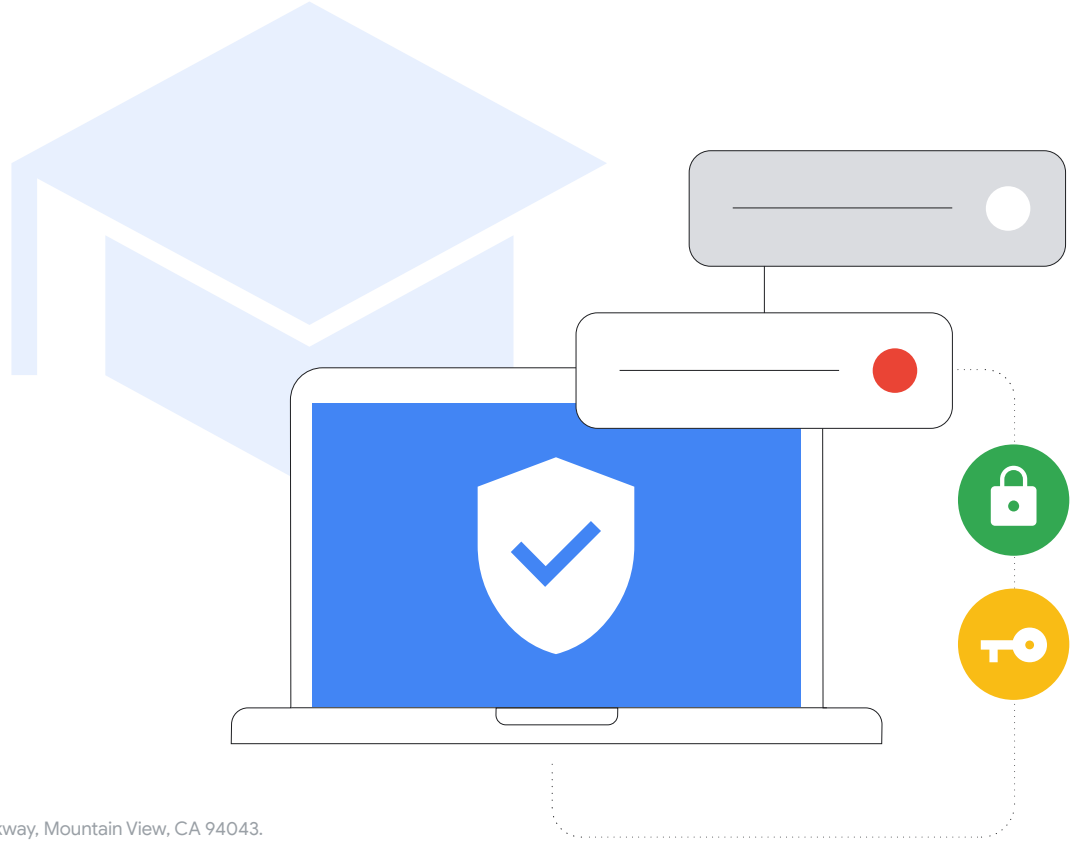
Google for Education

कडिरगार्टन से बारहवीं क्लास तक के छात्र-छात्राओं को सायबर सुरक्षा के बारे में जानकारी देने वाली गाइडबुक



Safer with Google

रपिोर्ट की खास जानकारी

जैसा कि CISA की हमारे भविष्य की सुरक्षा रपिोर्ट में हाइलाइट कयि गया है, कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों को सायबर सुरक्षा में नविेश करना चाहिए. छात्र-छात्राओं, उनके परविारों, शक्षिकों, कर्मचारयिों, और समुदायों की सुरक्षा के लिए ऐसा करना ज़रूरी है. इस दस्तावेज़ में, कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों में सायबर सुरक्षा को मज़बूत करने के दशिा-नर्दिेश दिए गए हैं और इससे जुड़े सबसे सही तरीके बताए गए हैं. इनकी मदद से स्कूल के आईटी एडमनि, हार्डवेयर और सॉफ़्टवेयर को सेट अप और कॉन्फ़गिर कर सकेंगे. दस्तावेज़ में, आम तौर पर इस्तेमाल होने वाले सबसे सही तरीकों के साथ-साथ, Google प्रॉडक्ट और सेवाओं से जुड़े खास दशिा-नर्दिेश दिए गए हैं. Google का मशिन, दुनयि भर की जानकारी को व्यवस्थति करना, इसे सबके लिए उपलब्ध कराना, और मददगार बनाना है. यह मशिन हमें Google for Education टीम के लिए, सीखने-सखिाने की प्रक्रयिा को बेहतर करने से जुड़े टूल बनाने की प्रेरणा देता है. ऐसे टूल बनाने के अनुभव को हम इस गाइड में शेयर करेंगे. यहां हमने अलग-अलग वर्षियों के आधार पर, सुरक्षा के सबसे सही तरीकों के बारे में बताया है. इनसे हार्डवेयर और सॉफ़्टवेयर को सेट अप और कॉन्फ़गिर करने से जुड़ी ज़्यादा जानकारी मलिती है. साथ ही, जोखमि कम करने की प्रोसेस के बारे में पता चलता है. हमने यह

भी बताया है कि Google, Google for Education की सेवाओं, खास तौर पर शक्षिा से जुड़े टूल के लिए सायबर सुरक्षा कैसे लागू करता है. इस दस्तावेज़ में हमने सुरक्षा के जनि तरीकों के बारे में बताया है वे कसिी भी प्रॉडक्ट या सेवा के लिए अपनाए जा सकते हैं. हमारा मानना है कि दूसरे प्रॉडक्ट और सेवाओं के मुकाबले, हमारे प्रॉडक्ट आम सायबर हमलों से बेहतर सुरक्षा देते हैं.

खतरा

शक्षिण संस्थान अक्सर सायबर हमलों का टॉप टारगेट रहते हैं, क्योंकि बुरे मकसद से काम करने वाले लोग, स्कूलों के बड़े डेटा को अपने फ़ायदे के लिए इस्तेमाल करना चाहते हैं. फ़लिहाल, 46% स्कूल अब तक सायबर हमलों से बचे हुए हैं. हालांकि, उनका मानना है कि वे भी ज़्यादा दनि तक सुरक्षति नहीं रह पाएंगे, क्योंकि रैंसमवेयर हमले बहुत ऐडवांस होते जा रहे हैं और उन्हें रोक पाना मुश्कलि होता जा रहा है. इनमें से 42% स्कूलों का मानना है कि रैंसमवेयर इतना आम हो गया है कि इससे बचना अब नामुमकनि है. साल 2020 में, स्कूलों को अचानक से डस्टिेंस लर्निंग को अपनाना पड़ा था. इस वजह से ही सायबर हमलों में बढ़ोतरी आई, क्योंकि स्कूल इनसे लड़ने के लिए पूरी तरह तैयार नहीं थे.

बचाव

इन हमलों को कम कयि जा सकता है. फ़लिहाल, ऐसी कोई भी टेक्नोलॉजी नहीं है जो सायबर हमलों के जोखमि को पूरी तरह से खत्म कर दे. हालांकि, अगर शक्षिा के क्षेत्र से जुड़े लोग और एडटेक वेंडर, सुरक्षा के सबसे सही तरीकों को अपनाने और लागू करने के लिए, साथ मलिकर काम करें, तो इन्हें काफ़ी हद तक कम कयि जा सकता है. साथ ही, प्लैटफ़ॉर्म की सुरक्षा बेहतर की जा सकती है. शक्षिण संस्थान अपने टूल, उपयोगकर्ताओं, और डेटा को सुरक्षति करने के लिए, सावधानी बरत सकते हैं और सुरक्षा से जुड़ी नीतयिां लागू कर सकते हैं. ऐसा करके, वे सायबर हमलों को कम कर सकेंगे और उन्हें बेहतर ढंग से मैनेज कर सकेंगे.

अहम सुझाव:

- **पहचान की पुष्टि करने के सुरक्षति तरीके इस्तेमाल करें** संवेदनशील जानकारी, ईमेल, फ़ाइलों, और बाकी कॉन्टेंट को सुरक्षति रखने के लिए, पहचान की पुष्टि करने के सुरक्षति तरीके इस्तेमाल करें. साथ ही, ऐसे लोग शक्षिा से जुड़े सस्टिम को ऐक्सेस न कर पाएं जनिके पास अनुमति नहीं है, यह पक्का करने के लिए भी ये तरीके अपनाएं. जहां संभव हो, उपयोगकर्ता की पुष्टि करने के लिए सबसे सही तरीके इस्तेमाल करें. इनमें मज़बूत पासवर्ड सेट करना, दो चरणों में पुष्टि की सुवधिा (2SV), पासकी, और पासवर्ड मैनेज करने वाले ऐप्लकिेशन इस्तेमाल करना शामलि है. खास तौर पर, उन आईटी एडमनि और कर्मचारयिों को इन तरीकों का इस्तेमाल करना चाहिए जो संवेदनशील जानकारी को ऐक्सेस करते हैं.
- **सुरक्षा से जुड़ी सही सेटगि लागू करें** अपने उपयोगकर्ताओं, डेटा, और प्लैटफ़ॉर्म को सुरक्षति रखने के लिए, सुरक्षा से जुड़ी सही सेटगि लागू करें. Google के प्रॉडक्ट, डफ़िॉल्ट रूप से सुरक्षति होते हैं. हालांकि, उन्हें सुरक्षति तरीके से इस्तेमाल करने के लिए यह ज़रूरी है कि एडमनि, नेटवर्क और सस्टिम को सही तरीके से कॉन्फ़गिर करके, उनका इस्तेमाल करें. स्कूलों को सुरक्षति रखने के लिए, ज़ीरो ट्रस्ट और कम से कम अधकिार जैसे सद्धिांतों को लागू करें: उपयोगकर्ताओं के पास सरि्फ़ उन सॉफ़्टवेयर, डेटा, ऐप्लकिेशन, और सस्टिम का ऐक्सेस होना चाहिए जनिकी ज़रूरत उन्हें अपना काम सही ढंग से करने के लिए होती है.
- **अपने सस्टिम अपडेट और अपग्रेड करें** अपने उपयोगकर्ताओं को नए खतरों से सुरक्षति रखने के लिए, सस्टिम अपडेट और अपग्रेड करते रहें. मॉडर्न ऑपरेटगि सस्टिम (ओएस) और ब्राउज़र इस्तेमाल करें. साथ ही, पक्का करें कि उपयोगकर्ताओं के सभी डवािइसों पर, नए सॉफ़्टवेयर वर्शन या स्वीकार कयि गए लॉन्ग-टर्म स्टेबल वर्शन चल रहे हैं और वे अपने-आप अपडेट भी होते हैं. Chromebook जैसे ज़्यादा सुरक्षति डवािइस पर अपग्रेड करने से भी सुरक्षा बढ़ सकती है. आज तक कसिी भी ChromeOS डवािइस पर कोई भी रैंसमवेयर हमला नहीं हुआ है.
- **रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सस्टिम का इस्तेमाल करें** अपने डवािइस की सुरक्षा बढ़ाने और संभावति समस्याओं को तेज़ी से कम करने के लिए, इस सस्टिम का इस्तेमाल करें. साथ मलिकर काम करने और कम्यूनकिेशन से जुड़े सॉफ़्टवेयर (जैसे, Google Workspace for Education) में पहले से मौजूद इन सुवधिाओं का इस्तेमाल कयि जा सकता है. इसके अलावा, सुरक्षा से जुड़े इवेंट को लॉग करने और इन्हें मॉनटिर करने से जुड़ी सुवधिाओं को अलग से डप्लिॉय कयि जा सकता है. अपने स्कूल के नेटवर्क, डवािइसों, ऐप्लकिेशन, उपयोगकर्ताओं, और डेटा से जुड़ी गतविधियिों को ट्रैक करते रहें. खाते में लॉगनि कए जाने, फ़ाइल शेयर कए जाने, ईमेल की संख्या (खास तौर पर, फ़शिगि और मैलवेयर वाले ईमेल), डवािइस पर की गई गतविधि, और कॉन्फ़गिरेशन में हुए बदलावों पर नज़र रखें. खतरों, अहम इवेंट, और सस्टिम में हुए बदलावों के बारे में सूचनाएं पाने के लिए, सूचना देने वाले और मॉनटिर करने वाले अपने प्लैटफ़ॉर्म को अप-टू-डेट रखें.
- **शक्षिकों, कर्मचारयिों, और छात्र-छात्राओं को ट्रेनगि दें** डवािइसों और सॉफ़्टवेयर को सुरक्षति तरीके से इस्तेमाल करने, संभावति खतरों को पहचानने, और उनकी रपिोर्ट करने की ट्रेनगि शक्षिकों, कर्मचारयिों, और छात्र-छात्राओं को दें. साथ ही, सबसे आम हमलों से बचने के लिए डेटा को सही तरीके से शेयर करने के बारे में भी उन्हें सखिाएं. स्कूल या डस्टिट्रक्टि, सबके लिए उपलब्ध पहले से तैयार ट्रेनगि मटीरयिल के साथ-साथ अपना ब्रैंडेड ट्रेनगि मटीरयिल इस्तेमाल करके, स्कूलों के लिए एक बेहतर टूलकटि बना सकते हैं.

[1] https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Google के प्रॉडक्ट के उपयोगकर्ताओं के लिए सुझाव:

Google Workspace for Education और Chromebook जैसे Google प्रॉडक्ट, आपके स्कूल की सायबर सुरक्षा को बढ़ा सकते हैं. साथ ही, इनकी मदद से इन सभी सुझावों को आसानी से लागू किया जा सकता है. ये सारे प्रॉडक्ट एक साथ इस्तेमाल करने पर ऐसी सुविधाएं देते हैं जो उपयोगकर्ताओं की निजता को सुरक्षित रखने में मदद करती हैं और आपके संस्थान के लिए सबसे बेहतर सुरक्षा देती हैं.

इन रणनीतियों और इस दस्तावेज़ में दिए गए अतिरिक्त दिशा-निर्देशों की मदद से, किंडरगार्टन से बारहवीं कक्षा तक के संस्थानों को सायबर हमलों से सुरक्षित रखा जा सकता है.

