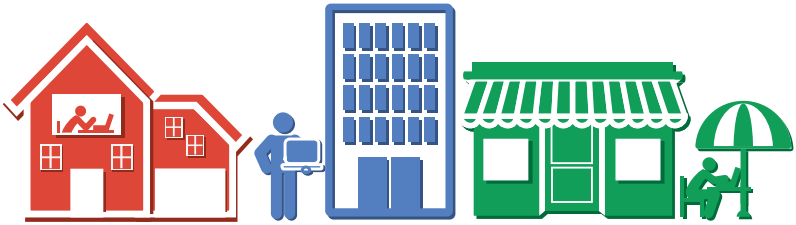
गूगल सुरक्षा केंद्र (सेफ्टी सेंटर)

ऑनलाइन सुरक्षित और निश्चिंत रहने के लिए मार्गदर्शक (गाइड)



Google

यह पुस्तिका किस बारे में है?

गूगल सुरक्षा केंद्र का लक्ष्य इंटरनेट पर सुरक्षित और निश्चिंत रहने में आपकी, आपके परिवार और आपके मित्रों की सहायता करना है।

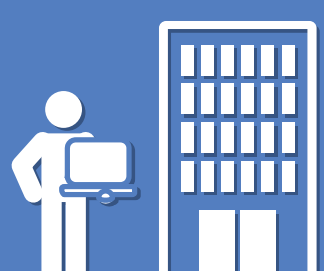
यह पुस्तिका आपको उपयोगी संकेत और सूत्र देने के लिए तैयार की गई है जिन्हें याद रखना और अमल में लाना आसान है। हमने कुछ प्रमुख सलाहों के साथ चिप्पियां या स्टिकर भी जोड़ दिए हैं ताकि उन्हें याद रखने में सहायता दिलाने के लिए आप उन्हें अपने कंप्यूटर या नोटबुक पर लगा सकें।

इस पुस्तिका के सभी विषयों के बारे में गहराई से जानकारी के लिए सुरक्षा केंद्र की वेबसाइट www-google-com/safetycenter पर जाएं।

विषयसूची

आप ऑनलाइन सुरक्षित और निश्चिंत कैसे रह सकते हैं

सुरक्षित ढंग से आरंभ करें। इंटरनेट खोजने, रचने और मिलकर काम करने के बहुत अधिक अवसर प्रदान करता है। वेब का अधिकाधिक लाभ उठाने के लिए आपको यह जानना आवश्यक है कि स्वयं को सुरक्षित और निश्चिंत कैसे रखें। आप इंटरनेट के नए उपयोगकर्ता हों या विशेषज्ञ, यहां दिए गए सुझाव और तरीके सुरक्षित और निश्चिंत ढंग से वेब की खोजबीन करने में आपकी सहायता कर सकते हैं।



• अक्षरों, संख्याओं और प्रतीकों या चिह्नों को मिलाएं

• प्रत्येक वेबसाइट के लिए अलग पासवर्ड का उपयोग करें

अपने पासवर्ड को सुरक्षित बनाएं।

पासर्वड साइबर अपराधियों के विरुद्ध पहली रक्षापंक्ति है। सुदृढ़ पासवर्ड चुनने अत्यंत आवश्यक हैं जो आपके प्रत्येक महत्त्वपूर्ण अकाउंट के लिए अलग–अलग हों, और अपने पासवर्ड को नियमित रूप से अपडेट करना अच्छी आदत है। सुदृढ़ पासवर्ड बनाने के लिए इन सूत्रों का पालन करें और उन्हें सुरक्षित रखें।

1. अपने प्रत्येक महत्त्वपूर्ण अकाउंट, जैसे ई–मेल और ऑनलाइन बैंकिंग, के लिए एक अनूठे पासवर्ड का उपयोग करें।

2. संख्याओं, अक्षरों और प्रतीकों को मिलाकर बनाए गए लंबे पासवर्ड का उपयोग करें।

3. यदि आपको अपने पासवर्ड को रिसेट करने की आवश्यकता हो तो कई सेवाएं आपको रिकवरी ई–मेल एड्रेस या पते पर ई–मेल भेजेंगी, इसलिए सुनिश्चित करें कि आपका रिकवरी ई–मेल पता अपडेट हो और एक ऐसे अकाउंट से जुड़ा हो जिस तक आप अभी भी पहुंच सकते हैं।

एक तरीका तो यह है कि एक ऐसा मुहावरा या वाक्यांश सोचें जो केवल आपको पता हो, और उसे याद रखने में सहायता के लिए किसी वेबसाइट विशेष के साथ संबंद्ध कर दें। अपने ई–मेल अकाउंट के लिए आप ऐसे किसी मुहावरे या वाक्यांश से आरंभ कर सकते हैं, जैसे "My friends Tom and Jasmine send me a funny email once a day" (मेरे मित्र टॉम और जैसमिन दिन में एक बार मुझे मजेदार ई–मेल भेजते हैं), और फिर इसकी पुनर्रचना करने के लिए संख्याओं और अक्षरों का उपयोग करें। "MfT&Jsmafe1ad" एक ऐसा पासवर्ड है जिसमें कई भिन्नताएं हैं। फिर इस प्रकिया को अन्य वेबसाइटों के लिए भी दोहराएं।

