EDGELANDS

संवेदनशीलता के साथ डिजिटल सेफ स्पेस का डिज़ाइन: एक टूलकिट

LANDSLANDS
EDGEEDGE
LANDSLANDS

यह दस्तावेज़ एजलैंड्स इंस्टीट्यूट के 'पॉप-डाउन एंड बियॉन्ड' चरण के तहत, शोधकर्ताओं, मेंटर्स, और कलाकारों की एक टीम द्वारा आठ सप्ताह तक किए गए सहयोगी कार्यों और अतिथि वक्ताओं के इनपुट का परिणाम है।

इस प्रोजेक्ट का दृष्टिकोण है, एक ऐसी टूलकिट जिसका उद्देश्य डिजिटल सेफ स्पेस के डिज़ाइन के लिए सुझाव प्रदान करना है। यह टूलकिट प्राथमिक स्रोत विश्लेषण, केस स्टडीज और सर्वे डेटा पर आधारित है। हमें उम्मीद है कि इसका उपयोग डेवलपर्स, शोधकर्ताओं, कलाकारों और खुद ऑनलाइन यूजर्स द्वारा किया जा सकेगा

यदि आप डिजिटल सुरक्षा, इसके हितधारकों और 'डिजिटल सुरक्षित स्थान' और 'ऑनलाइन सुरक्षा' की परिभाषाओं के बारे में अधिक पढ़ना चाहते हैं, तो आप इस टूलकिट के विस्तृत संस्करण को यहां (केवल अंग्रेजी में) देख सकते हैं।

LANDSLANDS
EDGE EDGE
LANDSLANDS

अभिस्वीकृति

इस टूलकिट को पुलकित मोगरा, तातियाना लिसोवा, लिलियन ओलिविया ओटेरो, कैथरीन कीगन, नीना मार्टिन, ममाबाथो ओके, जेसिका मैकक्लर्न और जियोवाना डी कस्टोडिया ने नीना बारानोव्स्का, डैनियल ओडोंगो, विरगिनिया लेबोराओ, वैनेसा गैथेचा और लॉरा गार्सिया वर्गास के गाइडेंस में डेवलप किया है। हम उन सभी को धन्यवाद देना चाहते हैं जिन्होंने हमारा सर्वे पूरा किया और डिजिटल सेफ स्पेस बनाने के लिए सुझावों को आकार देने में मदद की। उन गेस्ट स्पीकर्स को भी खास धन्यवाद जो रिसर्च स्प्रिंट के एंकरिंग सेशन में शामिल हुए और अपनी इनसाइट्स और इंस्पिरेशन शेयर कीं। डिज़ाइन और विज़ुअल लेआउट फ्लाविया लोज़ानो और लारिसा ओलिवेरा ने बनाया था।

सारांश

यह टूलकिट कंटेंट एनालिसिस , केस स्टडीज और क्वालिटेटिव सर्वे से मिले निष्कर्षों को एक साथ प्रस्तुत करता है। इसका उद्देश्य डिजिटल सेफ स्पेस के डिज़ाइन के लिए ऐसे सुझाव देना है, जो प्लेटफॉर्म-सेंट्रिक अप्रोच' के बजाय, संवेदनशीलता और समुदाय की विशिष्ट जरूरतों को प्राथमिकता देते हैं।

➔ समस्या

भौतिक सुरक्षित स्थानों के विपरीत, डिजिटल एनवायरनमेंट में सुरक्षा के कोई स्पष्ट संकेत या पैमाने नहीं होते। ऑनलाइन सुरक्षा को मुख्य रूप से तीन पक्ष) तय करते हैं - प्लेटफॉर्म, सरकारें और समुदाय । फिर भी वर्तमान तरीके नाकाफी साबित हो रहे हैं।

