

कार्यस्थल में डेटा गोपनीयता

कैंपस से कॉर्पोरेट तक: अपने डिजिटल जीवन को भारतीय संदर्भ में संचालित करना



व्यक्तिगत जीवन और सोशल मीडिया



व्यावसायिक पहचान और कॉर्पोरेट डेटा

नई वास्तविकता :
पुरानी कहावत हमेशा सही होती है...
रोकथाम इलाज से बेहतर है।

हमारी ज़िंदगी **उपकरणों** के माध्यम से जी जाती है:
लैपटॉप, स्मार्टफ़ोन, टैबलेट। ये **शिक्षा**, **वित्त** और **हमारे**
सामाजिक जीवन के लिए आवश्यक हैं।

जब आप नौकरी की तलाश करते हैं या किसी कार्यस्थल में
प्रवेश करते हैं, ये उपकरण एक **प्रवेश द्वार** बन जाते हैं। हर
क्लिक, पोस्ट और अपलोड एक स्थायी रिकॉर्ड बनाता है।



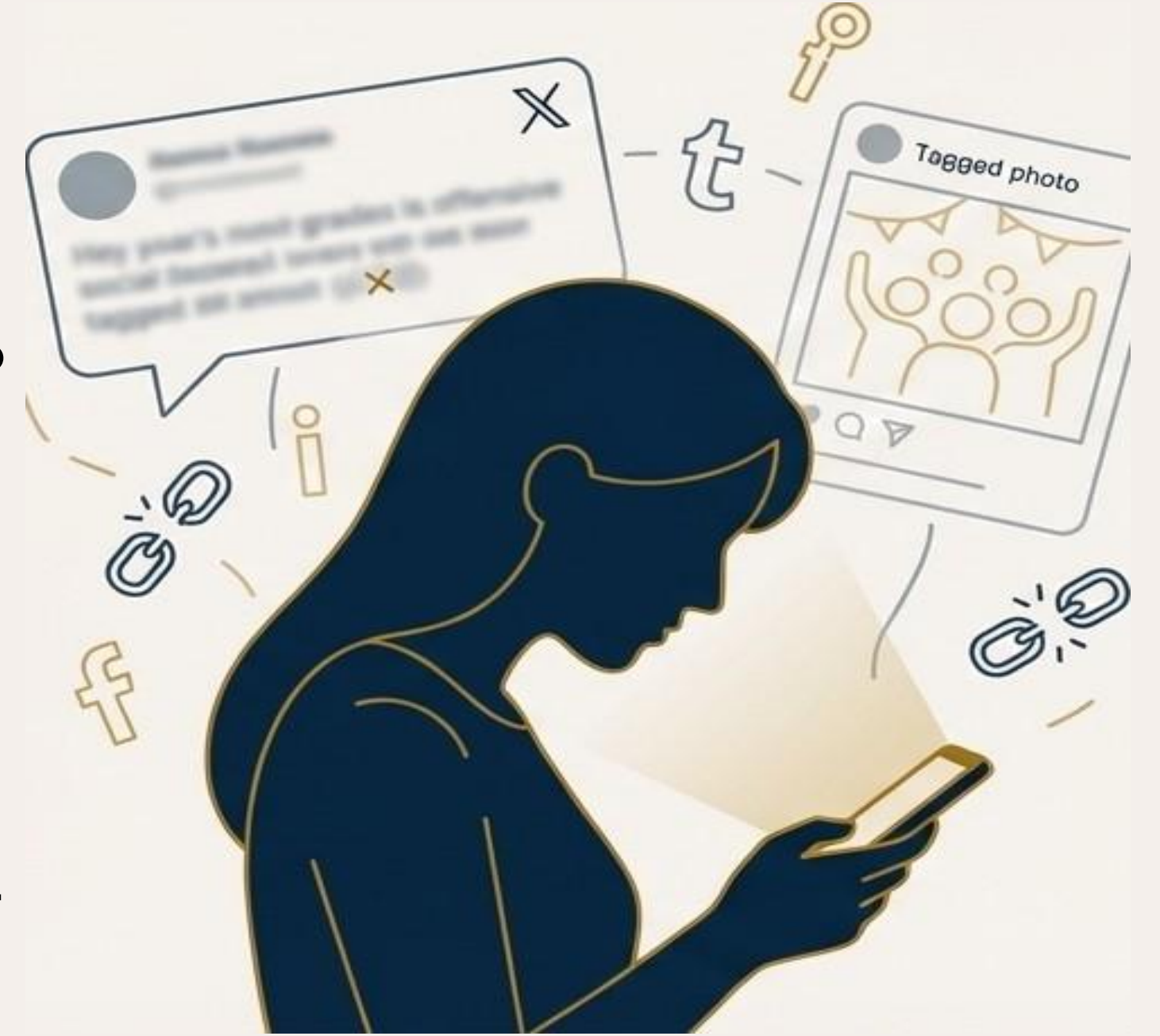
वो नौकरी जो आपको नहीं मिली

भारत में 70% नियोक्ता भर्ती से पहले सोशल मीडिया चेक करते हैं।

मिलिए प्रिया से। बेहतरीन अंक, शानदार साक्षात्कार। रिजेक्ट कर दिया गया। कारण?

एक 4 साल पुराना सार्वजनिक ट्वीट जिसमें आपत्तिजनक भाषा थी, जो 'डिजिटल बैकग्राउंड चेक' के दौरान पाया गया।

यह चेक आप इंटरव्यू कॉल पाने से पहले ही होता है।



आपकी डिजिटल छवि: पहली छाप जो आप बनाते हैं

भर्तीकर्ता क्या देखते हैं:

सार्वजनिक पोस्ट, टैग की गर्इ तस्वीरें, टिप्पणियाँ, और यहां तक कि आपकी 'लाइक्स'।

वे जिन चीज़ों की तलाश करते हैं:

पेशेवर क्षमता और संचार कौशल
भेदभावपूर्ण टिप्पणियाँ
संकट संकेत (अवैध गतिविधियाँ,