• संदिग्ध संदेशों के उत्तर में व्यक्तिगत जानकारियां न दें

पहचान को चोरी होने से को रोकें।

अपराधी जिन सामान्य तरकीबों का प्रयोग करते हैं, उनके बारे में जानने से आपको ऑनलाइन धोखाधड़ी और पहचान की चोरी से अपने को बचाने में सहायता मिलती है। यहां कुछ आसान सूत्र दिए गए हैं :

1. यदि आप अपनी व्यक्तिगत या वित्तीय जानकारी मांगने वाला कोई संदिग्ध ई–मेल, क्षणिक संदेश या एक वेबपेज देखें तो उसका उत्तर न दें।

2. यदि आप किसी ऐसे ई–मेल या चैट में दी गई लिंक के द्वारा एक साइट पर आएं हैं, जिस पर आप विश्वास न करते हों, तो उस पर अपना पासवर्ड कदापि न डालें।

3. ई–मेल के माध्यम से अपना पासवर्ड न भेजें और इसे दूसरों के साथ साझा न करें।

यदि आप एक ऐसे व्यक्ति का संदेश देखें जिसे आप जानते हैं, किंतु ऐसा लगता नहीं है कि यह उन्होंने भेजा है, तो हो सकता है कि उनका अकाउंट किसी साइबर अपराधी के हाथों में पड़ गया हो जो आपसे धन या जानकारी प्राप्त करने का प्रयास कर रहा हो। इसका उत्तर देते हुए सावधानी बरतें, या कोई उत्तर ही न दें। इन अपराधियों की साझा तरकीबों में शामिल हैं : तत्काल धन भेजने के लिए आपसे कहना, दूसरे देश में फंस जाने का दावा करना या कहना कि उनका फोन चोरी हो गया है इसलिए बात नहीं कर पा रहे हैं। ऐसा संदेश आपसे किसी लिंक पर क्लिक करने या एक तस्वीर या वीडियो देखने के लिए कह सकता है, जो वास्तव में आपको एक ऐसी साइट पर ले जाता है जहां आपकी जानकारी चुराई जा सकती है। क्लिक करने से पहले सोचें!

- संदिग्ध पोस्ट या ई–मेल का उत्तर न दें।
- घोटालों से बचने के लिए ऑनलाइन सौदों की जांच–पड़ताल करें
- यदि यह इतना अच्छा लगता है कि इसके सच्चे होने पर संदेह होता है, कि यह शायद ऐसा ही है

घोटालों से बचें।

वेब बहुत अच्छी जगह हो सकती है, लेकिन हरेक ऑनलाइन व्यक्ति के इरादे अच्छे नहीं होते। यहां तीन सरल उपाय दिए जा रहे हैं जिनसे वेब पर घोटालाबाजों से बचा और सुरक्षित रहा जा सकता है :

1. उपहार देने वाले अजनबियों से सावधान रहें। यदि कोई आपसे कहता है कि आप विजेता हैं और आपसे एक फॉर्म में आपकी निजी जानकारियां भरने के लिए कहता है, तो उस फॉर्म को भरने के प्रलोभन में न पड़ें। अगर आप 'सब्मिट' बटन को नहीं भी दबाते हैं, किंतु यदि उनके फॉर्म में अपनी जानकारियां भरना शुरू कर देते हैं, तब भी आप उन्हें अपनी जानकारी भेज रहे हो सकते हैं।

2. जांच–पड़ताल करें। जब ऑनलाइन खरीदारी कर रहे हों, तब विक्रेता के बारे में जांच–पड़ताल करें। संदेह पैदा करने वाली कम कीमतों से सावधान रहें, उसी तरह जैसे आप स्थानीय दुकान से सामान खरीदते समय होते हैं। ऑनलाइन सौदों की छानबीन करें जो इतने अच्छे लगते हैं कि उनके सच्चे होने पर संदेह होता है। कोई भी धोखे में पड़कर नकली सामान खरीदना नहीं चाहता।

3. जब भी संदेह हो, एहतियात बरतें। क्या आपको एक विज्ञापन या एक पेशकश को लेकर अजीब–सा महसूस हो रहा है? अपने मन की भावना पर विश्वास करें! केवल उन्हीं साइटों पर विज्ञापनों पर क्लिक करें या सामान खरीदें जो सुरक्षित, परखी हुई और भरोसेमंद हैं।

- सार्वजनिक या साझा कंप्यूटरों से लॉग आउट करें
- उपकरण या स्क्रीन को इस तरह सेट कर दें ताकि वे अपने आप लॉक हो जाएं।

अपनी स्क्रीन या उपकरण को लॉक करें।

आप जब अपने कंप्यूटर, लैपटॉप या फोन का उपयोग बंद कर रहे हों, तब आपको अपनी स्क्रीन हमेशा लॉक कर देनी चाहिए। यह कदम फोन या टैबलेट के लिए विशेष रूप से आवश्यक है, क्योंकि उनके इधर–उधर रखे जाने की और ऐसे लोगों के हाथों में पड़ने की ज्यादा संभावना होती है जिन्हें आप अपनी जानकारियों तक पहुंचने देना नहीं चाहते। साझा जगहों पर रखे घर के कंप्यूटरों के साथ भी ऐसा ही करें। अतिरिक्त सुरक्षा के लिए आपको अपने उपकरण को इस प्रकार सेट कर देना चाहिए जिससे वह स्लीप में जाते या बंद होते समय अपने आप लॉक हो जाए।