शिक्षा के बारे में Google का नज़रिया

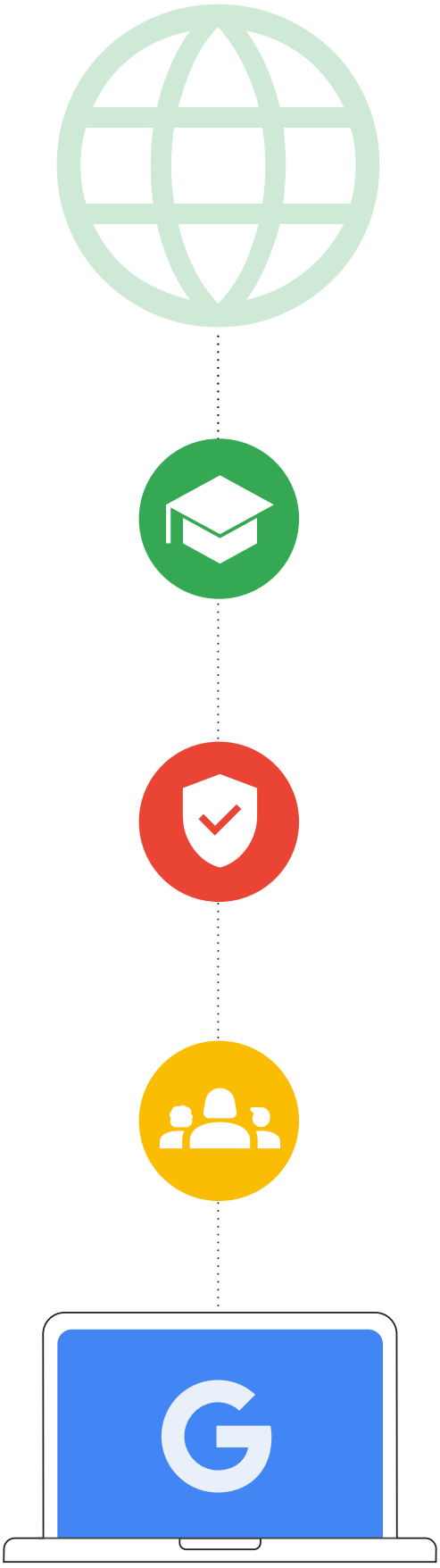
Google का मिशन, दुनिया भर की जानकारी को व्यवस्थित करना, इसे सबके लिए उपलब्ध कराना, और मददगार बनाना है. शिक्षा के क्षेत्र में भी Google का यही मिशन है. Google for Education की टीम में, हम Chromebook और Google Classroom जैसे टूल बनाकर ऐसा करते हैं. इन टूल की मदद से, छात्र-छात्राएं और शिक्षक आसान और सुरक्षित तरीके से अपना कॉन्टेंट बना सकते हैं, शेयर कर सकते हैं, और व्यवस्थित कर सकते हैं. साथ ही, ऑनलाइन टूल और शिक्षा से जुड़े संसाधनों को ऐक्सेस और इस्तेमाल कर सकते हैं.

स्कूलों को ऐसी टेक्नोलॉजी उपलब्ध कराना ज़रूरी है जो डिफ़ॉल्ट रूप से सुरक्षित हों, जिन्हें निजता को ध्यान में रखकर डिज़ाइन किया गया हो, जिस पर आपका पूरा कंट्रोल हो, और जिनमें भरोसेमंद कॉन्टेंट और जानकारी हो. Chromebook और Google Workspace for Education जैसे प्रॉडक्ट की मदद से, स्कूलों को सबसे अच्छी सुरक्षा मिलती है, जो दुनिया भर के शिक्षा के क्षेत्र से जुड़े नियम-कानूनों का पालन करती है. साथ ही, इनसे आईटी एडमिन को अपने डेटा और सुरक्षा नीतियों के बारे में साफ़-साफ़ जानकारी मिलती है और उन पर पूरा कंट्रोल मिलता है. इसके अलावा, इनकी मदद से छात्र-छात्राएं, सीखने-सिखाने के सुरक्षित माहौल में पढ़ाई कर पाते हैं. इन सुरक्षित प्लैटफ़ॉर्म पर, उम्र के हिसाब से कॉन्टेंट उपलब्ध कराया जाता है और स्पैम और सायबर हमलों से पूरी सुरक्षा दी जाती है.

हर किसी को सीखने-सिखाने का एक सुरक्षित माहौल देने के लिए, हमने अपने प्रॉडक्ट और सेवाओं में पहले से ही सुरक्षा सुविधाएं और कंट्रोल दिए हैं. साथ ही, निजता से जुड़े कड़े मानकों का पालन किया है और सुरक्षा से जुड़े बेहतर टूल के विकल्प दिए हैं. ChromeOS डिवाइस, स्कूलों पर होने वाले सायबर हमलों को कम करने में मदद करते हैं. साथ ही, ये रैंसमवेयर से सबसे अच्छा बचाव करते हैं, जो स्कूलों के लिए सबसे बड़ा खतरा है. Chromebook को आज तक कोई भी रैंसमवेयर हमला नुकसान नहीं पहुंचा पाया है.

Google Workspace for Education, क्लाउड-आधारित कम्यूनिकेशन और साथ मिलकर काम करने की सुविधा देने वाले, दुनिया के सबसे लोकप्रिय और सुरक्षित सुइट में से एक है. यहां दिए गए सुझावों के हिसाब से, हमारा हर प्लैटफ़ॉर्म सायबर हमलों से कैसे सुरक्षित करता है, इस बारे में ज़्यादा जानने के लिए कृपया आखिरी सेक्शन देखें.

इस दस्तावेज़ के दो सेक्शन हैं. पहले सेक्शन में, किंडरगार्टन से बारहवीं कक्षा तक के संस्थानों की आम सुरक्षा के दिशा-निर्देश दिए गए हैं. भले ही, सुरक्षा के लिए कोई प्रॉडक्ट इस्तेमाल किया जा रहा हो या नहीं. दूसरे सेक्शन में, Google Workspace for Education और Chromebook जैसे Google for Education प्रॉडक्ट का इस्तेमाल करने वाले संस्थानों के लिए, कॉन्फ़िगरेशन से जुड़े दिशा-निर्देश दिए गए हैं. दोनों ही सेक्शन में, आपको और आपके छात्र-छात्राओं को सायबर हमलों से सुरक्षित रहने के बारे में जानकारी मिलेगी.



बुनियादी जानकारी

कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों के डिवाइस और नेटवर्क, दोनों पर ही सायबर हमलों का बड़ा खतरा रहता है. यह बेहद ज़रूरी है कि कडिरगार्टन से बारहवीं कक्षा तक के संस्थान सुरक्षा के सबसे अच्छे तरीकों का इस्तेमाल करें, ताकि छात्र-छात्राएं सुरक्षित रहें. साथ ही, इन हमलों से होने वाले डेटा, सेवाओं, संसाधनों, समय, और पैसों के नुकसान को रोका जा सके. (सोर्स)

इस गाइड का मकसद, स्कूल एडमिन और स्कूल सिस्टम को सायबर सुरक्षा की अहमियत समझाना है. साथ ही, उन्हें इस बात के लिए बढ़ावा देना है कि वे अपने स्कूल के डेटा को बेहतर ढंग से सुरक्षित करने के लिए, सुरक्षा से जुड़े सबसे सही तरीकों का इस्तेमाल करें. सबसे सही इन तरीकों को लागू करके, कडिरगार्टन से बारहवीं कक्षा तक के संस्थान अपने एजुकेशनल सिस्टम पर होने वाले गंभीर सायबर हमलों को कम कर सकते हैं या रोक सकते हैं और इनसे होने वाले पैसों के नुकसान से भी बच सकते हैं. साथ ही, छात्र-छात्राओं, परिवारों, शिक्षकों, और कर्मचारियों की सुरक्षा भी कर सकते हैं.

आज-कल स्कूलों पर सायबर हमलों के गंभीर मामले काफ़ी बढ़ रहे हैं. कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों की सायबर सुरक्षा से जुड़े संसाधन केंद्र के मुताबिक, 2016 और 2021 के बीच सभी 50 स्टेट में, शिक्षण संगठनों पर 1,300 से ज़्यादा सायबर हमले हुए. इनके बारे में सार्वजनिक तौर पर जानकारी दी गई थी. सभी एजुकेशन लीडर को छात्र-छात्राओं, शिक्षकों, और कर्मचारियों के डेटा और निजी जानकारी के साथ-साथ, उनके संस्थान के सिस्टम और जानकारी की सुरक्षा भी करनी चाहिए. यह एक मुश्किल काम है, क्योंकि दूसरे क्षेत्रों की तुलना में, शिक्षा के क्षेत्र में सायबर सुरक्षा को लागू करने में पहले भी काफ़ी दिक्कतें हुई हैं.

सायबर हमलों, जैसे रैंसमवेयर, फ़िशिंग, मैलवेयर वगैरह से, व्यक्तिगत पहचान से जुड़ी जानकारी का बड़े पैमाने पर गलत इस्तेमाल हो सकता है और डेटा के बदले भारी रकम चुकानी पड़ सकती है (साल 2020 की तुलना में, फिरौती की औसत रकम 5 गुना बढ़कर $8,12,260 हो गई है). साथ ही, ऐसे हमले शिक्षा और स्कूल के अन्य कामों में काफ़ी लंबे समय तक के लिए रुकावट डाल सकते हैं. हाल ही में, रैंसमवेयर हमले से एक स्कूल का पूरा सिस्टम बंद हो गया. इससे पूरी स्कूल कम्यूनिटी पर असर पड़ा, क्योंकि छात्र-छात्राएं कई दिनों तक स्कूल नहीं जा पाए. सीमित संसाधनों और कम फ़ंडिंग की वजह से, कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों पर ऐसे हमलों का खतरा बना रहेगा. यह स्थिति तब तक नहीं बदलेगी, जब तक वे सायबर सुरक्षा में ज़्यादा निवेश नहीं करेंगे.

कम्यूनिकेशन, साथ मिलकर काम करने, और साझेदारी के ज़रिए, सबसे अच्छी तरह से सायबर सुरक्षा उपलब्ध कराई जा सकती है. इस दस्तावेज़ में, Google के सुरक्षा से जुड़े सुझाव, नैशनल इंस्टिट्यूट फ़ॉर स्टैंडर्ड्स ऐंड टेक्नोलॉजी के सायबर सुरक्षा फ्रेमवर्क, और साल 2023 की CISA की 'कडिरगार्टन से बारहवीं कक्षा तक के स्कूलों के लिए सायबर सुरक्षा से जुड़ी टूलकिट और सुझाव' में दिए गए सुझावों को शामिल किया गया है. इन सभी संसाधनों में सायबर सुरक्षा से जुड़े सबसे सही तरीके बताए गए हैं और इन्हें ज़्यादातर जगहों पर अपनाया जाता है. इस दस्तावेज़ में उन आम तरीकों पर चर्चा की गई है जिन्हें आईटी एडमिन को अपनाना चाहिए या अपनाने पर विचार करना

चाहिए. साथ ही, Google के प्रॉडक्ट इस्तेमाल करने के दिशा-निर्देश और सबसे सही तरीकों को शेयर किया गया है. इसके अलावा, अन्य कंपनियों की सुरक्षा से जुड़े दिशा-निर्देशों और सेवाओं पर भी चर्चा की गई है. एडमिन को प्रॉडक्ट बनाने वाली कंपनियों के सुरक्षा से जुड़े सभी दिशा-निर्देशों की समीक्षा करनी चाहिए और उनके सबसे नए दिशा-निर्देशों को लागू करना चाहिए, क्योंकि ये कंपनियां ही अपने प्रॉडक्ट और उनमें होने वाले किसी भी बदलाव के बारे में सबसे अच्छी तरह से बता सकती हैं.

नीचे दिए गए सुझावों को लागू करने से पहले, आपको इन बातों पर भी ध्यान देना चाहिए::

इन बातों का ध्यान रखें

1. **सभी छात्र-छात्राओं की सुरक्षा.**

   अलग-अलग स्कूलों की अलग-अलग ज़रूरतें होती हैं. ऐसे में, हो सकता है कि कुछ स्कूलों को अपने छात्र-छात्राओं और उनके डेटा की सुरक्षा के लिए, कुछ और तरीके अपनाने की ज़रूरत हो. कई एडटेक टूल में, उम्र के हिसाब से कॉन्टेंट ऐक्सेस करने की सुविधाएं होती हैं. जैसे- आपत्तिजनक कॉन्टेंट का ऐक्सेस सीमित करना या यह पक्का करना कि छात्र-छात्राओं की जगह और संपर्क की जानकारी किसी से शेयर न की जाए.

2. **आपके डिवाइसों में किस तरह का डेटा सेव है.**

   अगर आपके डिवाइसों में संवेदनशील डेटा सेव किया गया है, तो आपको अपना डेटा एन्क्रिप्ट करना होगा या उसे किसी अलग जगह पर स्टोर करना होगा.

3. **आपके पास किस तरह के डिवाइस हैं और आपका डिप्लॉयमेंट मॉडल क्या है.**

   डिवाइसों और उनके ऐप्लिकेशन को अपने-आप अपडेट होना चाहिए, ताकि सुरक्षा को बेहतर किया जा सके, डेटा को एन्क्रिप्ट किया जा सके, और खातों को दूसरे खातों से अलग किया जा सके. साथ ही, इससे यह भी पक्का किया जा सकेगा कि उपयोगकर्ताओं की जानकारी का ऐक्सेस सिर्फ़ उनके पास है.

4. **आपका स्कूल, डिस्ट्रिक्ट या क्षेत्रीय नीतियां.**

   ऐसा हो सकता है कि आपके स्कूल में टेक्नोलॉजी के इस्तेमाल के लिए, कुछ अलग नीतियां लागू हों. आपको सुरक्षा से जुड़े सभी उपाय, इन नीतियों के अनुसार लागू करने होंगे.

Gmail, फ़िशिंग की
10 करोड़
कोशिशों को हर दिन ब्लॉक करता है.

Google हर हफ़्ते
300,000
असुरक्षित वेबसाइटों की पहचान करता है.

हर दिन
7.4 करोड़
उपयोगकर्ता, Google के Password Manager का इस्तेमाल करते हैं.

सुरक्षा जांच की मदद से, हर साल
70 करोड़
लोग अपनी सायबर सुरक्षा को मज़बूत बनाते हैं.

पहचान की पुष्टि करने के सुरक्षित तरीके इस्तेमाल करें

सभी स्कूलों और शिक्षा से जुड़े अन्य संस्थानों को, पहचान की पुष्टि करने के सुरक्षित तरीके का इस्तेमाल ज़रूर करना चाहिए. साल 2022 की चौथी तिमाही में हुए सभी सायबर हमलों में से 48% हमलों की वजह, वे खाते हैं जिनका पासवर्ड या उपयोगकर्ता नाम कमज़ोर, डिफ़ॉल्ट या पुराना था. कुछ प्रमुख सुझावों को लागू करने से, उपयोगकर्ताओं की पहचान की पुष्टि करने में मदद मिल सकती है. साथ ही, हर उपयोगकर्ता को उसकी भूमिका के हिसाब से, कुछ खास डेटा का ऐक्सेस दिया जा सकता है.

आईटी एडमिन को, दो चरणों में पुष्टि यानी दो तरीकों से पुष्टि की सुविधा को लागू करना चाहिए. साथ ही, जहां संभव हो, बिना पासवर्ड के पुष्टि करने की सुविधा यानी पासकी का इस्तेमाल करना चाहिए. ऐसा खास तौर पर तब करना चाहिए, जब कोई व्यक्ति कहीं और से शिक्षण संस्थान के सिस्टम को ऐक्सेस कर रहा हो. दो चरणों में पुष्टि की सुविधा से, आपके ऑनलाइन खातों की सुरक्षा एक लेवल और बढ़ जाती है. इससे हमलावरों के लिए आपके खाते का ऐक्सेस पाना मुश्किल हो जाता है.