गोपनीय जानकारी का खुलासा)



खुद को गूगल करें। आपको क्या मिलता है?

'नौकरी' और 'इंटरनशिप' का जाल

किसी भी प्रतिष्ठित कंपनी से सत्यापित, आधिकारिक ऑफ़र लेटर प्राप्त होने से पहले अपना आधार, पैन या बैंक विवरण कभी भी साझा न करें।



डेटा बाज़ार : आपका रिज़्यूमे और डेटा मार्केटर्स को बेचा जाता है।

धोखा : डेटा संग्रह और धोखाधड़ी।

'वर्कप्लेस प्राइवेसी' क्या होता है?

कर्मचारी का यह अधिकार कि वे अपनी व्यक्तिगत जिंदगी और संचार को अपने पेशेवर जीवन से अलग रखें, भले ही वे काम पर हों।

नियोक्ता का अधिकार :

उत्पादकता सुनिश्चित करने, कंपनी की संपत्ति की सुरक्षा करने और सुरक्षित नेटवर्क बनाए रखने के लिए।



कर्मचारी का अधिकार :

सम्मान, व्यक्तिगत स्थान और निजी संचार का।

सर्वदर्शी नेत्र: 'बॉसवेयर' वास्तविक है

यदि डिवाइस कंपनी की है, तो इसकी कोई गोपनीयता नहीं मानें।

यह क्या है: कंपनी के लैपटॉप पर ऐसा सॉफ़्टवेयर जो कीस्ट्रोक को ट्रैक कर सकता है, दौरा किए गए वेबसाइटों का लॉग रख सकता है, और यहां तक कि हर कुछ मिनट में आपकी स्क्रीन का स्क्रीनशॉट ले सकता है।

भारतीय संदर्भ: IT सेवाओं, BPO, और कई रिमोट वर्क सेटअप्स में आम है।



केस स्टडी: जब व्यक्तिगत उपयोग कंपनी नीति से मिलता है

राहुल का दावा: "मेरी निजता का उल्लंघन!"

भारत में कानूनी वास्तविकता : कंपनी का अपनी संपत्ति की निगरानी का अधिकार लगभग हमेशा जीत जाता है।