प्लेटफॉर्म: प्लेटफॉर्म एक सामान्यीकृत 'औसत यूजर' को ध्यान में रखकर डिज़ाइन किए जाते हैं। यह यूजर आमतौर पर ग्लोबल नॉर्थ का श्वेत, उच्च-मध्यम वर्गीय इंसान होता है, जो सिजेंडर (जिसकी जेंडर पहचान जन्म से समान है) और विषमलैंगिक (जो विपरीत लिंग के प्रति आकर्षित है) होता है। इस वजह से, हाशिये पर रहने वाले समुदायों की कमजोरियां और जोखिम अनदेखे रह जाते हैं। कंपनियों का मुनाफा यूजर की भलाई से ज्यादा 'एंगेजमेंट मेट्रिक्स' पर टिका होता है।

सरकारें: सरकारी नियम-कानून केवल 'प्रत्यक्ष नुकसान' - जैसे बाल शोषण सामग्री, आतंकवाद और धोखाधड़ी - को रोकने तक ही सीमित रहते हैं। वे इस बात को नजरअंदाज कर देते हैं कि ऑनलाइन 'सुरक्षित महसूस करना' एक व्यक्तिगत अनुभव है जो हर व्यक्ति और संदर्भ के लिए अलग होता है।

समुदाय: समुदाय अपनी 'आचार संहिता' और स्वयंसेवकों के जरिए सुरक्षा व्यवस्था बनाए रखने की महत्वपूर्ण लेकिन नाजुक कोशिश करते हैं। इसके बावजूद, वे संरचनात्मक रूप से प्लेटफॉर्म के आर्किटेक्चर (बनावट) के अधीन ही रहते हैं।

➔ मुख्य शोध निष्कर्ष

हमारे विश्लेषण ने डिजिटल सुरक्षा के लिए चार बुनियादी शर्तों की पहचान की है:

संबंधपरक शर्तें : इसमें बिना किसी टकराव या लड़ाई के व्यक्तिगत सीमाओं का सम्मान करना शामिल है। इसमें मॉडरेशन को केवल नियम लागू करना नहीं, बल्कि रिलेशनल लेबर माना गया है। साथ ही, ऑनलाइन भागीदारी की 'भावनात्मक कीमत' को कम करना जरूरी है, ताकि इंसान को वहां मौजूद रहने के लिए लगातार अपना बचाव न करना पड़े।

सांस्कृतिक शर्तें: इसमें गरिमा और एक-दूसरे को जज न करने के सामाजिक नियम शामिल हैं। सभी भाषाओं और समुदायों के लिए भाषाई समावेशिता होनी चाहिए। साथ ही, ऐसे 'पीयर नेटवर्क' होने चाहिए जो कमजोर समूहों के लिए एक सुरक्षा कवच का काम करें।

प्रक्रियात्मक शर्तें : इसमें स्पष्ट और समान रूप से लागू होने वाले नियम शामिल हैं। इंसान को अपनी विजिबिलिटी और डेटा ट्रैकिंग पर खुद मुख्तारी होनी चाहिए। नियमों और गवर्नेंस के फैसले मनमाने कॉर्पोरेट निर्णयों के बजाय लोगों के 'जीवंत अनुभवों' पर आधारित होने चाहिए।

बुनियादी ढांचे से जुड़ी शर्तें : यह प्लेटफॉर्म की तकनीकी विश्वसनीयता और ईमानदारी से जुड़ा है। इसमें पारदर्शी डेटा प्रैक्टिस, रिपोर्टिंग के प्रभावी तरीके और सिस्टम फेल होने पर जवाबदेही शामिल है।

इन विषयों के आधार पर, सुरक्षित डिजिटल स्पेस बनाने के लिए सुझावों को तीन स्तरों में बांटा गया है:

- अत्यंत आवश्यक
- वांछनीय, और
- खतरे के संकेत।

➔ निष्कर्ष

यह टूलकिट एक व्यावहारिक गाइड होने के साथ-साथ, डिजिटल स्पेस को एक ऐसे समुदाय-संचालित वातावरण के रूप में फिर से सोचने का आह्वान है, जहाँ सुरक्षा उन लोगों द्वारा सह-निर्मित होती है जो इनका हिस्सा हैं। सुरक्षा को ऐसे कॉर्पोरेट आर्किटेक्चर द्वारा नहीं थोपा जाना चाहिए जो लोगों की भलाई (wellbeing) से ज्यादा 'एंगेजमेंट' के लिए बने हैं।