आज-कल स्कूल कई तरह के डिवाइसों और डिप्लॉयमेंट मॉडल का इस्तेमाल कर रहे हैं. साथ ही, किंडरगार्टन से बारहवीं कक्षा तक के संस्थानों में अलग-अलग क्लास के छात्र-छात्राओं के हिसाब से, अलग-अलग तरह की टेक्नोलॉजी का इस्तेमाल किया जाता है. संस्थानों की ज़रूरत के हिसाब से, अलग-अलग उपयोगकर्ताओं और डिवाइसों के लिए अलग-अलग सुरक्षा उपायों की ज़रूरत होती है. इसी हिसाब से, सुरक्षा के सबसे सही तरीके भी अलग-अलग होंगे: आईटी एडमिन, शिक्षकों, कर्मचारियों, और बड़ी क्लास के छात्र-छात्राओं को डिवाइस असाइन किए जाते हैं. वहीं, छोटी क्लास के छात्र-छात्राओं को 'शेयर किए गए डिवाइस' दिए जाते हैं. हर ग्रुप के लिए दिए गए खास सुझावों के बारे में हमने नीचे चर्चा की है.

पुष्टि करने के कई ऐसे तरीके उपलब्ध हैं जिन्हें ज़्यादातर सेटिंग में इस्तेमाल किया जाता है और जिन्हें सबसे सही तरीकों में गिना जाता है:

- **मज़बूत पासवर्ड**
  उपयोगकर्ताओं को पहली बार साइन-इन करने पर, अपना पासवर्ड बनाने का निर्देश दें. साथ ही, एक मज़बूत पासवर्ड बनाने के लिए, कम से कम लंबाई और कुछ ज़रूरी शर्तें तय करें. पासवर्ड को लंबा रखने से और उसमें मुश्किल वर्णों का इस्तेमाल करने से, आपके खाते की सुरक्षा एक लेवल बढ़ जाती है. उपयोगकर्ताओं को बार-बार पासवर्ड बदलने के लिए न कहें, क्योंकि इससे उपयोगकर्ता परेशान होकर आसान पासवर्ड बनाने लगते हैं या पासवर्ड में न के बराबर बदलाव करते हैं. जैसे- पुराने पासवर्ड में बस एक अक्षर को जोड़कर नया पासवर्ड बना देना.
- **दो चरणों में पुष्टि की सुविधा (2SV):**
  दो चरणों में पुष्टि की सुविधा की मदद से, खातों की सुरक्षा एक लेवल और बढ़ जाती है. इस सुविधा का इस्तेमाल अक्सर ऐसे टूल के ज़रिए किया जाता है जो उपयोगकर्ता के पास पहले से मौजूद होते हैं. जैसे- सुरक्षा कुंजी या मोबाइल फ़ोन पर मौजूद ऐप्लिकेशन, जो एक बार इस्तेमाल होने वाला वेरिफ़िकेशन कोड जनरेट करता है. दो चरणों में पुष्टि की किसी भी सुविधा से, खाते की सुरक्षा बढ़ती है, लेकिन एडमिन को, टेक्स्ट या कॉल के ज़रिए भेजे गए वेरिफ़िकेशन कोड इस्तेमाल करने से बचना चाहिए. इसकी वजह है कि कई बार सायबर हमलों में, हमलावरों को उपयोगकर्ता के फ़ोन नंबर का ऐक्सेस मिल जाता है. ऐसे में, इस तरह से भेजे जाने वाले कोड उन्हें मिल जाएंगे.
- **बिना पासवर्ड के पुष्टि करने की सुविधा**
  पासकी, पासवर्ड का एक सुरक्षित और आसान विकल्प हैं. उपयोगकर्ता पिन, पैटर्न, बायोमेट्रिक सेंसर (जैसे- फ़िंगरप्रिंट या चेहरे की पहचान) से या सुरक्षा कुंजी पर टैप करके, ऐप्लिकेशन और वेबसाइटों में साइन इन कर सकते हैं. इससे उन्हें पासवर्ड याद रखने और मैनेज करने की ज़रूरत नहीं होती. ऐसा हो सकता है कि फ़िलहाल ये हर एजुकेशनल सिस्टम के लिए सही न हों, लेकिन ये पुष्टि के आम तरीकों की जगह तेज़ी से ले रहे हैं. साथ ही, इनसे ज़्यादा सुरक्षित और आसान तरीके से साइन-इन किया जा सकता है. पासकी, उपयोगकर्ताओं को फ़िशिंग हमलों से बचाती हैं, क्योंकि ये रजिस्टर की गई उनकी वेबसाइटों और ऐप्लिकेशन पर ही काम करती हैं.
- **सिंगल साइन-ऑन (SSO)**
  एसएसओ (SSO) की मदद से उपयोगकर्ता, क्रेडेंशियल के एक सेट के ज़रिए कई ऐप्लिकेशन और वेबसाइटों को ऐक्सेस कर सकते हैं. जब उपयोगकर्ताओं को क्रेडेंशियल का सिर्फ़ एक सेट याद रखना होता है, तो इस बात की संभावना कम होती है कि वे उन क्रेडेंशियल को कहीं लिखें. इसके अलावा, जब स्कूलों को उपयोगकर्ता क्रेडेंशियल के अलग-अलग सेट मैनेज नहीं करने पड़ते, तब वे आईटी सपोर्ट और सहायता डेस्क पर होने वाले खर्च को बचा सकते हैं. Google Workspace for Education मूल रूप से एसएसओ (SSO) की सुविधा देता है, ताकि उपयोगकर्ता अपने Google खाते के क्रेडेंशियल का इस्तेमाल करके, तीसरे पक्ष के ऐप्लिकेशन में लॉग इन कर सकें या सेवा देने वाली किसी अन्य कंपनी के क्रेडेंशियल का इस्तेमाल करके, अपने Google खातों में लॉग इन कर सकें.
- **पासवर्ड मैनेज करने वाले ऐप्लिकेशन**
  पासवर्ड मैनेज करने वाले ऐप्लिकेशन, मज़बूत और यूनीक पासवर्ड बनाने में, उपयोगकर्ताओं की मदद कर सकते हैं. इन ऐप्लिकेशन की मदद से, उपयोगकर्ता उन खातों और सेवाओं के लिए पासवर्ड बना सकते हैं जिनका इस्तेमाल वे अपने स्कूल और ऑफ़िस के दौरान करते हैं. इनका इस्तेमाल तब किया जा सकता है, जब एसएसओ (SSO) की सुविधा न हो. ये डिवाइस के ऑपरेटिंग सिस्टम में लॉग इन करने में मदद नहीं करते, लेकिन उपयोगकर्ता के लॉग इन करने के बाद, पासवर्ड मैनेज कर सकते हैं. Google उपयोगकर्ता, किसी भी प्लैटफ़ॉर्म में Chrome पर, ChromeOS, और Android पर पासवर्ड मैनेज करने वाले ऐप्लिकेशन का इस्तेमाल कर सकते हैं.

किसी शिक्षण संस्थान में उपयोगकर्ताओं के अलग-अलग ग्रुप की खास ज़रूरतों को, पुष्टि करने के अलग-अलग तरीकों के खास सबसेट या कॉम्बिनेशन से पूरा किया जा सकता है. ये तरीके उनकी भूमिका, उनके सिस्टम के टाइप, डेटा के उनके ऐक्सेस, और उनकी उम्र के आधार पर चुने जा सकते हैं.

स्कूल के एडमिन

एडमिन, किंडरगार्टन से बारहवीं कक्षा तक के किसी भी संस्थान के सिस्टम और ज़्यादातर डेटा को कंट्रोल करते हैं. उनके खातों की सुरक्षा पूरे सिस्टम की सुरक्षा के लिए अहम है. इस सिस्टम में, इंफ्रास्ट्रक्चर, खाते के डेटा से लेकर संस्थान के मैनेज किए जा रहे डिवाइस शामिल हैं. ऐसे में, उन्हें पुष्टि करने के सबसे अच्छे तरीकों का इस्तेमाल करना चाहिए. इनमें मज़बूत पासवर्ड, पासवर्ड मैनेज करने वाला एक अच्छा ऐप्लिकेशन, और दो चरणों में पुष्टि की सुविधा इस्तेमाल करना शामिल है. ये सारे तरीके, खाते की सुरक्षा को एक और लेवल बढ़ा देते हैं. अगर ये तरीके एक साथ इस्तेमाल किए जाएं, तो ये एडमिन खातों और एंटरप्राइज़ सेवाओं को सबसे मज़बूत सुरक्षा दे सकते हैं.

- एडमिन को सुरक्षा कुंजी या क्रिप्टोग्राफ़िक तरीके से सुरक्षित बनाई गई 'दो तरीकों से पुष्टि' सुविधा का इस्तेमाल करना चाहिए. दो तरीकों से पुष्टि की सुविधा में, एक भरोसेमंद डिवाइस के साथ प्रॉम्प्ट का इस्तेमाल किया जाता है. इसमें Google Authenticator या सिर्फ़ एक बार की जाने वाली पहचान की पुष्टि का कोड बनाने वाले किसी ऐप्लिकेशन को शामिल किया जा सकता है. साल 2019 के बाद रिलीज़ किए गए, टीपीएम चिप वाले Chromebook में एक ऐसा पावर बटन होता है जिसका इस्तेमाल, दो तरीकों से पुष्टि के लिए किया जा सकता है.
- एडमिन को अलग-अलग सेवाओं के अपने पासवर्ड सेव करने के लिए, पासवर्ड मैनेज करने वाले एक भरोसेमंद ऐप्लिकेशन का इस्तेमाल करना चाहिए, जो दो चरणों में पुष्टि की सुविधा देता हो.

असाइन किए गए डिवाइस इस्तेमाल करने वाले शिक्षक और कर्मचारी

एडमिन की तरह, शिक्षकों और कर्मचारियों के पास भी संवेदनशील जानकारी का ऐक्सेस होता है, लेकिन वे डिजिटल इंफ्रास्ट्रक्चर को कंट्रोल नहीं करते हैं. साथ ही, उनकी टेक्निकल स्किल, एडमिन की स्किल से अलग होती हैं.

- जहां कानूनी रूप से अनुमति हो, Chromebook का इस्तेमाल करने वाले शिक्षकों और कर्मचारियों को, फ़िंगरप्रिंट जैसे बायोमेट्रिक वेरिफ़िकेशन की मदद से, साइन इन करने की सुविधा मिलनी चाहिए.
- आईटी एडमिन को, दो चरणों में पुष्टि की सुविधा को लागू करना चाहिए. साथ ही, जहां संभव हो, बिना पासवर्ड के पुष्टि करने की सुविधा का इस्तेमाल करना चाहिए. ऐसा खास तौर पर तब करना चाहिए, जब कोई व्यक्ति कहीं और से शिक्षण संस्थान के सिस्टम को ऐक्सेस कर रहा हो.

असाइन किए गए डिवाइस इस्तेमाल करने वाले, बड़ी क्लास के छात्र-छात्रा (आम तौर पर ग्रेड 4+ के छात्र-छात्रा)

बड़ी क्लास के छात्र-छात्राओं को खुद को सुरक्षित रखने के बारे में बेहतर जानकारी होती है. साथ ही, आम तौर पर उन्हें पुष्टि करने के ज़्यादा सुरक्षित तरीकों का इस्तेमाल करना आता है. उन्हें जिस तरह की सेवाओं की ज़रूरत पड़ती है उनके लिए, पुष्टि करने के ये तरीके बिलकुल सही हैं. उनके पास सिर्फ़ अपने खाते और उनके साथ शेयर की गई जानकारी का ऐक्सेस होना चाहिए.

- Chromebook का इस्तेमाल करने वाले छात्र-छात्राओं को अपने डिवाइस पर तेज़ी से साइन-इन करने की सुविधा मिलनी चाहिए. इसके लिए, उन्हें डिवाइस के लिए एक खास पिन बनाने का विकल्प दिया जाना चाहिए. ऐसा हो सकता है कि कई स्कूलों में, बायोमेट्रिक सिस्टम की मदद से पुष्टि करने की सुविधा उपलब्ध न हो.
- हर छात्र/छात्रा को यूनीक पासवर्ड बनाने की सुविधा दी जानी चाहिए, जिसमें नाम, होमरूम या जन्मदिन जैसी निजी जानकारी शामिल न हो. छात्र-छात्राओं को यह सिखाया जाना चाहिए कि कैसे लंबे पासवर्ड इस्तेमाल करने से, पासवर्ड याद रखने में आसानी होती है. साथ ही, पासवर्ड मज़बूत भी बनता है.

शेयर किए गए डिवाइस इस्तेमाल करने वाले, छोटी क्लास के छात्र-छात्रा (आम तौर पर किंडरगार्टन से तीसरी कक्षा के छात्र-छात्रा)

सबसे कम उम्र के छात्र-छात्रा, सीखने-सिखाने से जुड़ी टेक्नोलॉजी को इस्तेमाल करना सीख ही रहे होते हैं. ऐसे में, उन्हें पुष्टि करने के आसान तरीके उपलब्ध कराने चाहिए. ये तरीके, उन्हें मिलने वाली सीमित सेवाओं और डेटा के हिसाब से भी सही रहते हैं.

- जो स्कूल अपने सबसे कम उम्र के छात्र-छात्राओं के लिए, तीसरे पक्ष की पासवर्ड वाली सुविधाएं जैसे क्यूआर कोड या पिक्चर लॉगिन का इस्तेमाल करते हैं और जिनके छात्र-छात्रा, पासवर्ड से लॉगिन नहीं कर सकते उन्हें सुरक्षा के लिए ज़्यादा सावधानी बरतनी चाहिए, क्योंकि ये तरीके कम सुरक्षित होते हैं. जब भी कोई कोड खो जाता है या दूसरों के सामने ज़ाहिर हो जाता है, तो एडमिन को छात्र/छात्रा के पासवर्ड को बदल देना चाहिए और कोड को अपडेट कर देना चाहिए.
- स्कूलों को, छात्र-छात्राओं और उनके माता-पिता, दोनों को पासवर्ड को सुरक्षित रखने की अहमियत बतानी चाहिए. साथ ही, क्यूआर कोड जैसे ऑप्शनल क्रेडेंशियल को सुरक्षित रूप से सेव रखने के बारे भी बताना चाहिए.
- टैबलेट जैसे असाइन किए गए डिवाइस के लिए एक खास पिन का इस्तेमाल किया जा सकता है. यह पुष्टि करने का एक सुरक्षित, वैकल्पिक तरीका बन सकता है.