राहुल ऑफिस के लैपटॉप पर नौकरियों की तलाश करता है



IT गतिविधि को संकेत करता है।



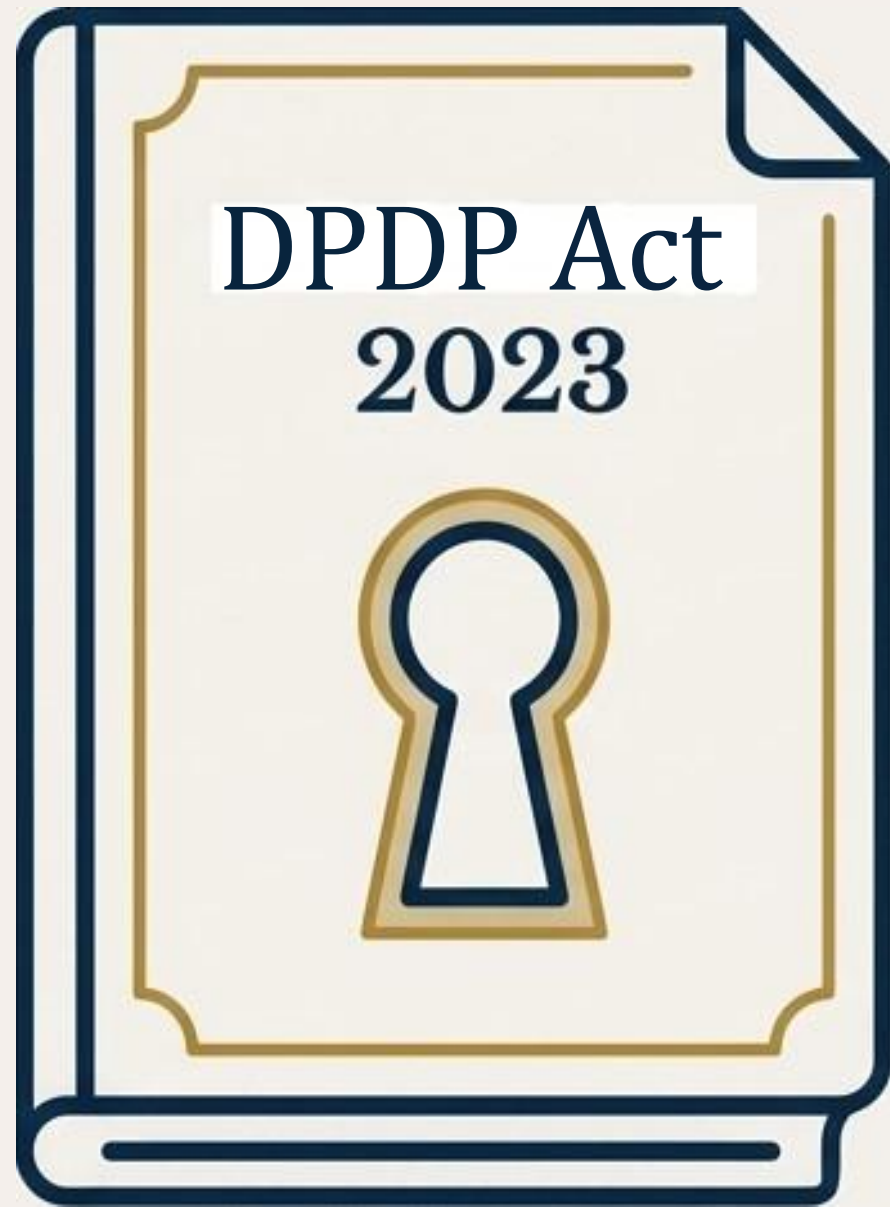
H R मीटिंग



नौकरी समाप्त होना

पाठ: अपनी नौकरी की खोज और व्यक्तिगत ब्राउज़िंग अपने 'व्यक्तिगत' डिवाइस पर अपने खुद के इंटरनेट कनेक्शन का उपयोग करके करें।

आपकी कानूनी ढाल: DPDP अधिनियम 2023



वैध उपयोग: आपका नियोक्ता आपके वेतन, उपस्थिति और करों के लिए आपके डेटा को हर बार स्पष्ट अनुमति के बिना संसाधित कर सकता है।

सीमा: वे आपका फोन नंबर किसी क्रेडिट कार्ड पार्टनर को नहीं बेच सकते और बिना आपकी स्पष्ट, विशेष सहमति के आपके डेटा का असंबंधित उद्देश्यों के लिए उपयोग नहीं कर सकते।

आपका पहुँच का अधिकार: आप औपचारिक रूप से एचआर से पूछ सकते हैं, "आप मेरे बारे में कौन सा व्यक्तिगत डेटा रखते हैं और इसका उपयोग कैसे किया जाता है?"

