Edge) मा स्वचालित रूपमा आउने 'Save Password' विकल्पलाई सधैं अस्वीकार (Never) गर्ने।

- **अटो-फिल र क्रेडिट कार्ड विवरण असुरक्षा (Disable Browser Auto-fill):**
  - वेब ब्राउजरमा पासवर्ड मात्र होइन, सदस्यहरूको बैंक खाता नम्बर, क्रेडिट/डेबिट कार्ड विवरण र व्यक्तिगत फारमहरू स्वचालित रूपमा भरिने 'Auto-fill' विकल्पलाई पनि अनिवार्य रूपमा बन्द (Disable) गर्ने।

- **मल्टी-फ्याक्टर अथेन्टिकेशन बाइपास सचेतना (MFA Fatigue/Push Prompt Scams):**
  - आफ्नो मोबाइलमा आफूले लगइन नगरेको अवस्थामा पनि अचानक आउने प्रणाली लगइनका 'Allow' वा 'Approve' गर्ने सूचनाहरू (Push Notifications) लाई तुरुन्तै अस्वीकार (Deny) गर्ने र प्राविधिक टोलीलाई जानकारी गराउने।

२. डिजिटल ठगी र सामाजिक सञ्जाल सचेतना

(Scams & Social Media Awareness)

- **सामाजिक सञ्जाल ठगी सचेतना (Social Media Fraud Prevention):**
  - फेसबुक, मेसेन्जर वा ह्वाट्सएपमा चिनजानकै व्यक्ति वा सहकर्मीले आकस्मिक समस्या देखाउँदै रकम मागेमा पैसा पठाउनु अघि अनिवार्य रूपमा फोन कल गरेर सत्यता यकिन गर्ने ।

- **शङ्कास्पद लिङ्क र इमेल (Suspicious Links & Emails):**
  - अनाधिकृत व्यक्ति वा अपरिचित स्रोतबाट चिट्ठा परेको, आकर्षक उपहार जितेको वा खाता बन्द हुन लागेको भनी आउने भ्रमपूर्ण इमेल र लिङ्कहरूमा क्लिक नगर्ने ।

- **फोन कल मार्फत हुने ठगी (Vishing/Phone Fraud):**
  - बैंक, राष्ट्र बैंक वा कुनै आधिकारिक संस्थाको कर्मचारी भन्दै फोन गरेर खाता विवरण, पिन वा पासवर्ड माग्नेहरूलाई कुनै पनि जानकारी नदिने ।

२. डिजिटल ठगी र सामाजिक सञ्जाल सचेतना

(Scams & Social Media Awareness)

- **पार्सल वा गिफ्ट ठगी (Parcel or Gift Fraud):**
  - विदेशबाट महँगो पार्सल वा उपहार पठाइदिएको र सो लिनका लागि भन्सार शुल्क वा डेलिभरी चार्ज स्वरूप अग्रिम रकम माग्ने गिरोहबाट सचेत रहने ।

- **सिम स्वाप ठगी (SIM Swap Fraud):**
  - आफ्नो मोबाइलको नेटवर्क वा सिग्नल अचानक लामो समयसम्म हराएमा वा बन्द भएमा तुरुन्तै टेलिकम सेवा प्रदायक र बैंकमा सम्पर्क गर्ने ।

- **फर्जी विज्ञापन र आकर्षक जागिर (Fake Advertisements & Lucrative Jobs):**
  - फेसबुक वा अन्य सञ्जालमा देखिने 'घरमै बसीबसी कमाइने' आकर्षक अनलाइन रोजगारीका नाममा सुरुमा रकम लगानी गर्न वा दर्ता शुल्क तिर्न लगाउने प्रलोभनमा नफस्ने ।

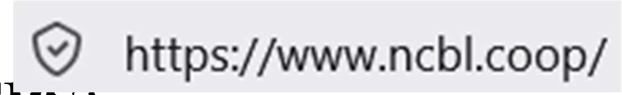
२. डिजिटल ठगी र सामाजिक सञ्जाल सचेतना (Scams & Social Media Awareness)

- **नक्कली बैंकिङ र वित्तीय एपहरू (Malicious Financial/Cooperative Apps):**
  - सहकारीको प्रणाली चलाउन वा सदस्यहरूलाई डिजिटल सेवा दिन प्ले स्टोर (Play Store) वा एप स्टोर (App Store) बाहेकका अपरिचित वेबसाइट र लिङ्कबाट एपीके (.apk) फाइलहरू डाउनलोड गरेर इन्स्टल नगर्ने ।