हम अपने शोध की सीमाओं को स्वीकार करते हैं, जिसमें अधिक तकनीकी दृष्टिकोणों की आवश्यकता, व्यापक सामुदायिक भागीदारी, और मूलनिवासी भाषाओं में अनुवाद शामिल है। अंत में, हम ऑनलाइन सुरक्षा के विषय से जुड़े सवालों पर और गहरी खोज का आह्वान करते हैं।

ऑनलाइन सेफ स्पेस की पहचान, निर्माण और प्रबंधन: एक मार्गदर्शिका

नीचे हमारे शोध पर आधारित, ऑनलाइन सेफ स्पेस के लिए एक मार्गदर्शिका दी गई है।

➔ अनिवार्य तत्व

पॉलिसी और दस्तावेज़ीकरण

डिजिटल स्पेस में सुरक्षा की भावना के लिए स्पष्ट और सही ढंग से तैयार किया गया दस्तावेज़ीकरण एक महत्वपूर्ण भूमिका निभाता है। सुरक्षा तब बढ़ती है जब नियम स्पष्ट, सीधे, सुलभ हों और ग्रुप में शामिल होने से पहले ही दिखाई दें। यह पारदर्शिता इंसान को सोच-समझकर फैसला लेने में मदद करती है कि क्या वह डिजिटल स्पेस उनके मूल्यों और जरूरतों से मेल खाता है, और क्या वे उसमें शामिल होना चाहते हैं या नहीं।

नियमों में स्वीकार्य व्यवहार, संवाद के तौर-तरीकों और उनके परिणामों को स्पष्ट रूप से बताया जाना चाहिए। इससे अनिश्चितता कम होती है और यह समझ बनती है कि हानिकारक व्यवहार को रोका जाएगा, जिससे सुरक्षा की भावना मजबूत होती है। इसके अलावा, यह सब ऐसी भाषा में होना चाहिए जो समुदाय के सभी संभावित सदस्यों को आसानी से समझ आए।

कम्युनिटी के नियमों में उत्पीड़न, डराने-धमकाने, विद्वेषपूर्ण भाषण, चरमपंथी सामग्री और 'पहचान के दुरुपयोग' को स्पष्ट रूप से मना किया जाना चाहिए।

अगर नियम थोड़े अस्पष्ट हैं, तो उन पर चर्चा, संशोधन और सुधार की गुंजाइश होनी चाहिए। "सकारात्मक" बातचीत जैसे गोलमोल शब्दों की जगह सम्मान, पारदर्शिता और पूर्वाग्रह-मुक्त (नॉन-जजमेंट) जैसी स्पष्ट उम्मीदें रखना नियमों को समझने और लागू करने में आसान बनाता है।

समुदाय की भागीदारी कम्युनिटी गाइडलाइंस को खुद समुदायों के योगदान से तैयार किया जाना चाहिए। इसके अलावा, जमीनी स्तर पर सदस्यों के अनुभवों के आधार पर इनकी लगातार समीक्षा और सुधार किया जाना चाहिए।

डेटा प्रशासन (डेटा गवर्नेंस) को स्पष्ट रूप से बताया जाना चाहिए कि पर्सनल डेटा कैसे इकट्ठा, इस्तेमाल, स्टोर और सुरक्षित किया जाता है। डिजिटल स्पेस में सुरक्षित महसूस करने के लिए नैतिक डेटा प्रैक्टिस, 'प्राइवेसी-बाय-डिज़ाइन' सिद्धांत और डेटा सुरक्षा के बारे में पारदर्शी जानकारी होना बहुत जरूरी है।