सुरक्षा से जुड़ी सही सेटिंग लागू करें

स्कूलों के डिवाइस और नेटवर्क, दुनिया भर के साइबर हमलावरों के लिए मुख्य टारगेट होते हैं, क्योंकि स्कूलों के बारे में आसानी से जानकारी मिल जाती है. ऐसे में, सेवाओं, संसाधनों, समय, और पैसों के नुकसान से बचने के लिए, सुरक्षा के सबसे सही तरीके लागू करना अहम है. सभी सिस्टम एडमिन को अपने संस्थानों में इस्तेमाल किए जाने वाले प्रॉडक्ट में, सुरक्षा से जुड़ी असरदार और बेहतर सुविधाओं को लागू करना चाहिए. हालांकि, उन्हें यह भी ध्यान रखना चाहिए कि ये सुविधाएं लागू करने के बाद भी, शिक्षक, कर्मचारी, और छात्र-छात्राएं आसानी से सिस्टम इस्तेमाल कर पाएं. सुरक्षा और निजता से जुड़ी अहम सेटिंग को ऐसे कॉन्फ़िगर किया जाना चाहिए कि दूसरे उपयोगकर्ता, न उन्हें बंद कर सकें और न उनमें बदलाव कर सकें. साथ ही, बाकी सेटिंग के लिए एडमिन को सुरक्षित डिफ़ॉल्ट सेटिंग लागू करनी चाहिए. सेवाओं, संसाधनों, समय, और पैसों के नुकसान से बचने के लिए, सुरक्षा से जुड़े सबसे सही तरीकों का इस्तेमाल करना अहम है. अगर आपके पास Chromebook है, तो आखिरी सेक्शन में, डिवाइस से जुड़ी नीतियां सेट करने के लिए हमारे सुझाव देखें.

अंत में, लोगों की निजी जानकारी को इकट्ठा करने, इस्तेमाल करने, और उसे ज़ाहिर करने की वजहों और तरीकों को कम करके, अपने संस्थान में "डेटा इकट्ठा करने पर प्रतिबंध लगाना" नीति लागू करें. इसके बजाय, लोगों की उतनी ही जानकारी को इकट्ठा, इस्तेमाल, और ज़ाहिर करें जितनी सेवा देने के लिए या उपयोगकर्ता को बेहतर सुविधाएं देने के लिए ज़रूरी हो.

ऐप्लिकेशन और अपडेट

अपने उपयोगकर्ताओं को सिर्फ़ चुनिंदा ऐप्लिकेशन को इंस्टॉल करने की अनुमति दें, क्योंकि डिवाइस पर जितने ज़्यादा ऐप्लिकेशन इंस्टॉल होंगे, साइबर हमलों का खतरा उतना ही ज़्यादा होगा. अगर संभव हो, तो भरोसेमंद सोर्स के ऐप्लिकेशन का ही इस्तेमाल करें. उदाहरण के लिए, उपयोगकर्ताओं को Google Play Store पर पुष्टि वाले निशान को देखने की सलाह दी जाती है. इससे यह पता चलता है कि उपयोगकर्ता, आधिकारिक ऐप्लिकेशन डाउनलोड कर रहे हैं, जिनकी सुरक्षा की समीक्षा पूरी हो चुकी है. ओएस या हार्डवेयर में अगर जेलब्रेकिंग या रूटिंग जैसा कोई भी बदलाव किया जाता है, तो सुरक्षा से जुड़ी गंभीर समस्याएं हो सकती हैं. इसलिए, ऐसा करने से बचना चाहिए.

ऐक्सेस और पारदर्शिता

एडमिन को यह पक्का करना चाहिए कि उपयोगकर्ताओं के पास सिर्फ़ ऐसे डेटा, सॉफ़्टवेयर, सेवाओं, और सिस्टम का ऐक्सेस हो जो उनके काम के लिए या बेहतर ढंग से सीखने के लिए ज़रूरी हैं. इससे ऐक्सेस को मैनेज करने और यह ट्रैक करने में मदद मिलती है कि किसिके पास किन संसाधनों का ऐक्सेस है. बेहद संवेदनशील जानकारी, जैसे उपयोगकर्ता की व्यक्तिगत पहचान से जुड़ी जानकारी और सिस्टम (जैसे एचआर, पेरोल, ग्रेडिंग, सुरक्षा, और कॉन्फ़िगरेशन) पर खास ध्यान दें. इसके लिए, देखें कि कौनसे उपयोगकर्ता, डेटा को कब ऐक्सेस कर सकते हैं. साथ ही, स्कूल के मालिकाना हक वाले डिवाइसों के ऐक्सेस को सीमित करें और यह पक्का करें सिर्फ़ कुछ कर्मचारियों के पास ही इनका ऐक्सेस हो.

सहयोगी टूल में, डेटा शेयर करने से जुड़ी अपनी नीतियों की समीक्षा करें, ताकि डेटा को गलत तरीके से या गलत लोगों के साथ शेयर करने से रोका जा सके. साथ ही, उसे बिना अनुमति के ऐक्सेस किए जाने से भी रोका जा सके. अपने संगठन से बाहर कॉन्टेंट शेयर करने पर पाबंदी लगाएं या इसे सीमित करें. खास तौर पर, छात्र-छात्राओं के लिए ऐसा करें. साथ ही, शेयर की जाने वाली संवेदनशील जानकारी की निगरानी करने वाली नीतियों को चालू करें.

डिवाइस खो जाना या चोरी हो जाना

डिवाइस खोने का मतलब यह नहीं है कि आपका डेटा भी खो जाएगा. किसी डिवाइस के खोने या चोरी होने के बाद भी, जानकारी और दस्तावेज़ों पर आपका ऐक्सेस बना रहे, यह पक्का करने के लिए एडमिन को एक स्टैंडर्ड प्लान बनाना चाहिए. जैसे- किसी क्लाउड प्लैटफ़ॉर्म में दस्तावेज़ों का बैकअप रखना. खाते को ऐक्सेस करने में कोई रुकावट न आए, इसके लिए दो चरणों में पुष्टि की अपनी सुविधा के बैकअप कोड डाउनलोड और प्रिंट करें.

जब किसी डिवाइस के खो जाने या चोरी हो जाने की सूचना मिलती है, तब अगर संभव हो सके, तो डिवाइस को रिमोट तरीके से लॉक कर दें. साथ ही, संबंधित खातों को लॉक कर दें या उन्हें फ़्लैग कर दें. इससे, खोए या चोरी हुए डिवाइस का इस्तेमाल करके, कोई खातों को ऐक्सेस नहीं कर सकेगा. अगर Chromebook खो जाता है, तो उस पर मौजूद डेटा को दूर से मिटाया जा सकता है. साथ ही, ज़रूरत पड़ने पर Google Workspace for Education खातों पर संदिग्ध गतिविधि के लिए निगरानी की जा सकती है या उन्हें निलंबित यानी लॉक किया जा सकता है.

बहुत ज़्यादा जोखिम वाले उपयोगकर्ताओं के लिए ऐडवांस सुरक्षा

बहुत ज़्यादा जोखिम वाले और संवेदनशील जानकारी का ऐक्सेस रखने वाले उपयोगकर्ताओं के लिए Google, Advanced Protection Program (APP) की सुविधा देता है. इन उपयोगकर्ताओं में, Google Workspace for Education के एडमिन शामिल हैं. APP से उपयोगकर्ताओं को फ़िशिंग, नुकसान पहुंचाने वाले डाउनलोड, और पासवर्ड का गलत इस्तेमाल करने जैसे हमलों से अतिरिक्त सुरक्षा मिलती है. APP को खास तौर पर, Google खातों को टारगेट बनाकर किए जाने वाले साइबर हमलों को रोकने के लिए डिज़ाइन किया गया है. इसमें, पहचान की पुष्टि करने का सुरक्षित तरीका अपने-आप इस्तेमाल किया जाता है, सुरक्षा कुंजी का इस्तेमाल किया जाता है, और खाते के डेटा पर तीसरे पक्ष के ऐक्सेस को सीमित किया जाता है. ऑनलाइन खाते वाली अन्य सेवाएं भी ज़्यादा जोखिम वाले उपयोगकर्ताओं के खातों को मज़बूत सुरक्षा उपलब्ध कराती हैं. अगर एडमिन और कर्मचारियों के पास, उपयोगकर्ताओं की निजी जानकारी या टेक्नोलॉजी सिस्टम का ऐक्सेस है, तो उन्हें हमेशा इन सुरक्षा उपायों का इस्तेमाल करना चाहिए..

अपने सिस्टम को अपडेट और अपग्रेड करें

अपने डिवाइस की सुरक्षा के लिए सबसे ज़रूरी चीज़ों में से एक है, अपने डिवाइस के ऑपरेटिंग सिस्टम और ऐप्लिकेशन को अपडेट रखना. कंडिरगार्टन से बारहवीं कक्षा तक के संस्थानों के लिए यह और भी अहम है, क्योंकि वे बच्चे की शिक्षा और रोज़मर्रा के जीवन का एक अहम हिस्सा हैं. शिक्षा के क्षेत्र से जुड़े मामलों और ज़्यादा जोखिम वाले अन्य क्षेत्र के मामलों, दोनों में ज़्यादातर मैलवेयर हमले Windows वाले डिवाइस पर हुए हैं. इनमें SolarWinds पर हुआ हमला, लॉस एंजेलिस यूनिफ़ाइड स्कूल डिस्ट्रिक्ट पर हुआ रैंसमवेयर हमला, लिटिल रॉक स्कूल डिस्ट्रिक्ट पर हुई हैकिंग, Microsoft Exchange Server के डेटा का गलत इस्तेमाल, अलबुकर्की स्कूल डिस्ट्रिक्ट पर हुआ रैंसमवेयर हमला, और अमेरिकी एजेंसियों के डेटा के गलत इस्तेमाल की हाल ही में हुई घटना शामिल है. ऐसे मामलों में, क्लाउड-आधारित प्रॉडक्ट और सेवाओं का इस्तेमाल करके, एडमिन के काम को आसान बनाया जा सकता है. ये प्रॉडक्ट और सेवाएं, हमले की जगह को कम करती हैं और यह पक्का करती हैं कि एडमिन के सिस्टम और ऐप्लिकेशन अपने-आप अपडेट होते रहें.

किसी मॉडर्न ऑपरेटिंग सिस्टम पर अपग्रेड करें और इसे अप-टू-डेट रखें

किसी भी ऑपरेटिंग सिस्टम (ओएस) के नए वर्शन में आम तौर पर, सुरक्षा से जुड़ी नई सुविधाएं शामिल होती हैं. इनसे, पहले से मालूम अटैक वेक्टर से बचाव में मदद मिलती है. आपको डिवाइस ओएस में, अपने-आप अपडेट होने की सुविधा चालू करनी चाहिए. इसके अलावा, अगर अपने-आप अपडेट होने की सुविधा उपलब्ध नहीं है, तो कम से कम हर महीने किसी भरोसेमंद वेंडर से, पैच और अपडेट डाउनलोड और इंस्टॉल करने चाहिए.

Chromebook, ChromeOS पर चलते हैं, इसलिए वे समय-समय पर नए सुरक्षा पैच के साथ-साथ अपने-आप अपडेट होते रहते हैं. इनसे, सुरक्षा से जुड़ी नई सुविधाएं डिवाइस में तेज़ी से लागू हो जाती हैं. साथ ही, Chromebook बूट करने से पहले रीड-ओनली ऑपरेटिंग सिस्टम के रखरखाव की पुष्टि करते हैं. Chromebook, डिवाइस पर सेव सभी डेटा को एन्क्रिप्ट करते हैं और इसे बिना अनुमति के ऐक्सेस करने से रोकते हैं. साथ ही, हर वेब पेज और ऐप्लिकेशन को एक अलग सैंडबॉक्स में रन करते हैं, ताकि अगर किसी एक वेबसाइट या ऐप्लिकेशन पर मैलवेयर का हमला हो भी जाए, तो यह डिवाइस के अन्य हिस्सों में न फैले.

अगर आपका स्कूल अभी Chromebook का इस्तेमाल नहीं कर रहा है, तो आपके पास स्कूल के डिवाइस पर ChromeOS Flex इस्तेमाल करने का विकल्प है. यह ChromeOS का एक वर्शन है जो आपके स्कूल के डिवाइसों को मॉडर्न बनाने के लिए डिज़ाइन किया गया है. ChromeOS Flex, सभी डिवाइसों पर काम करता है और इससे हर डिवाइस पर सीखने-सिखाने का मॉडर्न और एक जैसा अनुभव मिलता है. यह एक तेज़, सुरक्षित, और आसानी से मैनेज किया जा सकने वाला क्लाउड-आधारित ऑपरेटिंग सिस्टम है. इसमें, सुरक्षा से जुड़ी कई सुविधाएं पहले से मौजूद हैं. इसके तहत, डिवाइस के मौजूदा हार्डवेयर को बदले बिना, सुरक्षा से जुड़ी सुविधाएं अपने-आप मिलने लगती हैं. साथ ही, ये नुकसान पहुंचाने वाले एक्ज़ीक्यूटेबल फ़ाइल और ऐप्लिकेशन को ब्लॉक कर सकता है.

एक मॉडर्न ब्राउज़र पर अपग्रेड करें और इसे अप-टू-डेट रखे

ब्राउज़र को भी अपडेट और सुरक्षित रखना अहम है. मॉडर्न ब्राउज़र, सुरक्षा से जुड़ी ऐडवांस सुविधाएं देते हैं और इन्हें आसानी से चालू करने के लिए, उपयोगकर्ताओं को निर्देश भी उपलब्ध कराते हैं. साथ ही, इन सुविधाओं को संस्थान के डिवाइसों पर, डिफ़ॉल्ट रूप से चालू करने के लिए, एडमिन कॉन्फ़िगरेशन कर सकते हैं. इनसे डिजिटल प्लैटफ़ॉर्म पर मौजूद संवेदनशील जानकारी को सुरक्षित रखने में मदद मिलती है. ब्राउज़र को अप-टू-डेट रखा जाना चाहिए. चाहे काम करना हो, सीखना हो या कोई अन्य ऑनलाइन गतिविधि करनी हो, एक अप-टू-डेट मॉडर्न ब्राउज़र ये काम करेगा:

- **मज़बूत सुरक्षा देगा:** उपयोगकर्ताओं को गलती से खतरनाक वेबसाइटों पर जाने से रोकने के लिए, ब्राउज़र आपको साइट आइसोलेशन और सुरक्षित ब्राउज़िंग जैसी कई सुविधाएं देगा.
- **अपने-आप अपडेट करने की सुविधा देगा:** आपके ब्राउज़र को सुरक्षा से जुड़े अपडेट समय पर मिलते रहें, इसके लिए अपने-आप अपडेट करने की सुविधा देगा.
- **पक्का करेगा कि कनेक्शन सुरक्षित है:** मॉडर्न ब्राउज़र को ट्रांसपोर्ट लेयर सिक्योरिटी का इस्तेमाल करना चाहिए. इसके तहत, उपयोगकर्ता किसी भी वेबसाइट के यूआरएल के आगे क्लिक करके, यह जांच सकते हैं कि कनेक्शन सुरक्षित है या नहीं

Chrome को सुरक्षा को ध्यान में रखकर बनाया गया है. इसमें सुरक्षित ब्राउज़िंग जैसी सुरक्षा सुविधाएं डिफ़ॉल्ट रूप से चालू रहती हैं. साथ ही, इसमें एक पासवर्ड मैनेजर इंटिग्रेट किया जाता है जो आपकी वेब ब्राउज़िंग के दौरान, पासवर्ड को ऑटोमैटिक तरीके से भर सकता है. इससे आसानी से मज़बूत पासवर्ड का इस्तेमाल किया जा सकता है.

रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सिस्टम का इस्तेमाल करें

रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सिस्टम, नुकसान पहुंचाने वाले खतरों की पहचान करने और उनके ख़िलाफ़ तुरंत कार्रवाई करने में, स्कूलों की मदद कर सकते हैं. आपको समय-समय पर यह देखते रहना चाहिए कि सुरक्षा से जुड़े टूल बैकग्राउंड में चल रहे हैं. साथ ही, आपके सभी सिस्टम में होने वाली सुरक्षा से जुड़ी गतिविधियों को इकट्ठा और लॉग कर रहे हैं. AI टूल, बड़ी मात्रा में इकट्ठा किए गए डेटा को फ़िल्टर करने और अनियमितताओं और पैटर्न को खोजने का काम बहुत अच्छे से करते हैं. इनका इस्तेमाल, खतरों का ज़्यादा तेज़ी और आसानी से पता लगाने, जोखिम की आशंका को समझने, और उनका हल निकालने के लिए किया जा सकता है. इससे आईटी एडमिन या कर्मचारियों को यह समझने में मदद मिलती है कि किन गतिविधियों की समीक्षा पहले करनी है.

स्कूल साथ मिलकर काम करने और कम्यूनिकेशन से जुड़े अपने सॉफ़्टवेयर (जैसे, Google Workspace for Education) में पहले से मौजूद, रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सिस्टम का इस्तेमाल कर सकते हैं. इसके अलावा, एसआईईएम से जुड़े अलग समाधान डिप्लॉय कर सकते हैं.

रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सिस्टम, स्कूल के नेटवर्क, डिवाइस, ऐप्लिकेशन, उपयोगकर्ताओं, और डेटा से जुड़ी अलग-अलग तरह की गतिविधियों को ट्रैक कर सकते हैं. जैसे- उपयोगकर्ताओं के लॉगिन, फ़ाइलों के ऐक्सेस, संभावित मैलवेयर, डेटा की चोरी या चोरी की कोशिश की जानकारी, और एडमिन की गतिविधियां.

अगर सिस्टम को किसी संदिग्ध गतिविधि का पता लगता है, तो यह स्कूल के आईटी स्टाफ़ को इसकी सूचना भेजता है. इससे एडमिन को समस्या की जांच करने और खतरे को कम करने के लिए कार्रवाई करने में मदद मिलती है.

इसके अलावा, स्कूलों पर आने वाले खतरों को बेहतर तरीके से समझने के लिए, रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले टूल का इस्तेमाल किया जा सकता है. इन रीयल टाइम सिस्टम से मिले डेटा का विश्लेषण करके, स्कूल उन रुझानों और पैटर्न की पहचान कर सकते हैं जो उन्हें खुद को बेहतर ढंग से सुरक्षित रखने में मदद कर सकते हैं.

रीयल टाइम में सूचना देने वाले और मॉनटिर करने वाले सिस्टम (इनमें एसआईईएम शामिल है) इस्तेमाल करने के लिए, सबसे सही तरीके यहां दिए गए हैं:

1. **सुरक्षा से जुड़े अपने लक्ष्य तय करें**
   पहचान करें कि कौनसी जानकारी और सिस्टम, स्कूल के लिए सबसे अहम हैं. साथ ही, इन पर किस तरह के खतरों का जोखिम है. फिर उन खतरों को मॉनटिर करने के लिए ज़रूरी डेटा को पहचानने का काम शुरू करें.

2. **सही डेटा इकट्ठा करें और उसे ठीक से कॉन्फ़िगर करें**
   सुरक्षा से जुड़े अपने सबसे अहम लक्ष्यों को पूरा करने के लिए, सही डेटा इकट्ठा करना और ऐप्लिकेशन कॉन्फ़िगर करना अहम है. इसमें फ़ायरवॉल, कॉन्टेंट से जुड़े फ़िल्टर, मैलवेयर गतिविधि की पहचान करने वाले सिस्टम, वेब सर्वर, और सुरक्षा से जुड़े अन्य डिवाइसों का डेटा शामिल होता है. साथ ही इसमें, साथ मिलकर काम करने और कम्यूनिकेशन से जुड़े सॉफ़्टवेयर, छात्र-छात्राओं की जानकारी का रिकॉर्ड रखने वाले सिस्टम (SIS), और लर्निंग मैनेजमेंट सिस्टम का डेटा भी शामिल होता है.

3. **सूचनाओं की जांच करके, उन पर कार्रवाई करें**
   मॉनटिर करने वाले सिस्टम से सूचना मिलने पर, उसकी जांच करनी चाहिए और उचित कार्रवाई करनी चाहिए. इसमें, सूचना के सोर्स की जांच करने के लिए कई टीमों को एक साथ लाना और यह पता करना कि कहीं यह फ़ॉल्स पॉज़िटिव तो नहीं है, शामिल हो सकता है. इसके अलावा, इसमें खतरे को कम करने के लिए ज़रूरी कदम उठाना शामिल हो सकता है. जैसे- खातों को स्थगित करना, उपयोगकर्ता के पासवर्ड को रीसेट करना, ईमेल को क्वॉरंटीन करना या मिटाना, फ़ाइलों की अनुमतियां बदलना या डिवाइस का डेटा मिटा देना.

शिक्षक, कर्मचारियों, और छात्र-छात्राओं को ट्रेनिंग दें

किंडरगार्टन से बारहवीं कक्षा तक के संस्थानों को, स्कूल कम्यूनिटी को सुरक्षा के बारे में जागरूक करना चाहिए. साथ ही, उन्हें सुरक्षा से जुड़े सबसे सही तरीकों को इस्तेमाल करने के लिए प्रोत्साहित करना चाहिए. इसके लिए, संस्थान अलग-अलग कैंपेन चला सकते हैं और अलग-अलग संगठनों के साथ पार्टनरशिप कर सकते हैं. शिक्षकों, कर्मचारियों, और छात्र-छात्राओं को सुरक्षा की अहमियत के बारे में जानकारी देना बहुत ज़रूरी है. इससे वे खुद को गंभीर साइबर हमलों से सुरक्षित रख सकेंगे और ऐसे खतरों को रोकने में भी मदद कर सकेंगे. उन्हें सिखाएं कि संस्थान के प्रॉडक्ट और सेवाओं का इस्तेमाल कैसे करें और फ़िशिंग ईमेल जैसे खतरों को कैसे पहचानें और कैसे उनकी रिपोर्ट करें. साथ ही, उन्हें यह ज़रूर बताएं कि इन हमलों को रोकने के लिए कार्रवाई कैसे करें. स्कूल और डिस्ट्रिक्ट को, स्कूल कम्यूनिटी को सुरक्षा के बारे में जागरूक करना चाहिए. साथ ही, उन्हें सुरक्षा से जुड़े सबसे सही तरीकों को इस्तेमाल करने के लिए प्रोत्साहित करना चाहिए. इसके लिए, स्कूल अलग-अलग कैंपेन चला सकते हैं और अलग-अलग संगठनों के साथ पार्टनरशिप कर सकते हैं.

डिवाइस और सॉफ़्टवेयर का सुरक्षित तरीके से इस्तेमाल कैसे करें

एडमिन, शिक्षकों और विशेषज्ञों के साथ मिलकर, अलग-अलग उम्र के छात्र-छात्राओं के हिसाब से, साइबर सुरक्षा से जुड़ा पाठ्यक्रम बनाने में मदद कर सकते हैं. इससे छात्र-छात्राओं को डिवाइस, सॉफ़्टवेयर, और सिस्टम का सुरक्षित तरह से इस्तेमाल करने के बारे में जानकारी मिलती है. किसी स्कूल या डिस्ट्रिक्ट के लिए खास ट्रेनिंग मटीरियल बनाने से, आपके शिक्षकों और छात्र-छात्राओं के हिसाब से सुझाव दिए जा सकते हैं. हालांकि, वे पहले से उपलब्ध ट्रेनिंग मटीरियल का भी फ़ायदा पा सकते हैं और इन्हें अपनी ज़रूरत के हिसाब से इस्तेमाल कर सकते हैं. जैसे- Safety. Google पेज पर उपलब्ध Be Internet Awesome और Khan Academy पर उपलब्ध संसाधन. ये संसाधन आपके उपयोगकर्ताओं को सुरक्षित रहने में मदद कर सकते हैं, चाहे वे कहीं भी डिवाइस का इस्तेमाल कर रहे हों - स्कूल में या अपनी कम्यूनिटी में.

खतरों की पहचान करना

शिक्षकों, कर्मचारियों, और छात्र-छात्राओं के लिए, खतरों की पहचान करना बहुत अहम है. उन्हें इस बारे में ट्रेनिंग देकर, उन्हें सुरक्षित रखने में मदद मिलती है. बच्चों को यह सिखाना अहम है कि कोई चीज़ खतरा है या नहीं, क्योंकि हो सकता है कि उन्हें यह न पता हो कि किसी चीज़ के सही होने की पुष्टि कैसे की जाती है. उन्हें कुछ खास तरह के खतरों की पहचान होनी चाहिए और पता होना चाहिए कि उनकी रिपोर्ट कैसे करनी है. साथ ही, बच्चों को सिखाते समय, एडमिन को उन विषयों पर सबसे ज़्यादा ध्यान देना चाहिए जिन पर समय देने से सबका फ़ायदा होगा. अहम बात यह है कि ट्रेनिंग में उपयोगकर्ताओं को सिर्फ़ खतरों को पहचानना नहीं सिखाया जाना चाहिए, बल्कि कार्रवाई करने के तरीकों की भी ट्रेनिंग दी जानी चाहिए. जिन सामान्य खतरों की उपयोगकर्ताओं को पहचान होनी चाहिए उनमें रैंसमवेयर, फ़िशिंग, सोशल इंजीनियरिंग, मैलवेयर, और स्कैम शामिल हैं. हालांकि, अगर कोई संस्थान कुछ खास तरह के खतरों का ज़्यादा सामना करता है, तो स्कूल कम्यूनिटी को इन खतरों के बारे में ज़रूर पता होना चाहिए.

डेटा और फ़ाइलों को सुरक्षित तरीके से शेयर करना

शिक्षकों और कर्मचारियों को, फ़ाइलों और डेटा को सुरक्षित तरीके से शेयर करने का तरीका पता होना चाहिए. साथ ही, ईमेल से आने वाले आपत्तिजनक अनुरोधों को पहचानने के बारे में भी जानकारी होनी चाहिए. उन्हें इस बात का हर हाल में ध्यान रखना होगा कि संवेदनशील निजी जानकारी, सिर्फ़ ज़रूरी होने पर ही शेयर या प्रोसेस की जा रही है. साथ ही, इसे शेयर करते समय, अतिरिक्त सुरक्षा उपायों का पालन किया जा रहा है. जैसे- इस जानकारी को ईमेल के ज़रिए या संगठन से बाहर कभी शेयर नहीं किया जाएगा. उन्हें डेटा लीक होने की रोकथाम से जुड़ी सुविधाओं (ये सुविधाएं ChromeOS और Workspace for Education में मिलती हैं) का इस्तेमाल, असली उपयोगकर्ताओं को सोशल सिक्योरिटी नंबर जैसी संवेदनशील जानकारी वाली फ़ाइलें शेयर करने से रोकने और इसकी चेतावनी देने के लिए करना चाहिए. साथ ही, डोमेन के बाहर संवेदनशील जानकारी को कॉपी करने और चिपकाने से रोकने और इसकी चेतावनी देने के लिए भी इनका इस्तेमाल करना चाहिए.

कार्रवाई को लेकर Google का नज़रिया: सीखने-सिखाने से जुड़े डिवाइस और सेवाएं

स्कूल डिस्ट्रिक्ट के लिए, सॉफ़्टवेयर सबसे दमदार टूल में से एक होते हैं. अपनी सुरक्षा के लिए सही सॉफ़्टवेयर प्रोक्योर करना ज़रूरी होता है. सॉफ़्टवेयर को जोखिम को कम करने के लिहाज़ से डिज़ाइन किया जाना चाहिए और इसमें हर स्तर पर सुरक्षा के लिए सुविधाएं मौजूद होनी चाहिए. ऑनलाइन सुरक्षा के क्षेत्र में अच्छा ट्रैक रिकॉर्ड रखने वाली कंपनियों के सॉफ़्टवेयर या सुरक्षित सॉफ़्टवेयर खरीदना, स्कूलों के लिए ज़रूरी बनाएं. इससे साइबर हमलों के खतरे को काफ़ी हद तक कम किया जा सकेगा. उदाहरण के लिए, हमने अपने ChromeOS की सुरक्षा सुविधाओं को और बेहतर कर दिया है. साथ ही, हम बेहतर तरीके से काम करने वाले स्मार्ट समाधानों को पहले की तरह डिप्लॉय कर रहे हैं, जो हमारी मशीन लर्निंग, क्लाउड, और पहचान करने से जुड़ी विशेषज्ञता का पूरा इस्तेमाल करते हैं.

Google ऐसे प्रॉडक्ट बनाता है जिनके इस्तेमाल से छात्र-छात्राओं और शिक्षकों की निजता को कोई खतरा नहीं होता है. साथ ही, आपके संस्थान को सुरक्षा की बेहतर सुविधाएं मिलती हैं. आप बेफ़िक्र होकर Google for Education के प्रॉडक्ट और सेवाओं का इस्तेमाल कर सकते हैं. इन्हें इस तरह से डिज़ाइन किया गया है कि ये उपयोगकर्ताओं, डिवाइसों, और डेटा को हर तरह के खतरे से सुरक्षित रखते हैं. इस सेक्शन में इस बारे में जानकारी दी गई है कि सभी स्कूल के आईटी एडमिन को Google for Education प्रॉडक्ट का इस्तेमाल करते समय, सुरक्षा से जुड़े किन सुझावों का ध्यान रखना चाहिए.

Google Workspace for Education

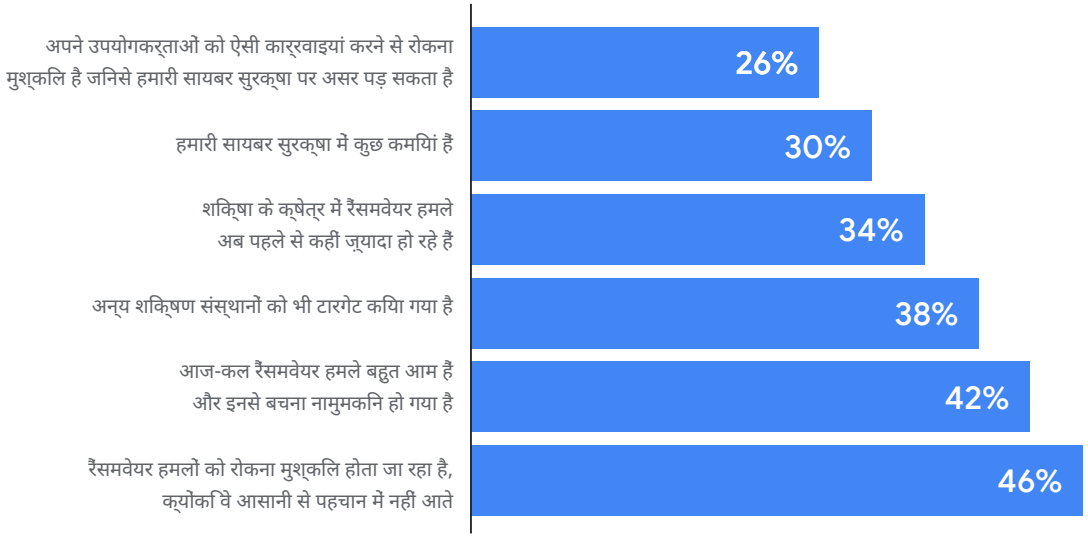
Google Workspace for Education, Google के कुछ टूल और सेवाओं का एक सेट है. यह स्कूल में, साथ मिलकर सीखने-सिखाने और व्यवस्थित तरीके से निर्देश देने की सुविधा देता है. साथ ही, सीखने-सिखाने के लिए एक सुरक्षित माहौल भी उपलब्ध कराता है. Google for Education के प्रॉडक्ट और सेवाएं, उपयोगकर्ताओं, डिवाइसों, और डेटा को गंभीर खतरों से हमेशा बचाती हैं. साथ ही, सूचना और सुरक्षा केंद्र, ई-खोज के लिए Vault, पहचान और ऐक्सेस मैनेजमेंट, और डेटा लीक होने की रोकथाम जैसे टूल उपलब्ध कराती हैं.