शिक्षकों के लिए: स्कूल एक कार्यस्थल के रूप में



स्टाफ रूम में सीसीटीवी :
सुरक्षा के लिए आमतौर पर अनुमति है, लेकिन यह खुली बातचीत को प्रभावित कर सकता है।

बायोमेट्रिक और आधार-आधारित उपस्थिति : यह संवेदनशील व्यक्तिगत डेटा है। स्कूल की इसे सुरक्षित रखने की कानूनी जिम्मेदारी है।

आपका पूछने का अधिकार : अपने डेटा की सुरक्षा के लिए लागू सुरक्षा उपायों के बारे में जानकारी प्राप्त करें।

देखभाल का दायित्व : बच्चों की ऑनलाइन जानकारी साझा करना और छात्र गोपनीयता

शिक्षक के रूप में, आप छात्र डेटा (student data) के संरक्षक हैं।



सहमति (Consent) महत्वपूर्ण है: स्पष्ट, लिखित अभिभावकीय सहमति के बिना सोशल मीडिया पर छात्रों की तस्वीरें कभी न डालें।

मेटाडेटा (Metadata) से सावधान रहें: तस्वीरों में छिपा हुआ जीपीएस डेटा होता है। एक तस्वीर पोस्ट करने से छात्र का सटीक स्थान सामने आ सकता है।

सुनहरा नियम (The Golden Rule): जब संदेह हो, तो चेहरों को धुंधला करें (blur करें) या इमोजी का उपयोग करें। अपने छात्रों की गोपनीयता की उतनी ही सख्ती से रक्षा करें जितनी आप अपनी खुद की करेंगे।

BYOD (Bring Your Own Device): अदृश्य संकट

अपने व्यक्तिगत फोन का काम के लिए उपयोग करना सीमाओं को धुंधला कर देता है।
जब आप कंपनी के ऐप्स इंस्टॉल करते हैं, तो आप "डिवाइस एडमिनिस्ट्रेटर" अनुमतियाँ दे सकते हैं।



IT एडमिन कंपनी के डेटा को हटा देता है, लेकिन आप अपनी सभी
व्यक्तिगत फ़ोटो और संपर्क भी खो सकते हैं।

वह परीक्षा जिसके लिए आपने अध्ययन नहीं किया: फ़िशिंग सिमुलेशन

कंपनियाँ अपने कर्मचारियों की सुरक्षा जागरूकता का सक्रिय रूप से परीक्षण करती हैं।



- **सिमुलेशन (Simulation):** आपकी कंपनी यह देखने के लिए नकली घोटाले वाले ईमेल भेजती है कि कौन क्लिक करता है।
- **खतरे के संकेत (The Red Flags):** तात्कालिकता ("कार्रवाई आवश्यक है!"), बेमेल यूआरएल (URL) (क्लिक करने से पहले होवर करें), और सामान्य अभिवादन ("प्रिय उपयोगकर्ता") पर ध्यान दें।
- **परिणाम (The Consequences):** क्लिक करने पर अक्सर अनिवार्य उपचारात्मक सुरक्षा प्रशिक्षण (mandatory remedial security training) लेना पड़ता है।

निर्देश 1: अपने ऑपरेटिंग सिस्टम को सुरक्षित करें



The OS Security Shield

लाइसेंस प्राप्त सॉफ्टवेयर का उपयोग करें:

पाइरेटेड सॉफ्टवेयर अक्सर छिपे हुए मैलवेयर के साथ आता है।

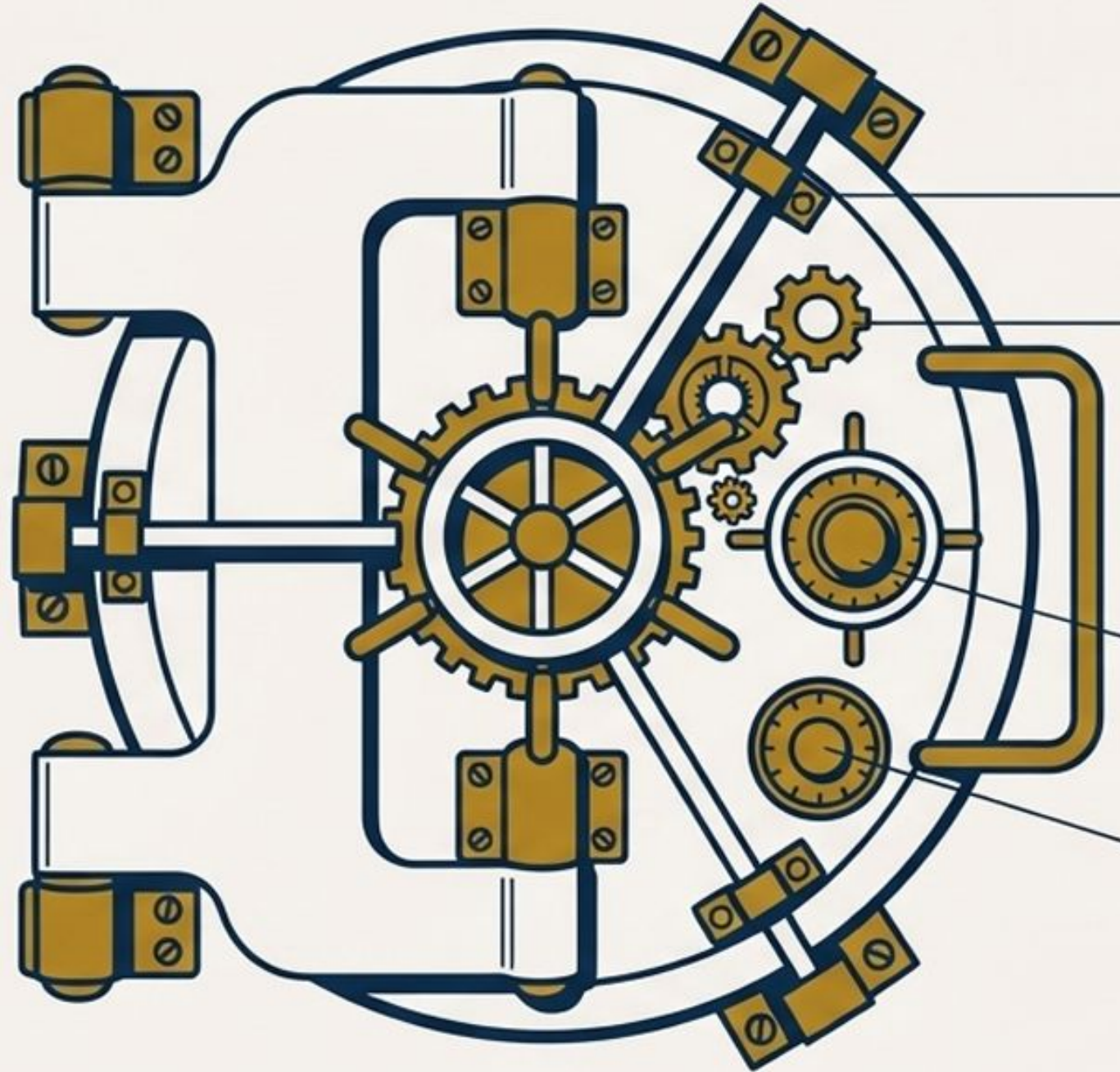
ऑटो-अपडेट सक्षम करें:

अपडेट में महत्वपूर्ण सुरक्षा पैच होते हैं जो आपको नए खतरों से बचाते हैं।

अपने डेटा का बैकअप लें:

नियमित रूप से महत्वपूर्ण फ़ाइलों को बाहरी ड्राइव या क्लाउड में सहेजें।

निर्देश 2: अटूट पासवर्ड



मजबूत पासवर्ड के लिए आपकी चेकलिस्ट :

लंबाई : कम से कम 12+ अक्षर।

जटिलता : बड़े अक्षर, छोटे अक्षर, संख्याएँ और प्रतीकों का संयोजन।

Th!5iS@g0odP4s5wD

विशिष्टता : महत्वपूर्ण खातों में कभी भी पासवर्ड को दोबारा इस्तेमाल न करें।

पासफ्रेज़ पर विचार करें : "मुश्किल वक्त कमांडो सख्त" याद रखना आसान और सुरक्षित है।

निर्देश 3: फ़ायरवॉल और सुरक्षित ब्राउज़िंग



फ़ायरवॉल आपके इंटरनेट कनेक्शन के लिए एक सुरक्षा रक्षक है। डिफ़ॉल्ट OS फ़ायरवॉल हमेशा को चालू रखें।