अगर कोई डिजिटल टूल बहुभाषी है, तो यह बहुत महत्वपूर्ण है कि डेटा सुरक्षा सहित सभी जानकारी उन सभी भाषाओं में अनुवादित हो।

अंत में, नियम तभी प्रभावी होते हैं जब वे मॉडरेटर्स और एडमिन्स सहित सभी पर समान रूप से और लगातार लागू हों। जब नियमों का पालन मनमाने ढंग से या भेदभावपूर्ण तरीके से होता है, तो भरोसा तेजी से टूटता है और इंसान खुद को अकेला या असुरक्षित महसूस करने लगता है।

तकनीकी तत्व

मजबूत और अद्यतन सुरक्षा उपकरण डिजिटल सुरक्षा के महत्वपूर्ण घटक हैं, लेकिन साथ ही उनका गोपनीयता-सम्मत, संदर्भ-संवेदी और गैर-दंडात्मक होना भी आवश्यक है। सुरक्षा का अहसास कराने वाले प्रमुख तकनीकी तत्वों में सामग्री फिल्टर, परेशान करने वाली या अवैध सामग्री का स्वचालित निष्कासन और रिपोर्टिंग तंत्र शामिल हैं। एन्क्रिप्शन, अनामिकरण तंत्र, डेटा रिसाव की रोकथाम और द्वि-स्तरीय प्रमाणीकरण जैसे अद्यतन सुरक्षा उपाय भी डिजिटल स्पेस में सुरक्षा की भावना पैदा करने के लिए महत्वपूर्ण हैं।

हालाँकि, स्वचालित मॉडरेशन अक्सर सीमा पार कर जाता है और संदर्भ की कमी या बहुत सख्त नियमों के कारण हानिरहित सामग्री को भी हटा देता है। इस तरह का अतिरेक भागीदारी को सीमित कर सकता है, जायज अभिव्यक्ति को दबा सकता है और प्लेटफॉर्म पर विश्वास को कमजोर कर सकता है। इसलिए, स्वचालित मॉडरेशन को मानवीय निगरानी के साथ मिलकर काम करना चाहिए। इसके अतिरिक्त, यदि मॉडरेशन बहुत सख्त हो, तो प्लेटफॉर्म से संपर्क करने और संदर्भ या स्पष्टीकरण देकर उसे चुनौती देने का अवसर होना चाहिए।

तकनीकी सुरक्षा का विस्तार सामुदायिक दुर्व्यवहार, निजी डेटा के दुरुपयोग और संवेदनशील या कमजोर समुदायों में शत्रुतापूर्ण घुसपैठ को रोकने के लिए भी होना चाहिए। सुरक्षा सुविधाएँ तब अधिक प्रभावी होती हैं जब वे नुकसान होने के बाद प्रतिक्रिया करने के बजाय, इन जोखिमों को सक्रिय रूप से सीमित करती हैं।

उपयोगकर्ताओं को प्लेटफॉर्म पर अपनी गोपनीयता पर नियंत्रण होना चाहिए। प्लेटफॉर्म को प्रोफाइल की दृश्यता का प्रबंधन करने, चुनिंदा व्यक्तिगत जानकारी साझा करने और भागीदारी के सार्वजनिक या निजी तरीकों के बीच चयन करने के लिए उपकरण प्रदान करने चाहिए। ये सुविधाएँ उपयोगकर्ताओं को उनकी आवश्यकताओं और जोखिमों के अनुसार अपने 'एक्सपोज़र' पर अधिक नियंत्रण देती हैं।

जब सुरक्षा के लिए गुमनामी और गोपनीयता महत्वपूर्ण होती है, तब 'असली नाम की नीतियां' हानिकारक हो सकती हैं। कई उपयोगकर्ताओं के लिए, विशेष रूप से वंचित समुदायों या राजनीतिक रूप से संवेदनशील संदर्भों से आने वाले लोगों के लिए, गुमनामी कोई पसंद नहीं बल्कि एक महत्वपूर्ण सुरक्षा उपाय है।