- अपने घर के रॉउटर को डब्ल्यूपीए2 पासवर्ड से सुरक्षित करें

सुरक्षित नेटवर्क का उपयोग करें।

जब भी आप किसी ऐसे नेटवर्क का उपयोग करते हुए ऑनलाइन जाते हैं, जिसे आप जानते या विश्वास नहीं करते, जैसे जब आप स्थानीय कैफे के मुफ्त वाई–फाई का उपयोग करते हैं, तो अतिरिक्त सावधानी बरतना हमेशा अच्छा होता है। यह संभव है कि सेवा प्रदाता अपने नेटवर्क पर सारी आवाजाही देख रहा हो, जिसमें आपकी व्यक्तिगत जानकारी भी शामिल हो सकती है।

जब आप सार्वजनिक वाईफाई से माध्यम से जुड़ते हैं, तब यदि आपका कनेक्शन एनक्रिप्टेड नहीं है तो आसपास का कोई भी व्यक्ति आपके कंप्यूटर और वाईफाई हॉटस्पॉट के बीच जाने वाली सारी जानकारी पर नजर रख सकता है। सार्वजनिक नेटवर्कों पर बैंकिंग या खरीदारी जैसे महत्त्वपूर्ण कार्य करने से बचें।

यदि आप घर पर वाईफाई का उपयोग करते हैं, तो अपने नेटवर्क को सुरक्षित बनाना सुनिश्चित करें ताकि अन्य लोग इसका उपयोग न कर सकें। अपने वाईफाई नेटवर्क की सुरक्षा के लिए एक पासवर्ड लगाकर इसे सुरक्षित करें – और ठीक जिस प्रकार आप अन्य पासवर्ड चुनते समय करते हैं, सुनिश्चित करें कि आप एक लंबा, संख्याओं, अक्षरों और प्रतीकों या चिह्नों के अनूठे मिश्रण वाला पासवर्ड चुनें ताकि दूसरे आसानी से आपके पासवर्ड का अंदाज नहीं लगा पाएं। अधिक सुदृढ़ सुरक्षा के लिए अपना नेवटर्क समनरूप बनाते या कन्फिगर करते समय डब्ल्यूपीए2 सेटिंग चुनें।

अंत में, सुरक्षा की अतिरिक्त परत के लिए पासवर्ड का उपयोग करके अपने रॉउटर की सुरक्षा सुनिश्चित करें। रॉउटर का पूर्वनिश्चित या डिफॉल्ट पासवर्ड अपराधियों को पता हो सकता है, इसलिए इसका उपयोग करने के स्थान पर स्वयं अपना पासवर्ड सेट करने के लिए अपने इंटरनेट सेवा प्रदाता अथवा रॉउटर विनिर्माता द्वारा दिए गए निर्देशों का पालन करें। यदि अपराधी आपके रॉउटर तक पहुंचने में सफल हो जाते हैं, तो वे आपकी सेटिंग बदल सकते हैं और आपकी ऑनलाइन गतिविधियों में ताकझांक कर सकते हैं।

- गूगल खाते के लिए दो चरणों का सत्यापन सेट करें
- साझा करने से पहले सेटिंग की जांच करें

अपने गूगल सुरक्षा और गोपनीयता टूल को जानें।

गूगल के साथ आपके पास कई प्रकार के टूल होते हैं जो आपको सुरक्षित रखने और आपकी जानकारी को निजी और सुरक्षित रखने में सहायता कर सकते हैं। यहां हमारे कुछ सबसे लोकप्रिय टूल की जानकारी दी जा रही है जो आपके लिए गूगल को बेहतर कार्य करने में सहायता करते हैं।

दो–चरण सत्यापन

आपके गूगल खाते को और भी सुदृढ़तर स्तरों की सुरक्षा प्रदान करने के लिए हम अपने उपयोगकर्ताओं को दो चरणों के सत्यापन की पेशकश करते हैं। इस टूल में गूगल खाते में साइन–इन करने के लिए न केवल पासवर्ड की बल्कि एक सत्यापन कोड की भी आवश्यकता होती है, जिससे यह सुरक्षा की एक अतिरिक्त परत जोड़ देता है। दो–चरण सत्यापन में आपसे केवल आपके फोन पर भेजा गया एक कोड डलवा कर गूगल यह सुनिश्चित करता है कि यह आप ही हैं – बहुत ही कम संभावना होती है कि कोई दूर बैठा आक्रमणकर्ता कोड और आपका पासवर्ड दोनों हासिल कर सकेगा।

गूगल खाते की सेटिंग

अपने अकाउंट सेटिंग पेज पर आप गूगल खाते के साथ जुड़ी सेवाओं और जानकारियों को देख सकते हैं और अपनी सुरक्षा और प्राइवेसी सेटिंग बदल सकते हैं।

यू ट्यूब प्राइवेसी सेटिंग

हो सकता है कि कभी आप अपने यू ट्यूब वीडियो को अपने मित्रों के छोटे–से समूह के साथ बांटना या केवल स्वयं अपने तक सीमित रखना चाहते हों। यदि ऐसा है, तो अपने वीडियो को अपलोड करते समय आप अपने वीडियो को या तो "अनलिस्टेड" या असूचीबद्ध (सर्च या खोज के परिणामों से छिपा रहेगा, किंतु वे लोग देख सकेंगे जिनके पास इसकी लिंक है) अथवा "प्राइवेट" या निजी (केवल आप ही देख सकेंगे) रखने का चुनाव कर सकते हैं।