भिन्नता खोजने की परीक्षा

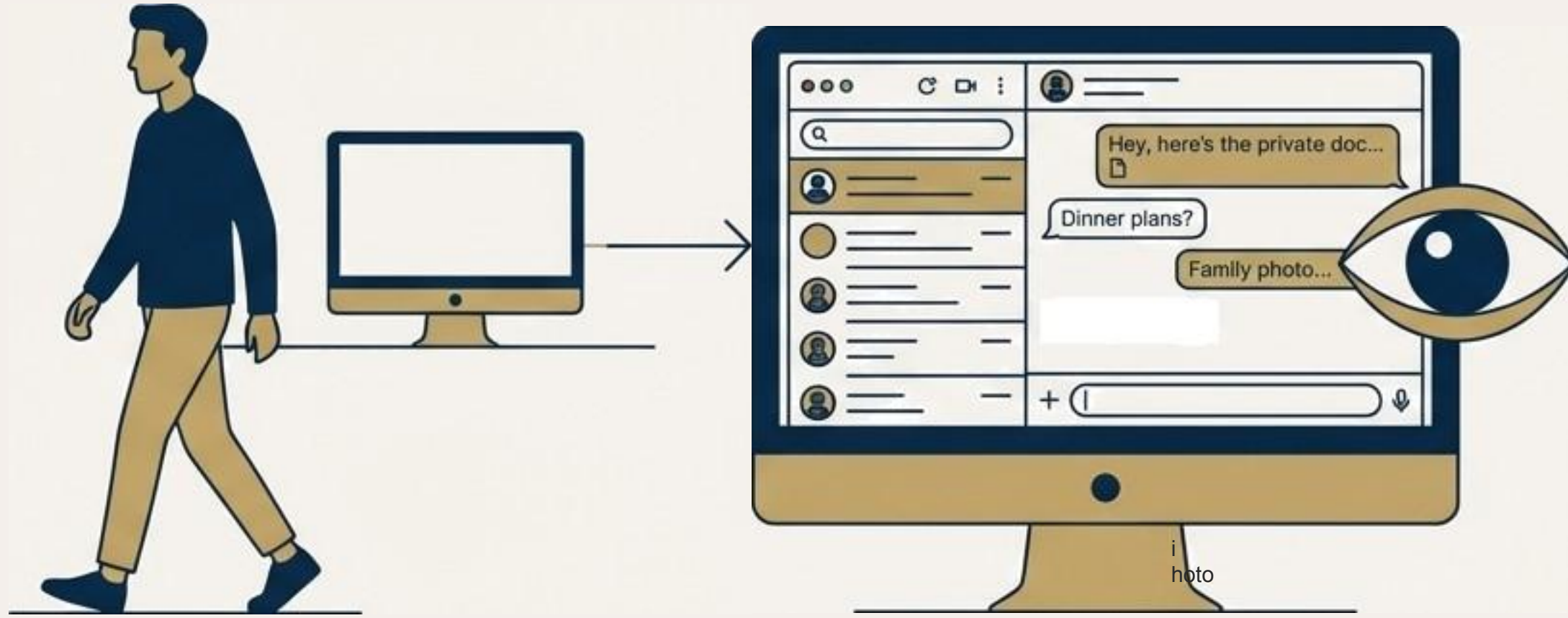
इनमें से कौन असली स्टेट बैंक ऑफ इंडिया है?

www.online-sbi.com

www.onlinesbi.sbi

सूक्ष्म वर्तनी की गलतियों से सावधान रहें (जैसे, 'G00GLE.COM').

'WhatsApp Web': गलती और लॉगआउट स्वच्छता



अगला उपयोगकर्ता या IT प्रशासक आपके निजी चैट और ईमेल तक पूरी पहुंच रखते हैं।

स्वर्णमय नियम

- ✓ **बचें:** कभी भी कार्य उपकरणों पर व्यक्तिगत खातों में लॉग इन न करें।
- ✓ **यदि आवश्यक हो:** हमेशा 'इन्कॉग्निटो' या 'प्राइवेट ब्राउज़िंग' मोड का उपयोग करें।
- ✓ **हमेशा:** सभी सेवाओं से स्पष्ट रूप से लॉग आउट करें और ब्राउज़र बंद करें।

'प्लेसमेंट रेडी' प्राइवेट चेकलिस्ट

प्लेसमेंट से 3 महीने पहले, ये करें:



खुद को गूगल करें: देखें कि क्या निकलता है। जो कुछ भी आप नहीं चाहते कि किसी भर्तीकर्ता को दिखाई दे, उसे डिलीट या अनटैग करें।



सोशलस लॉक करें: इंस्टाग्राम/फेसबुक प्रोफाइल को 'प्राइवेट' में बदलें।



लिंकडइन को साफ करें: आपकी सार्वजनिक प्रोफाइल में आपका व्यक्तिगत फोन नंबर या घर का पता नहीं होना चाहिए।



Pro



Personal

अलग ईमेल का उपयोग करें: एक पेशेवर नौकरी के आवेदन के लिए, दूसरा व्यक्तिगत/सामाजिक उपयोग के लिए।