- **इमेल स्पूफिङ र नक्कली बिल/बीजक (Email Spoofing & Invoice Fraud):**
  - संस्थाका मुख्य सप्लायर्स वा भेन्डरहरूको इमेल आईडी जस्तै देखिने नक्कली इमेलबाट आउने बैंक खाता परिवर्तन सम्बन्धी पत्र वा भुक्तानी माग गरिएका बिलहरूलाई फोन मार्फत पुन: प्रमाणीकरण नगरी रकम भुक्तानी नगर्ने ।

३. उपकरण र नेटवर्क सुरक्षा (Device & Network Security)

- **सुरक्षित वाइफाइको प्रयोग (Browsing Safe Wi-Fi):**
  - सहकारीको वित्तीय कारोबार गर्दा, सदस्यहरूको डाटा चलाउँदा वा संवेदनशील काम गर्दा सार्वजनिक, खुल्ला वा असुरक्षित फ्रि-वाइफाइ नेटवर्क कहिल्यै प्रयोग नगर्ने।



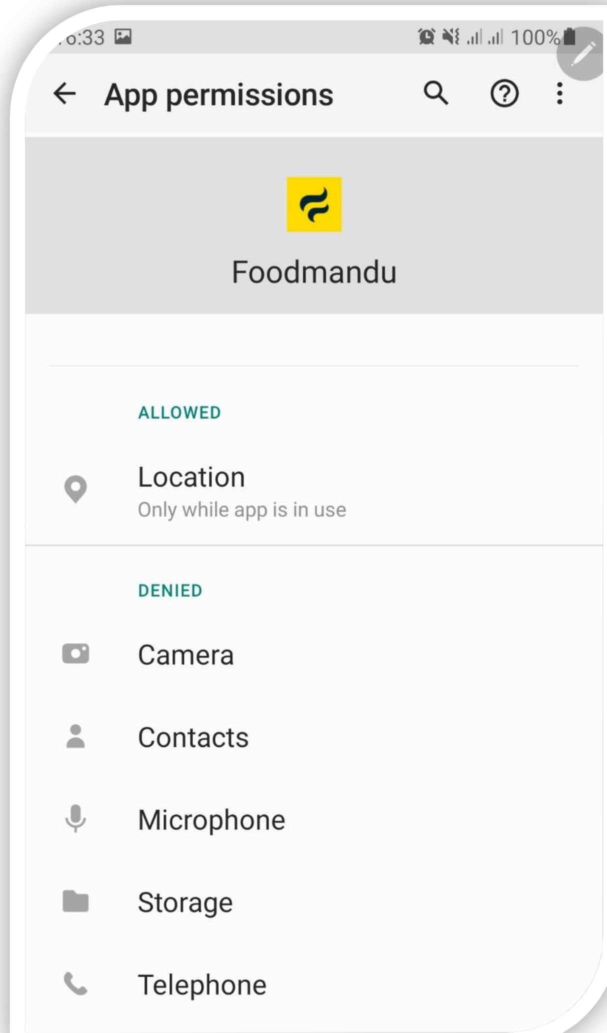
- **सुरक्षित वेबसाइट पहिचान (Secure Browsing - HTTPS):**
  - कुनै पनि वेबसाइटमा संस्थागत वा व्यक्तिगत विवरणहरू राख्नु अघि लिङ्कको सुरुमा https:// र सुरक्षित लक (Padlock) को चिन्ह छ वा छैन अनिवार्य यकिन गर्ने।
- **अपरिचित पेनड्राइभ वा बाह्य हार्डडिस्क (USB/External Devices):**
  - बाटोमा भेटिएका, उपहारमा पाइएका वा अपरिचित व्यक्तिका पेनड्राइभ तथा बाह्य हार्डडिस्कहरू संस्थाको कम्प्युटरमा सिधै जोडेर प्रयोग नगर्ने।
- **सिस्टम र एन्टिभाइरस अपडेट (Updating System & Antivirus):**
  - सहकारीमा प्रयोग हुने सबै कम्प्युटर, ल्यापटप र सर्भरका सफ्टवेयरहरू समय-समयमा अपडेट गर्ने र आधिकारिक एवं लाइसन्सप्राप्त एन्टिभाइरस मात्र प्रयोग गर्ने।