अपने गूगल सुरक्षा और निजता उपकरणों को जानें।

अपने गूगल खाते में रखे डाटा का प्रबंध करें।

गूगल डैशबोर्ड आपको दिखाता है कि आपके गूगल खाते में क्या रखा है और यह आपकी हाल ही की कुछ खाता गतिविधियों की संक्षिप्त जानकारी प्रदान करता है। एक केंद्रीय स्थान से आप अपना डाटा और गतिविधि आसानी से देख सकते हैं और सेवाओं जैसे ब्लॉगर, गूगल कैलेंडर, गूगल डॉक्स, गूगल और कई अन्य के लिए अपनी सेटिंग तक पहुंच सकते हैं।

अपनी पसंद के एड्स या विज्ञापन का प्रबंध करें।

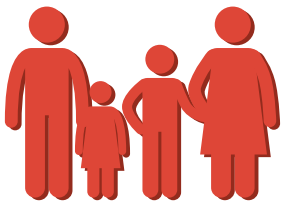
एड्स या विज्ञापन ऐसी अनेक निशुल्क ऑनलाइन सेवाओं के लिए धन जुटाते हैं जिन्हें आप बहुत चाहते और प्रति दिन उपयोग करते हैं। गूगल की एड्स सेटिंग्ज के साथ आप समझ सकते हैं कि आपके लिए विज्ञापन कैसे चुने जाते हैं, एड्स के चयन के लिए उपयोग की गई जानकारी को नियंत्रित कर सकते हैं और कुछ निश्चित विज्ञापनों को रोक सकते हैं।

प्रबंध करें कि आप जो साझा करें उसे कौन देखे।

गूगल+ सर्कल आपको मित्रों और संपर्कों का प्रबंध करने में सहायता करते हैं। आप अपने मित्रों को एक सर्कल में, अपने परिवार को दूसरे सर्कल में और अपने बॉस को एक सर्कल में बिल्कुल अकेला रख सकते हैं – ठीक वैसे ही जैसे आप वास्तविक जीवन में करते हैं। फिर आप संबंधित सामग्री जैसे गूगल पोस्ट, यू ट्यूब वीडियो, या गूगल लोकल लिस्टिंग एड्स अपने चुने हुए किसी भी समय पर सही लोगों के साथ साझा कर सकते हैं।

ऐसी सुरक्षा चुनें जो आपके परिवार के लिए उपयुक्त हो

नींव डालने का काम करें। माता–पिता या अभिभावक के नाते आप जानते हैं कि आपके परिवार के लिए क्या अच्छा महसूस होता है और आपके बच्चे अच्छे से अच्छा कैसे सीख सकते हैं। निरंतर बदलती ऑनलाइन दुनिया में नई टेक्नोलॉजी, गैजेट्स और सेवाओं की छानबीन करने में अपने परिवार की सहायता करने के लिए आपको व्यावहारिक सलाह लेने की आवश्यकता होती है। यही कारण है कि हम दुनिया भर के सुरक्षा विशेषज्ञों, माता–पिताओं, शिक्षादाताओं और समुदायों से लगातार बात करते रहते हैं – ताकि हमें अच्छी तरह पता हो कि क्या उपयोगी और सफल है। साथ मिलकर हम उत्तरदायी डिजिटल नागरिकों का एक समुदाय विकसित करने में सहायता कर सकते हैं।



पारिवारक सुरक्षा की बुनियादी बातें

व्यस्त माता–पिताओं के लिए यहां कुछ तुरंत सुझाव हैं कि वे अपने परिवार को ऑनलाइन सुरक्षित कैसे रख सकते हैं :

1. **ऑनलाइन सुरक्षा के बारे अपने परिवार के साथ बात करें।**
   अपने परिवार के नियम–कायदों और टेक्नोलॉजी से अपेक्षाओं, साथ ही अनुचित उपयोग के परिणामों के बारे में पूरी तरह स्पष्ट रहें। और सबसे महत्त्वपूर्ण बात, सुनिश्चित करें कि आपका परिवार कठिन निर्णयों का सामना करने पर पर्याप्त सहजता के साथ मार्गदर्शन के लिए कह सके। यह चर्चा इंटरनेट पर अकेले खोजबीन करते समय आपके परिवार को सुरक्षित महसूस करने में सहायता कर सकती है और यह जानने में भी कि अपनी शंकाओं के समाधान के लिए वे किसके – आपके – पास आएं।

2. **साथ मिलकर प्रौद्योगिकी का उपयोग करें।**
   यह ऑनलाइन सुरक्षा सिखाने का अच्छा तरीका है, और इससे आपको ऐसे अवसर मिलते हैं जब आप ऑनलाइन सुरक्षा के विषय सामने आने पर अपने परिवार के साथ उन्हें सुलझा सकते हैं।

3. **ऑनलाइन सेवाओं और साइटों की चर्चा करें।**
   अपने परिवार से बात करें कि उन्हें किस किस्म की साइटें अच्छी लगती हैं और परिवार के प्रत्येक सदस्य के लिए क्या उपयुक्त है।

4. **पासवर्डों की सुरक्षा करें।**
   यह सीखने में अपने परिवार की सहायता करें कि ऑनलाइन सुरक्षित पासवर्ड कैसे सेट किए जाते हैं। अपने परिवार को याद दिलाएं कि वे विश्वासपात्र बड़ों, जैसे माता–पिता, को छोड़कर अपने पासवर्ड किसी को भी न दें। सुनिश्चित करें कि जब वे स्कूल में, कैफे में या पुस्तकालय में सार्वजनिक कंप्यूटरों पर हों तो अपने ऑनलाइन अकाउंट या खातों से साइन–आउट करने की आदत डालें।