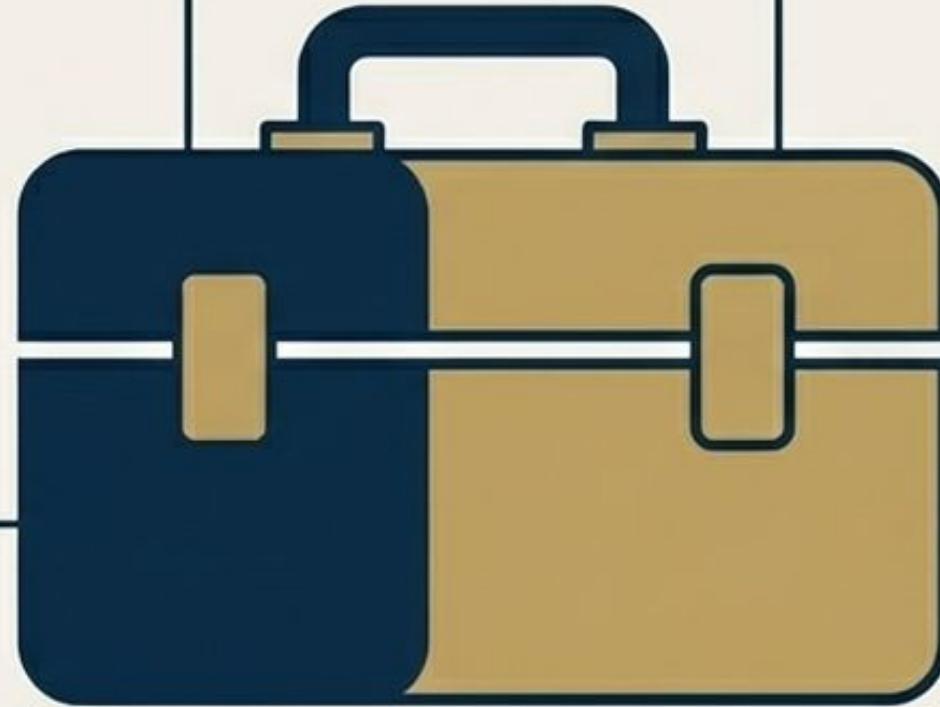
‘प्रोफेशनल हाइजीन’ किट



अपने वेबकैम को ढकें:
एक साधारण स्टिकर या स्लाइडर अनधिकृत देखने से रोक सकता है।



पासवर्ड मैनेजर का उपयोग करें: अपने सभी अद्वितीय, जटिल पासवर्ड को सुरक्षित रूप से संग्रहीत करने के लिए।