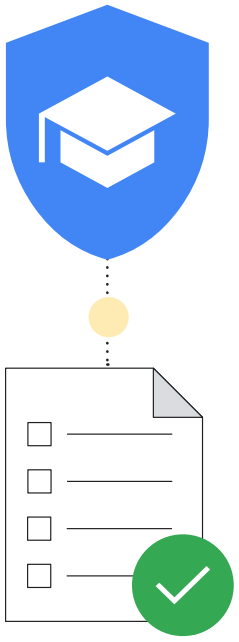
अगर आपने हाल ही में Google Workspace for Education का इस्तेमाल शुरू किया है, तो हम आपको बताना चाहते हैं कि हमने आपकी मदद के लिए, काफ़ी सामग्री तैयार की है. इनमें से कई दस्तावेज़, इस गाइड में दिए गए सुझावों के हिसाब से प्रॉडक्ट को सेट अप करने में, आपकी मदद कर सकते हैं. Google Workspace for Education का इस्तेमाल शुरू करने में मदद पाने के लिए, यह क्विकस्टार्ट आईटी सेटअप गाइड देखें.

सुरक्षा और निजता से जुड़ी चेकलिस्ट

अपने संस्थान की सुरक्षा और निजता को मज़बूत करने के तरीके के बारे में ज़्यादा जानने के लिए, सुरक्षा और निजता से जुड़ी चेकलिस्ट ध्यान से देखें. Google Workspace for Education के Standard और Plus वर्शन का इस्तेमाल करने वाले स्कूल, अपने Admin console की सेटिंग के कॉन्फ़िगरेशन को मॉनिटर करने के लिए सिक्योरिटी हेल्थ पेज का भी इस्तेमाल कर सकते हैं. उदाहरण के लिए, स्कूल अपने-आप ईमेल फ़ॉरवर्ड होने की सुविधा, डिवाइस एनक्रिप्शन, Drive की शेयर करने की सेटिंग वगैरह की स्थिति की जांच कर सकते हैं. अगर ज़रूरत हो, तो सुरक्षा से जुड़े दिशा-निर्देशों और सबसे सही तरीकों के आधार पर, अपने डोमेन की सेटिंग में बदलाव किया जा सकता है. हालांकि, ऐसा करने के दौरान, आपके अपने संगठन की व्यावसायिक ज़रूरतों और जोखिम को मैनेज करने की नीति को ध्यान में रखना चाहिए.

शिक्षा के क्षेत्र में साइबर हमले होने की संभावना क्यों बनी रहती है





सोर्स: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Google Workspace for Education में पहले से मौजूद, सुरक्षा से जुड़ी सुविधाओं का ज़्यादा से ज़्यादा इस्तेमाल किया जा रहा है, यह पक्का करने के लिए यहां कुछ सलाह दी गई हैं:

संगठन की इकाई (ओयू) सेट अप करें

आपके Google Workspace for Education खाते के सभी उपयोगकर्ताओं के लिए, एक जैसी सेटिंग लागू करना ज़रूरी नहीं है. अलग-अलग उपयोगकर्ताओं के ग्रुप को संगठन की इकाइयां कहा जाता है. इनके तहत अलग-अलग उपयोगकर्ताओं को अलग-अलग सेवाएं, सेटिंग, और अनुमतियां दी जाती हैं. उदाहरण के लिए, शिक्षकों और कर्मचारियों के लिए, दो चरणों में पुष्टि की सुविधा का इस्तेमाल करना और कम उम्र के छात्र-छात्राओं के लिए, उम्र के हिसाब से पुष्टि की सुविधा का इस्तेमाल करना. उपयोगकर्ताओं के हर ग्रुप पर अलग-अलग नीतियां लागू करना है, तो कर्मचारियों, शिक्षकों, और छात्र-छात्राओं के लिए, संगठन की अलग-अलग इकाइयां सेट अप करें. आपके Google Workspace for Education खाते को असरदार और बेहतर तरीके से मैनेज करने के लिए, अच्छी तरह से बनाई गई संगठनात्मक संरचना अहम है.

पासवर्ड की नीतियां और एडमिन के खाते के लिए सुरक्षा नीतियां सेट अप करें

जैसा कि हमने ऊपर चर्चा की है, उपयोगकर्ता की पहचान की पुष्टि करना, अपने संस्थान को सुरक्षित रखने का एक अहम हिस्सा है. इसलिए, हमने एडमिन के लिए, उपयोगकर्ताओं की पहचान की पुष्टि को मैनेज करने के आसान तरीके तय किए हैं. इनसे यह पक्का किया जा सकेगा कि उपयोगकर्ताओं ने अपने खाते की सुरक्षा के लिए सही तरीके अपनाए हैं. पासवर्ड की नीतियां सेट करें, ताकि उपयोगकर्ता मज़बूत पासवर्ड बनाएं और एसएसओ (SSO) सेक्शन में दिए गए सुझावों के आधार पर जहां ज़रूरत हो वहां 2SV का इस्तेमाल करें. उपयोगकर्ताओं के एक ग्रुप के लिए, दो चरणों में पुष्टि की सुविधा को इस्तेमाल करने का नियम लागू किया जा सकता है. इससे उन्हें इसका सेट अप करने का समय मिल जाता है. साथ ही, अलग-अलग तरीकों का इस्तेमाल करके 2SV को डिप्लॉय किया जा सकता है. इन तरीकों में, सुरक्षा कुंजी (सबसे सुरक्षित तरीका), एक Google प्रॉम्प्ट (Google के Android और iOS वाले ऐप्लिकेशन का इस्तेमाल करके भेजा गया प्रॉम्प्ट), वेरिफ़िकेशन कोड जनरेट करने वाला ऐप्लिकेशन (जैसे- Google Authenticator), टेक्स्ट मैसेज या फ़ोन कॉल से पुष्टि करना (हालांकि, यह सबसे कम सुरक्षित तरीका है) वगैरह शामिल हैं.

अगर आपका संगठन, Google के अलावा किसी अन्य आइडेंटिटी प्रोवाइडर (आईडीपी) का इस्तेमाल करता है, तो आपके पास किसी तीसरे पक्ष के आइडेंटिटी प्रोवाइडर के ज़रिए सिंगल साइन-ऑन (एसएसओ) को सेट अप करने का विकल्प है. अगर आप चाहें, तो नॉन-सुपर एडमिन खातों के लिए, अब भी एसएसओ (SSO) के साथ 2SV का इस्तेमाल किया जा सकता है.

सेवाओं को चालू या बंद करें

सेवाओं को चालू या बंद करेंएडमिन यह कंट्रोल कर सकते हैं कि उपयोगकर्ता, अपने Google Workspace for Education खाते में किन Google सेवाओं को ऐक्सेस कर सकते हैं. Google Admin console में जाकर, एडमिन इन सेवाओं को चुन सकते हैं. संगठन की इकाई (ओयू) के हिसाब से सेवाओं को चालू या बंद करके, Calendar, Drive, और Meet जैसी Google सेवाओं के ऐक्सेस को कंट्रोल किया जा सकता है. ग्रुप सेक्शन का इस्तेमाल करने पर, सेवाओं को चालू भी किया जा सकता है. YouTube, Google Maps, और Blogger जैसी अन्य सेवाओं को चालू करने से पहले, Workspace के उपयोगकर्ताओं को मिलने वाली मूल सेवाओं और अन्य सेवाओं के बीच के अंतर की समीक्षा भी की जा सकती है. एडमिन को उम्र के आधार पर, Google सेवाओं का ऐक्सेस देना चाहिए. साथ ही, यह ध्यान रखना चाहिए कि Google Workspace for Education खाते का इस्तेमाल करने वाले 18 साल से कम उम्र के उपयोगकर्ता, अपने-आप ही कुछ Google सेवाओं से प्रतिबंधित होते हैं.

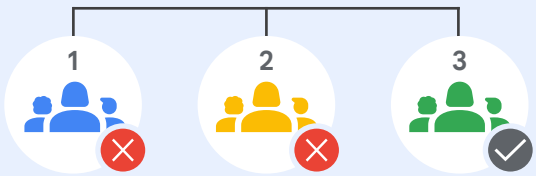
Gmail, Drive, और Calendar जैसे Google ऐप्लिकेशन के ऐक्सेस की अनुमति देने या ब्लॉक करने के लिए, कॉन्टेक्स्ट अवेयर ऐक्सेस (Workspace for Education Standard और Plus वर्शन में उपलब्ध) का भी इस्तेमाल किया जा सकता है. ऐसा डिवाइस के आईपी पते, क्षेत्र या देश के नाम, सुरक्षा नीतियों या ओएस के आधार पर किया जा सकता है. उदाहरण के लिए, कुछ देशों या क्षेत्रों में, कंपनी के मालिकाना हक वाले डिवाइसों पर ही Drive for desktop की सुविधा दी जा सकती है.

उपयोगकर्ताओं को सेवाओं का ऐक्सेस देने के तरीके

Google Admin console में जाकर संगठन की किसी इकाई के लिए, Google की कोई सेवा ऐक्सेस करने की सुविधा बंद की जा सकती है. जैसे, Google Drive इस्तेमाल करने की सुविधा. अगर उस इकाई में शामिल कुछ उपयोगकर्ताओं को Drive का इस्तेमाल करना है, तो उन्हें ऐक्सेस देने के लिए इनमें से कोई तरीका अपनाएं:

1. उन्हें संगठन की किसी ऐसी इकाई में शामिल करें जिसके लिए, Drive को ऐक्सेस करने की सुविधा चालू है.
2. उन्हें किसी ऐक्सेस ग्रुप में शामिल करके उस ग्रुप के लिए, Drive को ऐक्सेस करने की सुविधा चालू करें. इससे ग्रुप के सभी सदस्य यह सेवा इस्तेमाल कर सकेंगे. भले ही संगठन की जिस इकाई में वे शामिल हैं उसके लिए यह सुविधा बंद हो.

संगठन की इकाइयां



Google Drive को ऐक्सेस करने की सुविधा, संगठन की इकाई 1 और 2 के लिए बंद है.

ऐक्सेस ग्रुप में शामिल उपयोगकर्ता

संगठन की इकाई 1 और 2 में शामिल ऐसे उपयोगकर्ताओं का ग्रुप जो Google Drive का इस्तेमाल कर सकते हैं

सोर्स: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

डेटा शेयर करने से जुड़ी नीतियां और निजी डेटा के रखरखाव के नियम सेट करें

एडमिन यह कंट्रोल कर सकते हैं कि उपयोगकर्ता, अपने संगठन से बाहर के लोगों के साथ Google Drive की फ़ाइलों और फ़ोल्डर को शेयर कर सकते हैं या नहीं. इससे फ़ाइलें और डेटा, ज़रूरत से ज़्यादा लोगों के साथ शेयर नहीं किया जाता है. साथ ही, डेटा लीक को रोकने में भी मदद मिलती है. फ़ाइलों और ड्राइव को अलग करना, संगठन की इकाइयां बनाना, और कम से कम अधिकारों के सिद्धांत के तहत काम करना, साइबर हमलों को रोकने के लिए अहम है. ऐसा करने से, अगर हमलावर एक खाते को ऐक्सेस कर भी लेता है, तो उसे बाकी खातों और नेटवर्क का ऐक्सेस नहीं मिलता. संभावित हमलावर के पास जितने कम डेटा और नेटवर्क का ऐक्सेस होगा उतना ही कम नुकसान होगा.

छात्र-छात्राओं के लिए, संगठन से बाहर फ़ाइल शेयर करने की सुविधा बंद करें (या सिर्फ़ अनुमति वाली सूची में शामिल डोमेन के साथ फ़ाइलें शेयर करने की सेटिंग चालू करें) और "ऐक्सेस चेकर" को "सिर्फ़ पाने वाले लोग" पर सेट कर दें. अगर कुछ या सभी उपयोगकर्ताओं को अपने डोमेन के बाहर फ़ाइलें शेयर करने की अनुमति दी जाती है, तो चेतावनी देने की सुविधा चालू करें. इससे, जब भी कोई उपयोगकर्ता ऐसा करेगा, तब उसे चेतावनी दिखाई देगी. इसके अलावा, वेब पर फ़ाइल पब्लिश करने की सुविधा को बंद करें. साथ ही, संगठन से बाहर के सहयोगियों के लिए, Google खाते से साइन इन करने की शर्त रखें.

इसके अलावा, Workspace for Education Standard और Plus के ग्राहक, टारगेट ऑडियंस और ट्रस्ट रूल का इस्तेमाल करके, हर लेवल पर, शेयर करने से जुड़े सुझाव और प्रतिबंधों को लागू कर सकते हैं. उदाहरण के लिए, टारगेट ऑडियंस की मदद से, शिक्षक अपनी डिफ़ॉल्ट ऑडियंस के तौर पर "शिक्षकों और कर्मचारियों" को चुन सकते हैं. इससे, उनके शेयर किए गए लिंक को सिर्फ़ शिक्षक और कर्मचारी ऐक्सेस कर सकेंगे, न कि पूरा संस्थान. ट्रस्ट रूल की मदद से, छोटी क्लास के छात्र-छात्रा, बड़ी क्लास के छात्र-छात्राओं के साथ फ़ाइलें नहीं शेयर कर सकेंगे.

यह पक्का करने के लिए 'शेयर की गई ड्राइव' से जुड़ी नीतियों की समीक्षा करें कि सिर्फ़ अनुमति वाले उपयोगकर्ता ही 'शेयर की गई ड्राइव' बना सकते हैं और इन ड्राइव को संगठन से बाहर के उपयोगकर्ता ऐक्सेस नहीं कर सकते. हमारा सुझाव है कि आप एडमिन, कर्मचारियों, या शिक्षकों को ही 'शेयर की गई ड्राइव' बनाने की अनुमति दें और आप ड्राइव के ऐक्सेस को बारीकी से मैनेज करें.