5. **प्राइवेसी सेटिंग और साझेदारी के नियंत्रणों का उपयोग करें।**
   विचारों, तस्वीरों, वीडियो, स्टेटस अपडेट्स और बहुत कुछ साझा करने के लिए कई साइटें मौजूद हैं। इनमें से कई सेवाएं प्राइवेसी सेटिंग की पेशकश करती हैं जो आपको अपनी सामग्री पोस्ट करने से पहले यह तय करने में सहायता करती हैं कि कौन उसे देख सकता है। अपने परिवार से बात करके उन्हें बताएं कि उन्हें सार्वजनिक रूप से क्या साझा करना चाहिए और क्या नहीं करना चाहिए। परिवार और मित्रों के बारे में व्यक्तिगत विवरणों को निजी रखकर और सार्वजनिक रूप से साझा की जा रही सामग्री में नाम से लोगों को चिह्नित न करके दूसरों की गोपनीयता का सम्मान करने में उनकी सहायता करें।

6. **आयु संबंधी प्रतिबंधों की जांच करें।**
   कई ऑनलाइन सेवाओं – गूगल सहित – के आयु सीमा संबंधी नियम और प्रतिबंध हैं कि कौन उनकी सेवाओं का उपयोग कर सकता है। उदाहरण के लिए, आपको गूगल अकाउंट रखने के लिए आयु की शर्त को पूरा करना पड़ता है, और गूगल के कुछ उत्पाद 18 वर्ष या उससे ऊपर के उपयोगकर्ताओं के लिए ही हैं। अपने बच्चों को अकाउंट के लिए साइन–इन करने की अनुमति देने से पहले हमेशा उस वेबसाइट की उपयोग शर्तों या टर्म्स ऑफ यूज की जांच–पड़ताल करें, और यदि आपने पारिवारिक नियम बना रखे हों कि बच्चे कौन–सी साइटों और सेवाओं का उपयोग कर सकते है तो यह उन्हें पूर्णतः स्पष्ट कर दें।

7. **अपने परिवार को उत्तरदायी संचार के लिए शिक्षित करें।**
   एक अच्छा व्यावहारिक नियम यह है : यदि आप कोई बात किसी के मुंह पर नहीं कहेंगे, तो उसे टेक्स्ट, ई–मेल, इंस्टेंट मेसेज से भी न भेजें और न ही किसी के पेज पर कमेंट के रूप में पोस्ट करें। उनके साथ चर्चा करें कि आपकी ऑनलाइन कही हुई बात से दूसरे कैसा महसूस कर सकते हैं और पारिवारिक दिशानिर्देश तय करें कि किस किस्म का संचार उपयुक्त है।

8. **अन्य वयस्कों और विशेषज्ञों से चर्चा करें।**
   अपने मित्रों, विस्तारित परिवार, शिक्षकों, गुरुओं और परामर्शदाताओं के साथ चर्चा छेड़ें। विशेषकर यदि आपका वास्ता एक ऐसी टेक्नोलॉजी से है जिससे आप परिचित नहीं हैं, तो अन्य माता–पिता और बच्चों के साथ काम करने वाले पेशेवर व्यक्ति यह निर्णय करने में सहायता के लिए बड़ा संसाधन हो सकता है कि आपके परिवार के लिए क्या सही प्रतीत होता है।

9. **अपने कंप्यूटर और पहचान की रक्षा करें।**
   एंटीवायरस सॉफ्टवेयर का उपयोग करें और इसे नियमित रूप से अपडेट करें, जब तक कि आप क्रोमबुक का उपयोग न कर रहे हों जिसे एंटीवायरस सॉफ्टवेयर की आवश्यकता नहीं होती। अपने परिवार के साथ बात करके उन्हें बताएं कि किस प्रकार की व्यक्तिगत जानकारी – जैसे सामाजिक सुरक्षा नंबर, फोन नंबर या घर का पता – को ऑनलाइन पोस्ट नहीं करना चाहिए। अपने परिवार को सिखाएं कि अनजान लोगों से मिली फाइलें न तो स्वीकार न करें या न ही ई–मेल अटैचमेंट खोलें।

10. **हमेशा करते रहें।**
    सुरक्षित रहने के लिए एक बार उपाय करना काफी नहीं हैं – टेक्नोलॉजी विकसित होती रहती है और आपके परिवार की जरूरतें भी बढ़ती रहेंगी। सुनिश्चित करें कि आप लगातार बातचीत करते रहें। अपने परिवार के बुनियादी नियम–कायदों को फिर से कायम से करें, प्रत्येक सदस्य की प्रगति की पड़ताल करें और नियमित अंतराल से बात करने के लिए अलग से समय तय करें। यहां हमारे सहभागियों की ओर से कुछ सूत्र बताएं जा रहे हैं जो माता–पिता की चिंताओं से जुड़े साझा मुद्दों को संबोधित करते हैं।

उपयोग में सरल सुरक्षा उपकरणों के बारे में सीखें।

गूगल के सुरक्षा उपायों के बारे में जानें जो आपके परिवार द्वारा ऑनलाइन देखी जाने वाली चीजों पर नियंत्रण रखने में सहायता के लिए बनाए गए हैं।