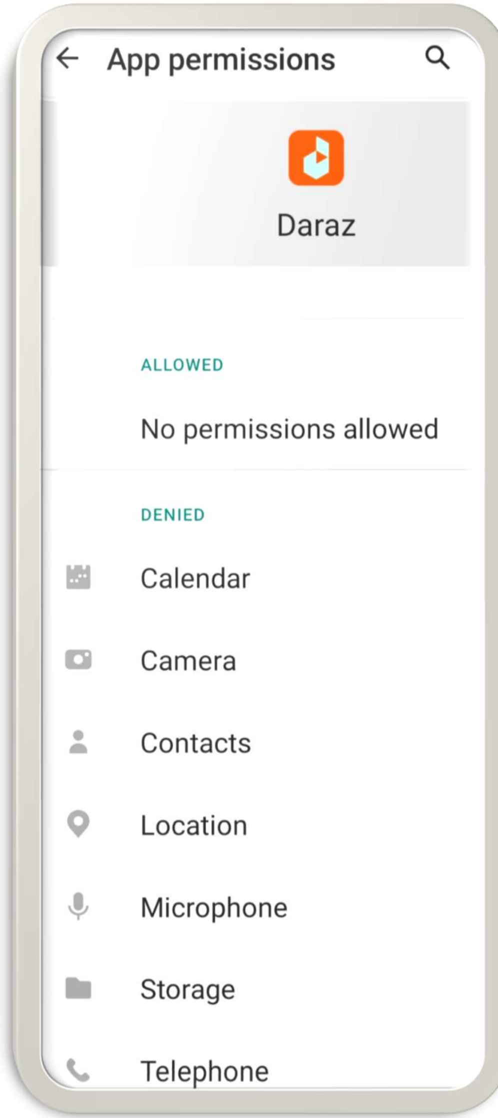
३. उपकरण र नेटवर्क सुरक्षा (Device & Network Security)

- **रिमोट डेस्कटप एक्सेस नियन्त्रण (Remote Access Software Control):**
  - प्राविधिक मर्मतका लागि बाहेक सामान्य समयमा एनिडेस्क (AnyDesk), टिमभ्युअर (TeamViewer) वा रस्टडेस्क (RustDesk) जस्ता रिमोट एक्सेस सफ्टवेयरहरू कम्प्युटरमा ब्याकग्राउन्डमा खुला राख्दै नराख्ने ।
- **इन्टरनेट अफ थिंग्स उपकरण सुरक्षा (IoT Device Isolation):**
  - सहकारीमा प्रयोग हुने सीसीटीभी क्यामेरा (CCTV), हाजिरी मेसिन (Biometric Attendance) र स्मार्ट टिभीहरूलाई मुख्य वित्तीय सफ्टवेयर चल्ने कम्प्युटर र सर्भरको नेटवर्कभन्दा छुट्टै नेटवर्क (VLAN) मा राख्ने ।
- **एप अनुमति व्यवस्थापन (Mobile App Permissions):**
  - संस्थागत कामकाजका लागि प्रयोग हुने मोबाइलहरूमा कुनै पनि नयाँ एप डाउनलोड गर्दा मागिने अनावश्यक अनुमतिहरू (जस्तै: SMS, Contacts, Camera) ध्यानपूर्वक हेरेर मात्र व्यवस्थापन गर्ने तथा एप्लिकेसनहरूलाई नियमित अपडेट गर्ने ।

Mobile App Permissions

- प्लेस्टोर (PlayStore) वा एपस्टोर (AppStore) बाट जथाभावी जुनसुकै एपहरू डाउनलोड नगर्ने र मोबाइललाई जेलब्रेक (Jail break/Root) नगर्ने ।
- हामीले प्रयोग नगर्ने पुराना वा अनावश्यक एप्लिकेसनहरूलाई मोबाइलबाट अनइन्स्टल (Uninstall) गर्ने ।
- प्रत्येक एप्लिकेसनलाई दिइएका अनुमतिहरू (Permissions) को नियमित जाँच गर्ने ।
- कुनै पनि एप्लिकेसन चलाउनका लागि जति आवश्यक छ, त्यति मात्र अनुमतिहरू दिने ।
- जस्तैः एउटा सामान्य Shopping एपले माइक्रोफोन, कन्ट्याक्ट वा क्यामेराको अनुमति माग्यो भने शङ्का गर्ने ।