जहां संभव हो, डायरेक्ट्री दिखने और संपर्क शेयर करने की सेटिंग को सीमित करें. इसके लिए, कुछ या सभी उपयोगकर्ताओं के साथ संपर्क शेयर करने की सुविधा को बंद कर दें या कस्टम डायरेक्ट्री बनाएं. इनसे यह सीमित किया जा सकेगा कि किसी उपयोगकर्ता की

संपर्क जानकारी, किसको दिखेगी.संवेदनशील जानकारी का पता लगाने और उसके ऐक्सेस को ब्लॉक करने के लिए, Drive और Gmail में, डेटा लीक होने की रोकथाम (डीएलपी) से जुड़ी नीतियां सेट अप करें. इनके साथ ही, पहले से मौजूद नीतियां भी उपलब्ध हैं, जिनकी मदद से बैंक की जानकारी या क्रेडिट कार्ड नंबर जैसी संवेदनशील जानकारी की सुरक्षा की जा सकती है. कीवर्ड, शब्दों की सूचियों, और रेगुलर एक्सप्रेशन के आधार पर, कस्टम नीतियां भी बनाई जा सकती हैं.

Gmail सेटिंग मैनेज करें

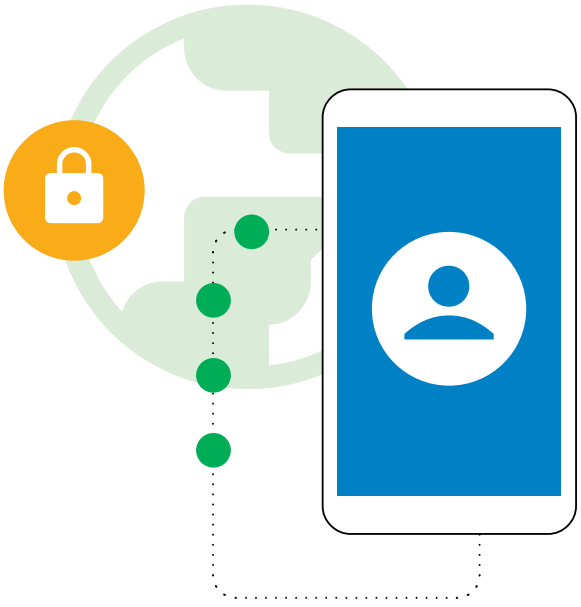
Gmail Gmail, Google Workspace for Education की मुख्य सेवाओं में से एक है. साथ ही, इसमें कई ऐसी सेटिंग उपलब्ध हैं जिनका इस्तेमाल करके, एडमिन अपने संस्थान और अपने उपयोगकर्ताओं की बेहतर तरीके से सुरक्षा कर सकते हैं. Gmail की पुष्टि करने की सुविधा की मदद से, स्पैम, फ़िशिंग, और झूठे नाम से मेल भेजे जाने से बचें. स्पैम फ़िल्टर से जुड़ी सेटिंग को कस्टमाइज़ करें. इनमें मंजूरी वाले सभी ईमेल पतों से आने वाले ईमेल की पुष्टि करना और संगठन के ईमेल पतों से आने वाले ईमेल के लिए, स्पैम फ़िल्टर बायपास करने की सुविधा को बंद करना शामिल है.

जब संभव हो, पीओपी/आईएमएपी के ऐक्सेस पर रोक लगाएं. साथ ही, मैसेज भेजने से पहले की स्कैनिंग की बेहतर सुविधा और फ़िशिंग और मैलवेयर से बेहतर सुरक्षा देने वाली सुविधाएं चालू करें. अगर कुछ या सभी उपयोगकर्ताओं को, अपने डोमेन के बाहर ईमेल भेजने या पाने की अनुमति दी जाती है, तो चेतावनी देने की सुविधा चालू करें. इससे, जब भी कोई उपयोगकर्ता ऐसा करेगा, तब उसे चेतावनी दिखेगी.

Google Workspace for Education Standard और Plus के ग्राहक, सिक्योरिटी सैंडबॉक्स का इस्तेमाल करके, नुकसान पहुंचाने वाले अटैचमेंट का पता लगाने के लिए नियम सेट कर सकते हैं. इससे मैलवेयर और रैंसमवेयर से सुरक्षा मिल सकेगी.

तीसरे पक्ष के ऐप्लिकेशन

तीसरे पक्ष के ऐसे ऐप्लिकेशन को मंजूरी देने के लिए, पहले से मौजूद, मंजूरी वाले वर्कफ़्लो का इस्तेमाल करें जो एपीआई के ज़रिए खाते का डेटा ऐक्सेस करते हैं. इससे, अनधिकृत डेटा को, तीसरे पक्ष के ऐसे ऐप्लिकेशन के साथ शेयर होने से रोका जा सकता है जिन्हें स्कूलों में इस्तेमाल किए जाने की अनुमति नहीं है.



रपिोर्ट और मॉनटिरिगि

एक एडमनि के तौर पर आपको Google Admin console में रपिोर्ट और लॉग इवेंट देखने की सुवधि मलिती है. इससे अपने संगठन में होने वाली गतविधि की समीक्षा की जा सकती है. जैसे- सुरक्षा पर संभावति खतरे, खातों में कब और कौन साइन इन करता है, और उपयोगकर्ता कैसे कॉन्टेंट बनाते और शेयर करते हैं. ग्राफ़ और टेबल के ज़रए, डोमेन लेवल के डेटा को, उपयोगकर्ता लेवल की बारीक जानकारी के साथ देखा जा सकता है. सुरक्षा से जुड़े जोखमिों की पहचान करने, सेवा उपयोग का वश्लिेषण करने, कॉन्फ़गिरेशन से जुड़ी समस्याओं का हल करने, उपयोगकर्ता गतविधि को ट्रैक करने, और ऐसी ही ज़्यादा जानकारी पाने के लए, रपिोर्ट और ऑडटि लॉग के साथ-साथ चेतावनी केंद्र देखें.

Google Workspace for Education Standard और Plus के एडमनि, सुरक्षा से जुड़ी अलग-अलग रपिोर्ट की खास जानकारी देखने, रुझानों की पहचान करने, और नए-पुराने डेटा की तुलना करने के लए, सुरक्षा डैशबोर्ड का इस्तेमाल कर सकते हैं. जैसे- Drive में फ़ाइल शेयर करना, Gmail में स्पैम, फ़शिगि, और मैलवेयर गतविधि, उपयोगकर्ता खाते से संदग्धि लॉगनि, और डवािइस पर संदग्धि गतविधियिां. सबसे ज़्यादा इस्तेमाल, गतविधि, और ऑडटि लॉग और सुरक्षा से जुड़ी रपिोर्ट, छह महीने के लए उपलब्ध रहती हैं. इन लॉग में, Admin console, Drive, Meet, और Chat के लॉग इवेंट शामलि हैं.

सुरक्षा केंद्र का इस्तेमाल करें

Google Workspace for Education Plus और Standard के एडमनि सुरक्षा केंद्र का इस्तेमाल कर सकते हैं. यह सुरक्षा से जुड़ी बेहतर जानकारी और वश्लिेषण उपलब्ध कराता है. साथ ही, इससे आपके डोमेन की सुरक्षा पर असर डालने वाली समस्याओं के बारे साफ़-साफ़ जानकारी मलिती है और इन्हें रोकने के तरीकों के बारे में पता चलता है.

सुरक्षा केंद्र में सुरक्षा जांच टूल शामलि है, जो एडमनि को सुरक्षा और नजिता से जुड़े मुद्दों को पहचानने, उनकी जांच करने, और उन पर कार्रवाई करने में, मदद कर सकता है. इन मुद्दों में, फ़शिगि हमले, गलत तरीके से फ़ाइलें शेयर करना, उपयोगकर्ता और डवािइस से जुड़ी संदग्धि गतविधि, और ऐसी ही अन्य समस्याएं शामलि हैं.

Google Workspace, बातचीत करने और साथ मलिकर काम करने की सुवधि देने वाला दुनयिा का सबसे सुरक्षति क्लाउड-नेटवि सुइट है

0

नवंबर 2021 से, Workspace में सॉफ़्टवेयर की कमयिों का फ़ायदा उठाए जाने का कोई भी मामला सामने नहीं आया है*

50%

Workspace का इस्तेमाल करके, सायबर सुरक्षा के बीमा प्रीमयिम पर 50% की बचत की जा सकती है

2गुना कम हैं

Microsoft 365 की तुलना मे, Workspace का इस्तेमाल करने वाले संगठनों में डेटा की सुरक्षा से जुड़े मामले 2 गुना कम हैं

2.5गुना कम हैं

Microsoft Exchange की तुलना में, Workspace का इस्तेमाल करने वाले संगठनों में डेटा की सुरक्षा से जुड़े मामले 2.5 गुना कम हैं

*वहीं CISA (सायबर सक्योरटिी ऐंड इन्फ़्रास्ट्रक्चर सक्योरटिी एजेंसी) के मुताबकि, इस क्षेत्र से जुड़े अन्य वेंडर के प्रॉडक्ट में ऐसे कई मामले सामने आए हैं.

Google Chromebooks for Education

Chromebook डिवाइसों में पहले से मौजूद, बेहतरीन सुरक्षा सुविधाओं की वजह से, यह छात्र-छात्राओं और शिक्षकों के लिए, एक सबसे सुरक्षित, स्केलेबल और इस्तेमाल में आसान कंप्यूटर है. कारोबार, शिक्षा या निजी ज़रूरतों के लिए इस्तेमाल होने वाले किसी ChromeOS डिवाइस पर, अब तक रैंसमवेयर हमले की कोई शिकायत नहीं मिली है. Chromebook, अप-टू-डेट सुविधाओं के ज़रिए स्कूलों को, आने वाले गंभीर खतरों से बचाने में मदद करते हैं. ये अपडेट, बैकग्राउंड में अपने-आप होते रहते हैं. इससे उपयोगकर्ताओं का समय भी बचता है.

मैलवेयर से सुरक्षा देने वाली, पहले से मौजूद सुविधाओं के साथ ओएस और ऐप्लिकेशन अपने-आप अपडेट होने "की सुविधा

साइबर हमलावर, ऑपरेटिंग सिस्टम, ब्राउज़र, और लोकप्रिय ऐप्लिकेशन में मौजूद गड़बड़ियों और खामियों का फ़ायदा उठाने की लगातार कोशिश कर रहे हैं, ताकि उनमें मैलवेयर इंस्टॉल किया जा सके और उपयोगकर्ता डेटा को चुराया जा सके. आपकी और आपके उपयोगकर्ताओं की सुरक्षा के लिए, Chromebook आपके ओएस और ऐप्लिकेशन को अप-टू-डेट रखता है. इस डिवाइस को डिफ़ॉल्ट रूप से सुरक्षित बनाया जाता है और इसकी सुरक्षा हमेशा अपडेट भी रहती है. क्लाउड ऐप्लिकेशन को, लोकल ऐप्लिकेशन की तरह सॉफ़्टवेयर अपडेट करने की कभी ज़रूरत नहीं होती. Chromebook पर मौजूद सुरक्षा चिप को Google ने डिज़ाइन किया है और यह डिवाइसों को सुरक्षित रखने, उपयोगकर्ता की पहचान की रक्षा करने, और सिस्टम को सुरक्षित रखने में मदद करती है.

आपका Chromebook, मैलवेयर से सुरक्षा देने जुड़े नए अपडेट अपने-आप लागू कर लेता है. पहले से मौजूद सुरक्षा सुविधाओं जैसे, डेटा एन्क्रिप्शन, वेरिफ़ाइड बूट, सैंडबॉक्सिंग, और अपने-आप अपडेट होने की सुविधा से, छात्र-छात्राओं और शिक्षकों को साइबर हमलों से सुरक्षित रखा जाता है.

उपयोगकर्ता का डेटा सुरक्षित करें

जब अपने Google खाते से Chromebook में साइन इन किया जाता है, तो आपका सारा डेटा एन्क्रिप्टेड फ़ाइलों में सेव हो जाता है. इससे यह पक्का होता है कि डिवाइस पर कोई भी आपके डेटा को नहीं देख सकता या आपके खाते का इस्तेमाल करके ऐप्लिकेशन में साइन-इन नहीं कर सकता है. इससे छात्रों के लिए क्लास में डिवाइसें शेयर करना और स्कूलों के लिए कंप्यूटिंग की कुल लागत को कम करना बहुत आसान और सुरक्षित हो जाता है. ज़्यादा बेहतर सुरक्षा सुविधाओं के लिए, डिवाइस को मैनेज करने से जुड़ा Chrome Education Upgrade लाइसेंस लें. इसके तहत, सुरक्षा से जुड़े मामलों को लेकर बेहतर विज़िबिलिटी मिलती है.

रिमोट तौर पर इस्तेमाल किए जा रहे और मैनेज किए जा रहे डिवाइस के लिए, सुरक्षा से जुड़ी नीतियां

स्कूल एडमिन ChromeOS की नीतियों को कॉन्फ़िगर कर सकते हैं और Google Admin console का इस्तेमाल करके, रिमोट तरीके से ही ऐप्लिकेशन इंस्टॉल/अपडेट कर सकते हैं. सिर्फ़ एक क्लिक से, एक सिंगल आईटी एडमिन लाखों Chromebook की नीतियों और कॉन्फ़िगरेशन को अपडेट कर सकता है.

इससे पक्का होता है कि

- छात्र-छात्राएं, स्कूलों की मंजूरी वाले कॉन्टेंट और ऐप्लिकेशन को ही ऐक्सेस कर सकते हैं
- सभी ऐप्लिकेशन और एक्सटेंशन पर सुरक्षा से जुड़े नए अपडेट लागू किए जाते हैं
- उपयोगकर्ता, स्कूल के डिवाइस के अलावा, किसी और डिवाइस पर स्कूल के डेटा की कॉपी नहीं बना सकते, उसे ट्रांसफ़र नहीं कर सकते या शेयर नहीं कर सकते
- साइबर हमलों से निपटने के लिए, Google के सुरक्षा से जुड़े कस्टमाइज़ सुझावों की मदद से, डेटा के आधार पर फ़ैसले लें
- सीधे Admin console में सभी उपयोगकर्ताओं के लिए, पहचान और ऐक्सेस मैनेजमेंट और सुरक्षा से जुड़ी नीतियों को एक ही जगह से मैनेज करें

यहां कुछ नीतियां हाइलाइट की गई हैं, जिन्हें एडमिन कॉन्फ़िगर कर सकते हैं:

डिवाइस की नीतियां

- **मेहमान मोड**
  आपके डिवाइस के मेहमान मोड को बंद करने का सुझाव दिया जाता है, ताकि छात्र-छात्राएं और शिक्षक, अपने क्रेडेंशियल का इस्तेमाल करके लॉग इन करें. मेहमान मोड में लॉग इन करने से यह पता नहीं चलता कि डिवाइस को किसने इस्तेमाल किया था.
- **साइन-इन करने से जुड़ी पाबंदियां**
  छात्र-छात्राओं और शिक्षकों को अपने स्कूल के Chromebook में लॉग इन करने के लिए, अपने निजी Gmail खातों का इस्तेमाल नहीं करना चाहिए. जिन डिवाइसों का इस्तेमाल खास तौर पर छात्र-छात्राएं करते हैं उनके लिए, सिर्फ़ अपने Workspace डोमेन में ही साइन-इन करने से जुड़े प्रतिबंध लागू करें.
- **उपयोगकर्ता और डिवाइस की रिपोर्टिंग**
  एडमिन को उपयोगकर्ता और डिवाइस की रिपोर्टिंग की सुविधा चालू करनी चाहिए, ताकि वे अलग-अलग मेट्रिक इकट्ठा कर सकें. जैसे- Chromebook का कितनी बार इस्तेमाल किया जा रहा है, कौन उनका इस्तेमाल कर रहा है, और उनके हार्डवेयर की स्थिति क्या है.
- **फ़ोर्स्ड री-एनरोलमेंट (डिवाइसों का अपने-आप फिर से रजिस्ट्रेशन)**
  किसी स्कूल में इस्तेमाल किए जा रहे Chromebook को तब तक स्कूल में ही रखना चाहिए, जब तक कि कोई एडमिन उसे इस्तेमाल से बाहर न कर दे. एडमिन को Chromebook के लिए, फ़ोर्स्ड री-एनरोलमेंट (डिवाइसों का अपने-आप फिर से रजिस्ट्रेशन) चालू करना चाहिए, ताकि Chromebook का डेटा मिटाए जाने या इसके चोरी होने के मामलों में, वह हमेशा खुद को री-एनरोल कर ले.