सर्च या खोज से परिवार के अनुकूल परिणाम प्राप्त करें।

गूगल सेफसर्च को समर्थ या एनेबल करके आप ऐसी अधिकांश वयस्क सामग्री को अलग हटा सकते हैं जिनसे आप और आपका परिवार बचना चाहता है। यदि कोई अनुपयुक्त परिणाम चोरी छिपे आ जाए तो आप गूगल को बता सकते हैं। हम सामग्री को छानने वाली हमारी छन्नियों या फिल्टरों में सुधार के लिए हमेशा काम करते रहते हैं और इस प्रकार की प्रतिपुष्टि या फीडबैक सेफसर्च को हरेक के लिए बेहतर बनाने में हमारी सहायता कर सकता है।

अनुपयुक्त सामग्री को बाहर रखने के लिए फिल्टर सेट करें।

यदि आप यू ट्यूब को पलटते समय वयस्क या आयु–निषिद्ध सामग्री को नहीं देखना चाहें, तो यू ट्यूब के किसी भी पेज के निचले भाग में जाएं और सेफ्टी मोड या सुरक्षा विधि को समर्थ या एनेबल कर दें। सेफ्टी मोड सर्च या खोज से संभावित रूप से आपत्तिजनक सामग्री, संबंधित वीडियो, प्लेलिस्ट, शो और फिल्मों को अलग करने में सहायता करता है।

साझा क्रोमबुक से उपयोगकर्ता पर निगाह रखें।

आप अपने परिवार की वेब गतिविधियों पर निगाह रखने के लिए हमेशा वहां मौजूद नहीं रह सकते। जब आप उनके साथ कमरे में न हों, उस समय के लिए सुपरवाइज्ड यूजर फॉर गूगल क्रोम है। इस उपाय को समर्थ या एनेबल करके आप उपयोगकर्ता द्वारा देखे गए पन्नों के इतिहास पर दोबारा नजर डाल सकते हैं, कुछ निश्चित साइटों की अनुमति दे सकते या उन्हें रोक सकते हैं, और तय कर सकते हैं कि आपके परिवार के सदस्य कौन–सी वेबसाइटें देख सकते हैं।

स्वीकृत ऐप्स और गेम्स तक पहुंच को सीमित करें।

आप अपने टैबलेट को इस तरह साझा करना चाहते हैं कि आपकी सारी सामग्री साझा न हो? 4.3 और उससे ऊपर के संस्करण से चलने वाले एंड्रोइड टैबलेट पर आप ऐसी निषिद्ध प्रोफाइलें बना सकते हैं जो आपके टैबलेट पर फीचर और सामग्री तक अन्य उपयोगकर्ताओं की पहुंच को सीमित कर देंगे।

आयु के अनुसार उपयुक्त ऐप्स चुनने के लिए ऐप रेटिंग का उपयोग करें।

ठीक फिल्मों की तरह ही आप रेटिंग देखकर तय कर सकते हैं कि कौन–से गूगल प्ले ऐप आपके परिवार के लिए उपयुक्त हैं। ये रेटिंग हैं : एवरीवन यानी हरेक के लिए, लो मैच्योरिटी यानी कम परिपक्व, मीडियम मैच्योरिटी यानी मध्यम परिपक्व या हाई मैच्योरिटी यानी उच्च परिपक्व। आप लेवल या स्तर से ऐप्स को छांट सकते हैं और छांटने के स्तर को एक सरल पिन कोड (अन्य उपयोगकर्ताओं को दुर्घटनावश फिल्टर को डिसएबल या असमर्थ करने से दूर रखकर) से लॉक भी कर सकते हैं।

गूगल के सुरक्षा उपायों के बारे में जानें जो आपके परिवार को अपनी ऑनलाइन प्रतिष्ठा की निगरानी में सहायता के लिए बनाए गए हैं।

अनचाहे कमेंट (टिप्पणियों) या टैग (चिटों) को रोकें।

यदि आप किसी व्यक्ति की पोस्ट गूगल पर देखना नहीं चाहते हों, तो आप उन्हें उनकी प्रोफाइल पर जाकर और रिपोर्ट/ब्लॉक (व्यक्ति का नाम) का चयन करके रोक सकते हैं। आप निश्चित पोस्ट को म्यूट या खामोश भी कर सकते हैं ताकि उनका आपकी धारा में दिखाई देना बंद हो जाए।

अपने वीडियो के बारे में बकबक को नियंत्रित करें।

अपने यू ट्यूब चैनल पर कमेंट या टिप्पणियों को नियंत्रित करना आसान है। आप टिप्पणियों को हटाना, या कुछ निश्चित लोगों की अथवा कुछ निश्चित कीवर्ड या प्रमुख शब्दों वाली टिप्पणियों को रोकना चुन सकते हैं, इससे पहले कि आप उन्हें दोबारा देखें।

आक्रामक यू ट्यूब उपयोगकर्ताओं को ब्लॉक करें।

यदि कोई आपके वीडियो या चैनल पर ऐसी टिप्पणियां कर रहा है जो आपको पसंद नहीं हैं, तो आप उन्हें यू ट्यूब पर ब्लॉक या अवरुद्ध कर सकते हैं। फिर वे आपकी सामग्री पर न तो टिप्पणी कर पाएंगे या न ही निजी संदेश भेज पाएंगे।