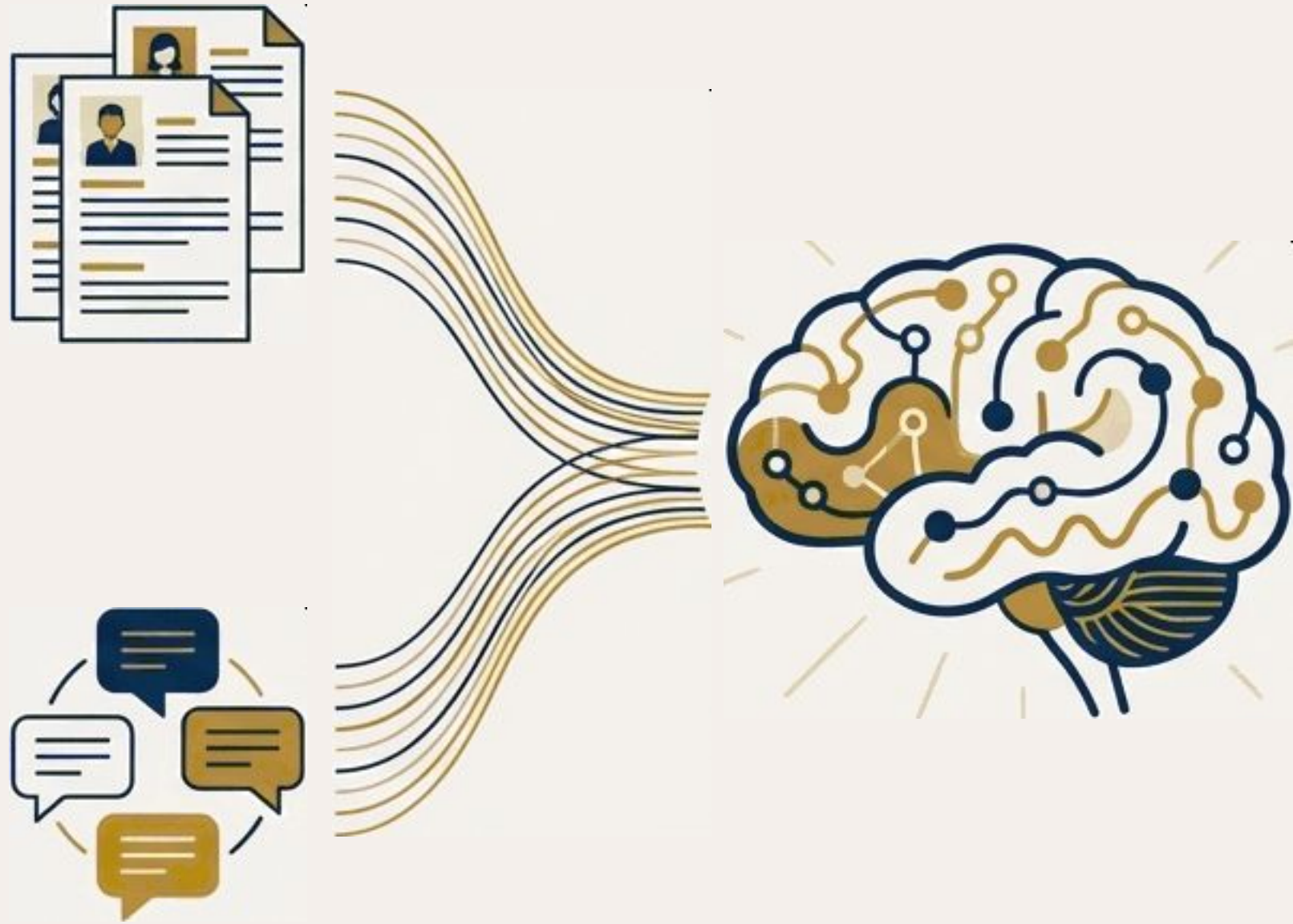


‘वर्क प्रोफाइल’ बनाएँ: अपने व्यक्तिगत कंप्यूटर पर, केवल काम के लिए एक अलग उपयोगकर्ता खाता बनाएँ।



दो-कारक प्रमाणीकरण (2FA) सक्षम करें: सभी महत्वपूर्ण खातों पर (विशेष रूप से ईमेल)।

भविष्य की झलक: कार्यस्थल में AI



भर्ती में AI: आपकी रिज्यूमे संभवतः किसी इंसान के देखने से पहले ही AI द्वारा पढ़ी जा रही है।

निगरानी में AI: भविष्य के उपकरण कंपनी चैट संदेशों का विश्लेषण 'भावनाओं' या 'असंतोष' के लिए कर सकते हैं, जिससे उन कर्मचारियों की पहचान हो सकती है जो कंपनी छोड़ने के जोखिम पर हैं।

सिद्धांत यथावत है: आप जो डिजिटल डेटा उत्पन्न करते हैं, उसके प्रति सचेत रहें। इसे इकट्ठा और विश्लेषण किया जा रहा है।

आपके तीन सुवर्ण नियम

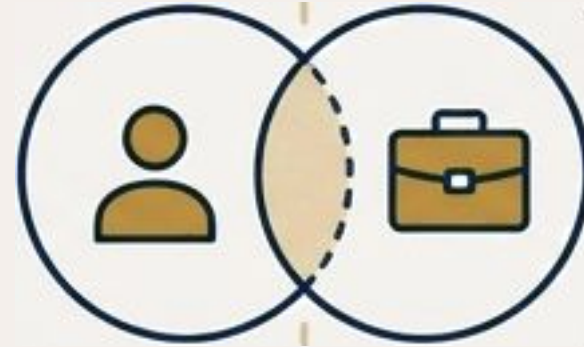
1



मान लें कि आप हमेशा सार्वजनिक क्षेत्र में हैं।

आप जो ऑनलाइन पोस्ट करते हैं उसे सालों बाद भी पाया जा सकता है। अपनी डिजिटल छाया को सावधानीपूर्वक संभालें।

2



अपने दुनिया को अलग करें

अपनी व्यक्तिगत और पेशेवर डिजिटल ज़िंदगियों को यथासंभव अलग रखें। अलग-अलग उपकरणों, खातों और नेटवर्क का उपयोग करें।

3



अपने संसाधनों के मालिक बनें, गोपनीयता के मालिक बनें

कंपनी के उपकरणों पर, निगरानी की उम्मीद करें। अपने खुद के उपकरणों पर, आप नियम तय करते हैं।

आपका पहला कदम आज से शुरू होता है

“भरोसा करना अच्छा है, पर एक अलग **Work-Phone** बेहतर है।”

आज ही घर जाएँ और अपने लिंकडइन (LinkedIn) प्रोफाइल की गोपनीयता सेटिंग्स (privacy settings) की जाँच करें। अपना फ़ोन नंबर और घर का पता सार्वजनिक दृश्य (public view) से हटा दें।



Thank You!