उपयोगकर्ता नीतियां

- **गुप्त मोड**
  स्कूलों के Chromebook का इस्तेमाल कर रहे छात्र-छात्राओं के लिए, इसका सेट अप कुछ ऐसे करना चाहिए कि उनका सारा ध्यान सीखने में लगे और वे सफल हो सकें. इसमें उन्हें एक सुरक्षित ब्राउज़र तक सीमित रखना शामिल है, ताकि वेब कॉन्टेंट के लिए फ़िल्टर की मदद से, उन्हें गलत वेबसाइटों से दूर रखा जा सके. एडमिन को गुप्त मोड को बंद रखना चाहिए, ताकि छात्र-छात्राएं फ़िल्टर से बचकर गलत वेबसाइटों पर न जा पाएं.
- **प्रॉक्सी मोड**
  कुछ स्कूल वेब फ़िल्टरिंग के लिए प्रॉक्सी का इस्तेमाल कर सकते हैं, लेकिन आपको इस बात का ध्यान रखना होगा कि आपके उपयोगकर्ता, प्रॉक्सी सेटिंग को खुद न बदल पाएं.
- **एक से ज़्यादा साइन इन ऐक्सेस**
  अगर उपयोगकर्ताओं को अपने स्कूल के Chromebook और Workspace खातों का इस्तेमाल करते समय, किसी सेकंडरी खाते में लॉग इन करने की अनुमति है, तो इससे उपयोगकर्ता को छात्र-छात्राओं या स्कूल के संवेदनशील डेटा या जानकारी को उस सेकंडरी खाते में आसानी से ट्रांसफ़र करने की अनुमति मिल सकती है. एडमिन को एक से ज़्यादा साइन इन ऐक्सेस को ब्लॉक करना चाहिए.
- **ब्राउज़िंग इतिहास**
  छात्र-छात्राओं के लिए, ब्राउज़िंग इतिहास को सेव रखना फ़ायदेमंद हो सकता है. अगर कोई सायबर हमला होता है, तो जांच के दौरान इतिहास के ये लॉग काम आ सकते हैं.

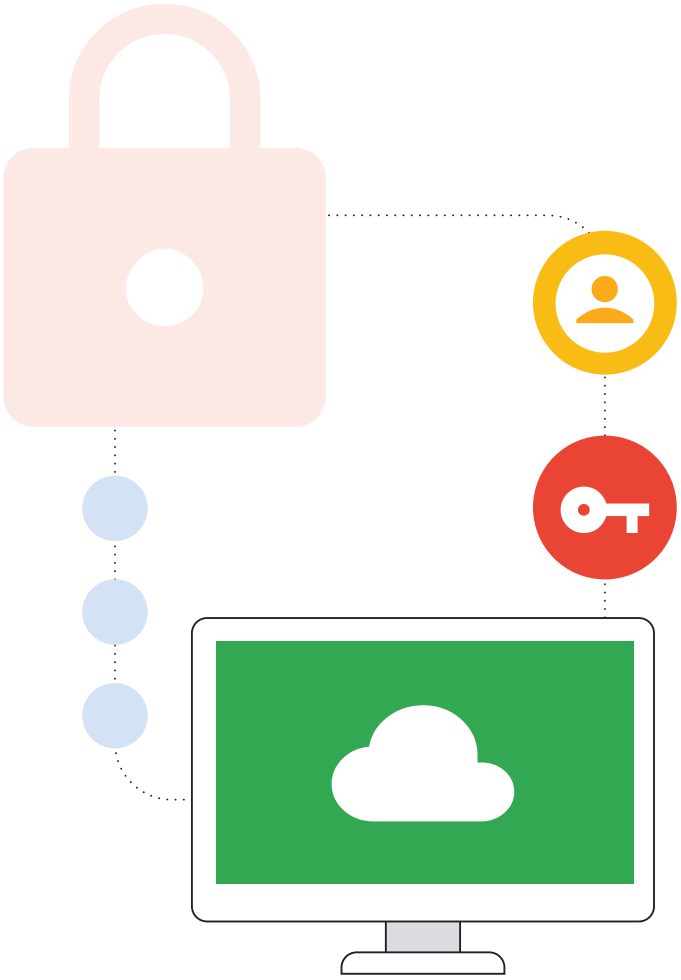
इस सूची की मदद से, यह पक्का किया जा सकता है कि आपके नेटवर्क सबसे आम तरह की गड़बड़ियों से सुरक्षित हैं. यही गड़बड़ियां, गंभीर सायबर हमलों की वजह बनती हैं. सुरक्षा नीतियों से जुड़े हमारे अन्य सुझाव, हमारी सुरक्षा चेकलिस्ट में उपलब्ध हैं.

कभी भी, कहीं भी सुरक्षित इस्तेमाल के लिए, एंडपॉइंट मैनेजमेंट

ChromeOS का रिमोट पॉलिसी मैनेजमेंट सिस्टम, एडमिन को सुरक्षा सेटिंग लागू करने में मदद करता है. साथ ही, स्कूल के नेटवर्क सर्वर के बजाय, डिवाइस पर कॉन्टेंट फ़िल्टरिंग सिस्टम जैसे सुरक्षा टूल इस्तेमाल करने में मदद करता है. इससे पक्का होता है कि छात्र-छात्राएं घर पर, स्कूल के Chromebook का वैसे ही इस्तेमाल कर सकते हैं, जैसे वे स्कूल में करते हैं. घर पर उन्हें स्कूल जैसी ही सुरक्षा सुविधाएं मिलती हैं. यह अब बहुत अहम हो गया है, क्योंकि स्कूल अब डिजिटल कॉपी-किताबों और सीखने-सिखाने के ऑनलाइन टूल की ओर बढ़ रहे हैं. साथ ही, छात्र-छात्राओं को अपना होमवर्क करने के लिए घर पर कंप्यूटर लाना पड़ता है.

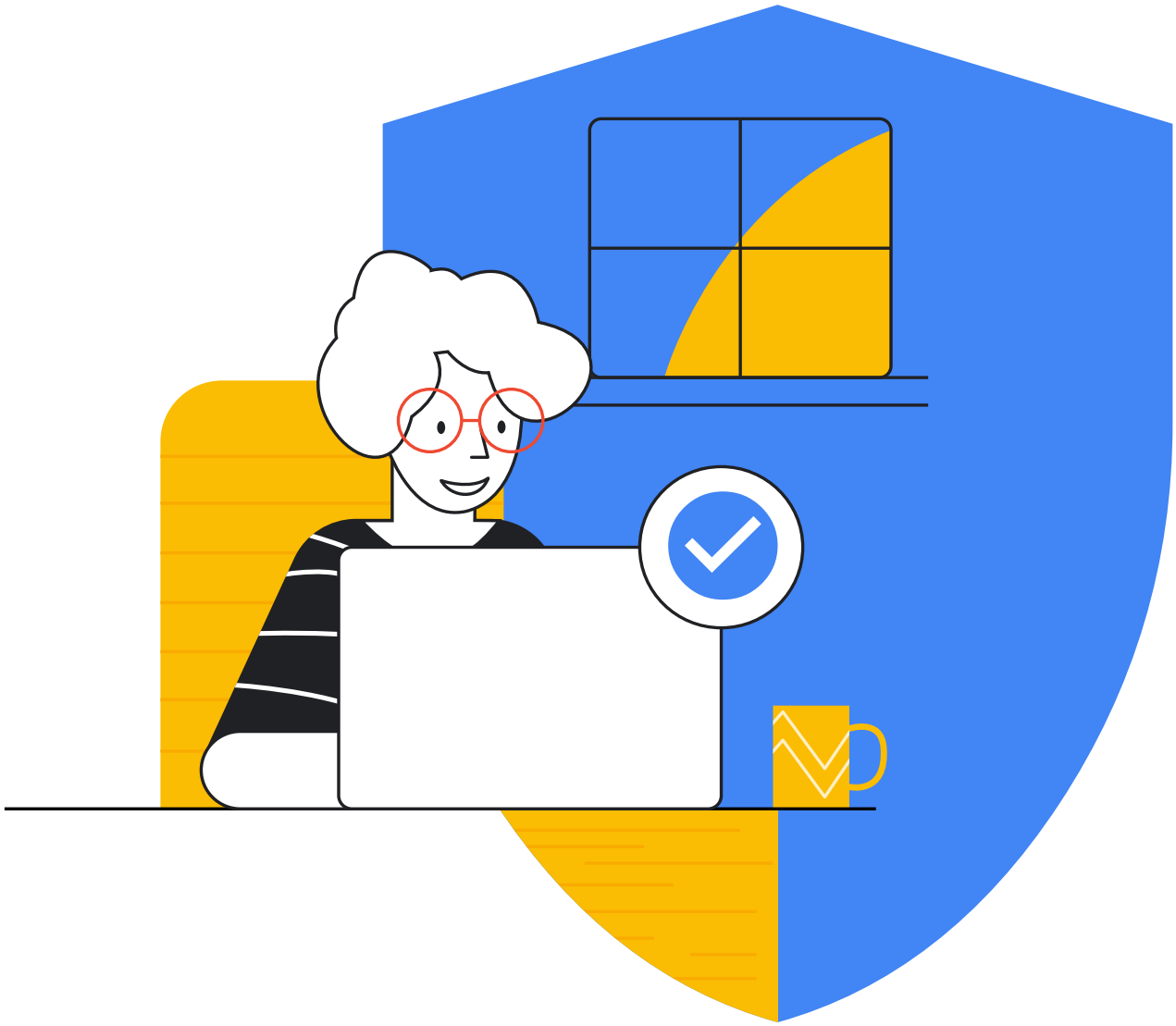
निष्कर्ष

कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों को सायबर हमलों से सुरक्षित रखने में काफ़ी चुनौतियां आती हैं, लेकिन अपनी, छात्र-छात्राओं, शिक्षकों, कर्मचारियों, और पूरे ऑनलाइन नेटवर्क की सुरक्षा के लिए, इसमें समय देना ज़रूरी है. इस दस्तावेज़ में दिए गए सुझाव, एक बहुत अच्छी शुरुआत हैं. हालांकि, हर स्कूल को अपनी खास ज़रूरतों के हिसाब से ढालकर, इन सुझावों को अपनाना होगा. साथ ही, हर दिन बढ़ रहे खतरे और उभरती टेक्नोलॉजी के साथ तालमेल बनाए रखना होगा. यह संसाधन, कडिरगार्टन से बारहवीं कक्षा तक के किसी भी संस्थान के सुरक्षा कार्यक्रम का एक ठोस आधार साबित होगा. इसकी मदद से, संस्थान अपने अगले चरण तय कर सकेंगे और सोच सकेंगे कि किन क्षेत्रों में उन्हें काम करने की ज़रूरत है. Google के पास अलग-अलग तरह के संसाधन, ट्रेनिंग मटीरियल, और सायबर सुरक्षा एक्सपर्ट भी उपलब्ध हैं. इनकी मदद से, स्कूलों और संगठनों को इस गाइडबुक का पालन करने और एआई जैसी उभरती टेक्नोलॉजी का इस्तेमाल करने में मदद मिल सकती है. सीखने-सिखाने के लिए तैयार किए गए Google प्रॉडक्ट, इस दस्तावेज़ में बताए गए कई सायबर हमलों का आसान समाधान उपलब्ध कराते हैं. हम आपके साथ काम करने के लिए उत्सुक हैं, क्योंकि आप अपने सुरक्षा कार्यक्रमों को खुद डिज़ाइन करते हैं और खुद लागू करते हैं.



संसाधन सूची

- [1]Google. “ऑनलाइन सुरक्षित रहने से जुड़ी सलाह.” Google सुरक्षा केंद्र, https://safety.google/security/security-tips/. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [2]एनआईएसटी. “साइबर सुरक्षा के इंफ्रास्ट्रक्चर में सुधार करने के लिए फ़्रेमवर्क, वर्शन 1.1.” एनआईएसटी टेक्निकल सीरीज़ पब्लिकेशन, 16 अप्रैल, 2018 https://doi.org/10.6028/NIST.CSWP.04162018. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [3]Microsoft. “Microsoft AccountGuard Program.” Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [4]Google. “Advanced Protection Program.” Google Advanced Protection Program, https://landing.google.com/advancedprotection. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [5]Google. “Google सुरक्षा केंद्र.” Google सुरक्षा केंद्र - ऑनलाइन सुरक्षित रहें, https://safety.google. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [6]Meta. “बुनियादी जानकारी: अपने खाते को सुरक्षित करने में मदद पाएं.” अपने खाते को सुरक्षित करने में मदद पाएं, https://www.facebook.com/gpa/resources/basics/security. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [7]Meta. “Facebook Protect.” Facebook, https://www.facebook.com/gpa/facebook-protect. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- [8]एनआईएसटी. “SP 800-124 Rev. 1: एंटरप्राइज़ में मोबाइल डिवाइसों की सुरक्षा को मैनेज करने के लिए दिशा-निर्देश.” एनआईएसटी टेक्निकल सीरीज़ पब्लिकेशन, https://doi.org/10.6028/NIST.SP.800-124r1. 6 अक्टूबर, 2022 को ऐक्सेस किया गया.
- पासकी: https://developers.google.com/identity/passkeys
- कडिरगार्टन से बारहवीं कक्षा तक के संस्थानों के लिए, CISA की साइबर सुरक्षा से जुड़ी रिपोर्ट: हमारे भविष्य की सुरक्षा https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO की रिपोर्ट https://www.gao.gov/products/gao-20-644
- Google for Education आपके संस्थान की सुरक्षा में कैसे मदद कर सकता है, इस बारे में ज़्यादा जानकारी के लिए, Google for Education के निजता और सुरक्षा केंद्र पर जाएं.
- Zscaler की फ़िशिंग रिपोर्ट



Google for Education