अंत में, प्लेटफॉर्म को विशिष्ट आवश्यकताओं वाले व्यक्तियों या समुदायों के लिए समायोजन और विकल्पों को सक्रिय रूप से और पहले से ही अपनी प्रणाली में समाहित कर लेना चाहिए, जिससे यह सुविधा एक सामान्य नियम बन जाए, न कि कोई विलासिता या ऐसी चीज जिसके लिए किसी को तर्क करना पड़े।

सामुदायिक तत्व

भौतिक सीमाओं के अभाव में, उपयोगकर्ता यह आकलन करने के लिए कि कोई जगह सुरक्षित है या नहीं, अनौपचारिक लेकिन शक्तिशाली डिजिटल संकेतों पर निर्भर करते हैं। वे दृश्य चिह्नों को खोजते हैं, जो एक तरह से प्लेटफॉर्म के 'हाव-भाव' को पढ़ने जैसा है। बायो में सर्वनाम, समावेशी प्रतीक, सामग्री चेतावनी, या फीड के सबसे ऊपर पिन की गई

'आचार संहिता'. ये सभी तत्काल संकेत देते हैं कि यहाँ सीमाएं मौजूद हैं और इस जगह को समझदारी से विकसित किया जा रहा है।

इन दृश्य संकेतों को भाषाई संकेतों द्वारा और मजबूती मिलती है, जो समुदाय के आपसी माहौल को आकार देते हैं। सुरक्षित स्थान अक्सर विरोधाभासी "हम बनाम वो" की बयानबाजी के बजाय समावेशी "हम" भाषा को अपनाते हैं, और अस्पष्टता को कम करने के लिए अक्सर 'लहजे के संकेतों' का उपयोग करते हैं। भाषा में समावेशिता और विविधता की मान्यता—सामुदायिक दिशानिर्देशों, नियमों और आचार संहिता के महत्वपूर्ण तत्व हैं। ये प्रथाएं विशेष रूप से न्यूरोडायवर्जेंट उपयोगकर्ताओं के लिए महत्वपूर्ण हैं, जिनके लिए स्पष्ट संचार चिंता और गलतफहमी को कम करता है।

अवांछित घुसपैठ को रोकने के लिए, समुदाय नए सदस्यों के लिए एक बुनियादी सत्यापन प्रक्रिया लागू कर सकते हैं। उदाहरण के लिए, एक 'प्रवेश चरण' हो सकता है, जिसमें नए सदस्यों को भाग लेने और पूर्ण एक्सेस प्राप्त करने से पहले उस स्थान के उद्देश्य, मूल्यों और सीमाओं को स्वीकार करना अनिवार्य हो।

हालाँकि, अंततः सबसे निर्णायक संकेत व्यावहारिक होता है। समुदाय के सदस्य यह देखते हैं कि नेतृत्व और संचालन व्यवहार में कैसे काम करते हैं। वे सुरक्षा का आकलन इस आधार पर करते हैं कि नुकसान और नियमों के उल्लंघन पर प्रतिक्रिया कितनी तेज, निरंतर और पारदर्शी है। जब विद्वेषपूर्ण भाषण को बने रहने दिया जाता है, या नियमों का पालन मनमाना लगता है, तो लिखित नियमों की विश्वसनीयता खत्म हो जाती है और सुरक्षा की भावना तेजी से बिखर जाती है।

समुदाय के भीतर संघर्ष या विवाद की स्थिति में, केवल रिपोर्टिंग और प्रतिबंध के उपकरणों पर निर्भर रहने के बजाय, प्लेटफॉर्म को सदस्यों को प्रोत्साहित करना चाहिए कि वे पहले विनम्रता और रचनात्मक संवाद के माध्यम से विवादों को सुलझाएं। इससे समुदाय में व्यक्ति की भूमिका फिर से स्थापित होती है। हालाँकि, जहाँ समाधान संभव न हो, वहाँ अनुशासनात्मक कार्रवाई तेजी से की जानी चाहिए।