ताकझांक करने वाली नजरों को अपने उपकरण से दूर रखें।

अपनी स्क्रीन को लॉक करना न केवल अपने अकाउंट की रक्षा करने का अत्यंत आवश्यक हिस्सा है, बल्कि यदि आप संयोग से अपना फोन कहीं दूर छोड़ दें तो यह यह भी सुनिश्चित करता है कि दूसरे लोग आपके फोन में ताकझांक न कर सकें। अपने फोन या टैबलेट पर स्क्रीन को लॉक करने की सेटिंग करने के लिए आप एक पिन, पासवर्ड या पैटर्न का चयन कर सकते हैं।

आक्रामक सामग्री के बारे में बताएं।

यदि कोई गूगल, यू ट्यूब, या ब्लॉगर पर अनुचित टिप्पणी या पोस्ट डालता है तो आप उसके बारे में रिपोर्ट कर सकते हैं। सामग्री के बारे में गूगल की स्पष्ट नीति है जो बताती है कि इन साइटों पर क्या करना उचित है और क्या नहीं, इसलिए यदि आप ऐसी सामग्री या व्यवहार देखें जो हमारी नीतियों का उल्लंघन करता हो, तो आप उसे समीक्षा के लिए फ्लैग कर सकते हैं। हम फ्लैग की हुई सामग्री की चौबीसों घंटे समीक्षा करते हैं, और हम सामग्री को हटा सकते हैं और हमारी नीतियों का उल्लंघन करने वाले उपयोगकर्ताओं के खातों को प्रतिबंधित या बंद भी कर सकते हैं।

आपकी सुरक्षा में गूगल कैसे सहायता करता है

इंटरनेट एक अद्भुत चीज है। लेकिन ऑफलाइन या वास्तविक दुनिया की तरह ही हरेक ऑनलाइन व्यक्ति के इरादे अच्छे नहीं होते। गूगल आपकी निजता और सुरक्षा को बहुत गंभीरता से लेता है। हम आपकी जानकारी की सुरक्षा के लिए प्रति वर्ष लाखों डॉलर का निवेश करते और विश्व विख्यात विशेषज्ञों की सेवाएं लेते हैं। वे आप और आपकी जानकारी को सुरक्षित रखने पर और साइबर अपराधियों से एक कदम आगे रहने पर अपना ध्यान लगाते हैं।

पहचान की चोरी, व्यक्तिगत धोखाधड़ी और ऑनलाइन घोटालों से आपको बचाने में सहायता करने के लिए; आपके कंप्यूटर की सुरक्षा के लिए; और इंटरनेट को अधिक सुरक्षित जगह बनाने के लिए गूगल कठोर परिश्रम करता है। हम आपको ऐसे टूल और जानकारी देते हैं, जिनकी स्वयं अपने आप को और अपने परिवार को ऑनलाइन सुरक्षित रखने के लिए आवश्यकता है। और आपकी ओर से लड़ने के लिए हम लगातार निवेश और सुधार कर रहे हैं।

हम पहचान की चोरी का मुकाबला करने में सहायता प्रदान कर रहे हैं।

गूगल आपको ऑनलाइन पहचान की चोरी से बचाने में सहायता के लिए और आपके गूगल खाते को सुरक्षित और निश्चिंत रखना सुनिश्चित करने के लिए कई प्रकार की टेक्नोलॉजी का उपयोग करता है।

दो–चरण सत्यापन

आपके गूगल खाते को और भी मजबूत स्तरों की सुरक्षा देने के लिए हम अपने उपयोगकर्ताओं को दो चरणों के सत्यापन की पेशकश करते हैं। इस टूल में गूगल खाते में साइन–इन करने के लिए न केवल पासवर्ड की बल्कि एक सत्यापन कोड की भी आवश्यकता होती है, जिससे यह सुरक्षा की एक अतिरिक्त परत जोड़ देता है। दो–चरण सत्यापन में आपसे केवल आपके फोन पर भेजा गया एक कोड डलवा कर गूगल यह सुनिश्चित करता है कि यह आप ही हैं – बहुत ही कम संभावना होती है कि कोई दूर बैठा आक्रमणकर्ता यह और आपका पासवर्ड दोनों हासिल कर सकेगा।

एनक्रिप्शन करना

गूगल आपकी व्यक्तिगत जानकारी को हमलावरों और ताकझांक करने वालों से सुरक्षित रखने के लिए कई कदम उठाता है। हम पूर्वनिश्चित या डिफॉल्ट से आपके कंप्यूटर और गूगल के बीच जीमेल कनेक्शन को एनक्रिप्ट कर देते हैं, जो आपकी गूगल गतिविधि को दूसरों की ताकझांक से सुरक्षित रखने में सहायता करता है। जब आपने गूगल ड्राइव और कई अन्य सेवाओं में साइन–इन किया होता है, तब भी हम इस सुरक्षा को, जिसे सत्र–वार एसएसएल एनक्रिप्शन के रूप में जाना जाता है, पूर्वनिश्चित या डिफॉल्ट बना देते हैं।

हम आपके कंप्यूटर और उपकरण को स्वच्छ रखने में सहायता करने के लिए काम कर रहे हैं।

आप मॉलवेयर (कंप्यूटर को बिगाड़ने के लिए बनाए गए सॉफ्टवेयर) से अपने कंप्यूटर की रक्षा करने में स्वयं अपनी सहायता सकते हैं, किंतु गूगल भी आपकी रक्षा करने में सहायता के लिए मेहनत से जुटा हुआ है। हमारे पास सैकड़ों सुरक्षा विशेषज्ञ हैं जो आपके डाटा और उपकरणों की सुरक्षा सुनिश्चित करने में सहायता के लिए चौबीसों घंटे काम कर रहे हैं।