४. गोपनीयता र संस्थागत आचरण (Privacy & Institutional Practices)

- **नियमित डाटा ब्याकअप (Regular Data Backup):**
  - संस्थाको महत्वपूर्ण वित्तीय विवरण, सदस्यहरूको रेकर्ड र दैनिक डाटाको नियमित रूपमा सुरक्षित क्लाउड भण्डारण वा एक्स्टर्नल हार्ड डिस्कमा सुरक्षित ब्याकअप लिने।
- **पासवर्ड जथाभाबी नलेख्ने बानी (Clean Desk Practice):**
  - आफ्ना गोप्य पासवर्ड, पिन वा संवेदनशील एकाउन्ट विवरणहरू कागजमा लेखेर कम्प्युटरको मनिटर, टेबल वा कसैले देख्ने गरी खुला ठाउँमा टाँसेर नराख्ने।
- **न्यूनतम पहुँचको नियम (Principle of Least Privilege):**
  - संस्थाभित्र जुन कर्मचारीलाई आफ्नो जिम्मेवारी पूरा गर्न जति सुविधाहरू आवश्यक पर्छ, कोर सफ्टवेयर र प्रणालीमा उसलाई त्यति मात्रै पहुँच (Access Role) प्रदान गर्ने।

४. गोपनीयता र संस्थागत आचरण (Privacy & Institutional Practices)

- **गोपनीयताको संरक्षण (Protection of Privacy):**
  - संस्थाको आन्तरिक वित्तीय विवरण, सफ्टवेयरको युजर आईडी, सदस्यहरूको व्यक्तिगत डाटा (KYM), र संवेदनशील तस्विर वा भिडियोहरू अनाधिकृत व्यक्ति वा तेस्रो पक्षसँग सेयर नगर्ने ।

- **कागजात फोहोर फाल्ने नियम (Shredding/Data Disposal Policy):**
  - सदस्यहरूको नागरिकता, कन्ट्र्याक्ट नम्बर वा खाता विवरण कोरिएका प्रिन्ट बिग्रेका कागजहरू सिधै फोहोरको टोकरीमा नफाली अनिवार्य रूपमा टुक्रा-टुक्रा पारेर (Shredder मेसिन प्रयोग गरेर) मात्र नष्ट गर्ने ।

- **बहिर्गमन व्यवस्थापन (Offboarding Access):**
  - कुनै पनि कर्मचारीले संस्थाबाट अवकाश लिएमा वा जागिर छोडेमा निजको पहुँचमा रहेका सबै प्रणालीका युजर आईडी, इमेल र पासवर्डहरू तुरुन्तै निष्क्रिय वा ब्लक गर्ने ।

५. घटना व्यवस्थापन र सचेतना (Incident Response & Awareness)

- **तुरुन्त उजुरी र रिपोर्टिङ (Reporting Mechanisms):**
  - यदि संस्थामा कुनै प्रकारको साइबर आक्रमण, शङ्कास्पद गतिविधि, वित्तीय ठगी वा अकाउन्ट ह्याक भएमा तुरुन्तै व्यवस्थापन, सम्बन्धित बैंक र **नेपाल प्रहरीको साइबर ब्युरो (Cyber Bureau)** मा लिखित उजुरी दिने ।

- **सचेतना र छलफल (Awareness & Discussion):**
  - सुरक्षित प्रविधिको प्रयोग, नयाँ डिजिटल प्रविधि र बजारमा देखा परेका नयाँ साइबर खतराहरूका बारेमा सहकारीका कर्मचारीहरू बीच समय-समयमा नियमित छलफल र तालिमको आयोजना गर्ने ।

Humans fall to be the Weakest Link in Cyber Security Chain

- हामी काममा जतिसुकै व्यस्त भए पनि साइबर सुरक्षा हाम्रो पहिलो प्राथमिकता हुनुपर्छ।
- हतारमा इमेल वा मेसेन्जरका लिङ्कहरू नबुझी क्लिक गर्दा सम्पूर्ण खाता ह्याक हुने र संस्थाको गोपनीयता संकटमा पर्ने जोखिम रहन्छ।
- त्यसैले, क्लिक गर्नु अघि सधैं विचार पुऱ्याउनुहोस्!
- **Please, Be Careful !**

Source: https://obtsynergy.com/why-you-are-your-biggest-online-security-threat/

Thank You!