➔ अनुशंसित चेकलिस्ट

अत्यंत आवश्यक / न्यूनतम आवश्यकताएं

- ◯ स्पष्ट, सीधे और सुलभ सामुदायिक दिशानिर्देश और नियम, और इनके टूटने पर हस्तक्षेप की व्यवस्था।
- ◯ मजबूत डेटा सुरक्षा नीति।
- ◯ निजी समुदायों के भीतर स्क्रीनशॉट लेने की सुविधा पर प्रतिबंध।
- ◯ हानिकारक सामग्री के लिए विश्वसनीय रिपोर्टिंग टूल्स।
- ◯ वैकल्पिक गुमनामी ।
- ◯ मॉडरेटर्स और एडमिन्स पर निगरानी।
- ◯ मानवीय मॉडरेटर्स जिन्हें विचलित करने वाली सामग्री से निपटने के लिए मनोवैज्ञानिक सहायता और संसाधनों तक पहुंच प्राप्त हो।
- ◯ समावेशी भाषा।
- ◯ हानिकारक भाषण या गतिविधि के खिलाफ प्रतिक्रियात्मक और सक्रिय उपाय।
- ◯ बहुभाषी प्लेटफॉर्म्स के लिए, उपयोगकर्ता समझौतों और आचार संहिता सहित सभी तत्वों का सभी भाषाओं (विशेषकर स्थानीय भाषाओं) में उचित अनुवाद।
- ◯ समर्पित इन-हाउस साइबर सुरक्षा क्षमता, विशेष रूप से जोखिम वाले समुदायों के लिए।

वांछनीय

- प्रवेश प्रक्रिया के दौरान जांच-परख।
- गोपनीयता और सुरक्षा उपायों का प्लेटफॉर्म के बुनियादी ढांचे में पहले से ही समाहित होना।
- डिजिटल स्पेस में व्यवहार और शिष्टाचार पर शैक्षिक संसाधन।
- सहभागी सह-डिज़ाइन जिसमें समुदाय की जरूरतों और प्राथमिकताओं को शामिल किया गया हो।
- ऐसे सपोर्ट एजेंट्स / मॉडरेटर्स जो उसी यूजर कम्युनिटी के सदस्य हों या कम से कम सांस्कृतिक संदर्भ का ज्ञान रखते हों, और जिनके पास विचारपूर्ण सहायता देने के लिए समय और भावनात्मक क्षमता हो।
- वास्तविक समय और प्रत्यक्ष मानवीय सहायता, उदाहरण के लिए: एक हेल्पलाइन जो सभी समय क्षेत्रों में उपलब्ध हो।
- विशिष्ट स्थानीय मानदंडों को लागू करने के लिए समर्पित एल्गोरिद्मिक टूल्स, जिसमें अल्पसंख्यक या स्थानीय भाषाएं शामिल हों।
- संरचित 'डिजिटल स्वच्छता', जैसे: 'शांत समय' या 'रात्रि समय' जिसमें मॉडरेटर्स और एडमिन्स के पास संदेशों को सीमित करने (जैसे प्रति मिनट एक संदेश) का टूल हो।

खतरे के संकेत

- नियमों को लागू करने में असंगतता, और विविध गैर-हानिकारक विचारों की सेंसरशिप।
- नुकसान के प्रति प्रतिक्रिया का लगातार अभाव, या नुकसान को "फ्री स्पीच" (अभिव्यक्ति की आज़ादी) बताकर अनुमति देना।
- वास्तविक पहचान उजागर करने की बाध्यता।
- "दिखावटी" सुरक्षा, जैसे: डिफ़ॉल्ट रूप से कम्युनिटी रूल्स को सिर्फ कॉपी-पेस्ट कर देना।
- असुरक्षित तकनीकी बुनियादी ढांचा, जैसे: घुसपैठ और डेटा लीक का खतरा।
- पारस्परिक संघर्षों को सुलझाने के लिए एल्गोरिदम या सामान्य 'सेवा की शर्तों' पर निर्भरता।

EDGELANDS

edgelands.institute