मॉलवेयर से बचने में सहायता

गूगल जिस प्रकार आपके प्रश्नों के सर्वश्रेष्ठ उत्तरों वाली साइटों के लिए वेब की खोज या सर्च करता है, ठीक उसी प्रकार हम उन साइटों की भी तलाश में रहते हैं जो उपयोगकर्ताओं के लिए हानिकारक या मॉलवेयर से युक्त प्रतीत होती हैं। हम प्रति दिन 10,000 से अधिक ऐसी असुरक्षित साइटों की पहचान करते हैं और हम अत्यधिक बड़ी संख्या में 1.4 करोड़ गूगल खोज परिणामों तथा 3,00,000 डाउनलोड के साथ चेतावनियां दिखाते हैं, जो हमारे उपयोगकर्ताओं को बताती हैं कि एक वेबसाइट विशेष या लिंक के पीछे कुछ संदिग्ध चल रहा हो सकता है।

आपके मोबाइल उपकरण को सुरक्षित रखने में सहायता

गूगल के एंड्रॉइड सॉफ्टवेयर पर चलने वाले स्मार्टफोन में भी नुकसान के जोखिम को कम करने के लिए मिलते–जुलते सुरक्षा उपाय लगे हैं। एंड्रॉइड में भी गूगल प्ले स्टोर के प्रत्येक ऐप के लिए यह बताना आवश्यक है कि वह आपके उपकरण से किस प्रकार की जानकारी तक पहुंचना या संग्रह करना चाहता है, जिससे आप निर्णय कर सकते हैं कि आप उस ऐप पर विश्वास करते हैं या नहीं। हम हानिकारक ऐप्स को रोकने या हटाने के लिए गूगल प्ले की बारीकी से स्वचालित जांच भी करते हैं। कुछ एंड्रॉइड फोनों के लिए हमारी गूगल एप्लीकेशन सत्यापन सेवा संभावित हानिकारक एप्लीकेशंस की जांच करेगी, फिर चाहे आपने उन्हें कहीं से भी लगाया गया हो।

हम इंटरनेट को हरेक के लिए और अधिक सुरक्षित बना रहे हैं।

उपयोगकर्ता की रक्षा करना साझा जिम्मेदारी है। हम सब तब अधिक सकुशल होते हैं जब हरेक व्यक्ति सबसे अच्छी सुरक्षा टेक्नोलॉजी और तकनीकियों का उपयोग करता है।

विशेषज्ञता और उपकरण साझा करना

आप भले ही आप किन्हीं भी सेवाओं या उत्पादों का उपयोग कर रहे हों, किंतु चूंकि आपकी सुरक्षा हमारे लिए अत्यधिक महत्त्वपूर्ण है, इसलिए हमें जिन भी खराब वेबसाइटों और लिंक के बारे में पता चलता है, हम उनकी जानकारी अन्य कंपनियों के साथ साझा करते हैं, ताकि वे भी अपने उपयोगकर्ताओं की रक्षा में सहायता कर सकें। साथ मिलकर काम करने और एक दूसरे की सहायता करने से पूरा वेब कहीं अधिक सुरक्षित स्थल है।

उपयोगकर्ताओं और वेबसाइट मालिकों के साथ संचार करना

अपने उपयोगकर्ताओं और उनकी जानकारी की सुरक्षा के लिए काम करते हुए हमें कभी–कभी असामान्य तौर–तरीकों वाली गतिविधि का पता चलता है और हम उसकी जांच करते हैं। प्रति दिन हम ऐसी 10,000 से अधिक असुरक्षित साइटों की पहचान और उन्हें फ़्लैग करते हैं। हम हर दिन ऐसी हजारों वेबसाइटों के मालिकों को संदेश भी भेजते हैं जिनके बारे में हमें लगता है कि वे आक्रमण से क्षतिग्रस्त हुई हो सकती हैं, ताकि वे अपनी साइटों को स्वच्छ कर सकें।

सुरक्षा संगठनों के साथ भागीदारी करना

गूगल ऐसे अनेक संगठनों का हिस्सा है जो अपने उपयोगकर्ताओं के लिए सुरक्षा में सुधार लाने में कंपनियों की सहायता करने के लिए काम कर रही हैं। उदाहरण के लिए, हम स्टॉपबैडवेयर.कॉम की स्थापना में सहायक रहे हैं और उसके साथ भागीदार हैं, ताकि मॉलवेयर या अन्य खराब सॉफ्टवेयर से बिगड़ी हुई वेबसाइटों को बंद करके, उन्हें कम करके या उन्हें स्वच्छ करके वेब को अधिक सुरक्षित बना सकें।

स्टिकर!

साथ रखने के लिए 15 टिप ताकि आपको ऑनलाइन सुरक्षित और निश्चिंत रहने में सहायता मिल सके। अधिक सुरक्षा टिप के लिए देखें : www.google.com/safetycenter.

सहभागियों और अधिक संसाधनों के लिए
www.google.com/safetycenter पर जाएं।

Google

ऑनलाइन सुरक्षित रहने के बारे में अधिक जानकारी के लिए
www.google.com/safetycenter.