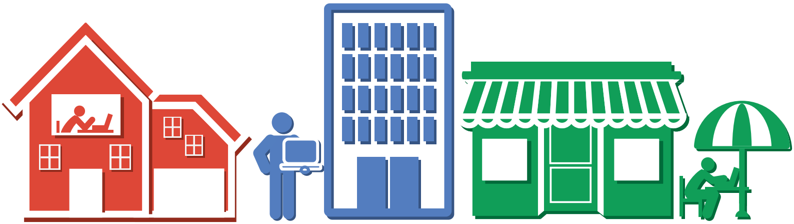
गुगल सेफ्टी सेंटर

ऑनलाईन सुरक्षीत आणि संरक्षीत रहाण्यासाठी मार्गदर्शन



ने बुकलेट कशाबद्दल आहे?

तुम्हाला, तुमच्या कुटूंबाला आणि तुमच्या मित्रांना इंटरनेटवर सुरक्षीत रहाण्यासाठी मदत करणे हा गुगल सेफ्टी सेंटरचा उद्देश आहे.

हे बुकलेट तुम्हाला लक्षात रहाण्यासारख्या व ज्या तुम्ही कृतीत आणु शकता अशा उपयुक्त टीप आणि हिंट्स देते. आम्ही यामध्ये सल्ला देणारे प्रमुख काही तुकड्यांचा समावेश केला आहे जेणेकरून तुम्ही ते मदतनीस आठवणींसाठी तुमच्या कंप्युटर किंवा नोटबूक मध्ये ठेवु शकता.

या बुकलेटमधील सर्व विषयांवरील सखोल माहितीसाठी आणि आणखी माहितीसाठी, सेफ्टी सेंटर संकेतस्थळाला www.google.com/safetycenter येथे भेट द्या.

मजकुर

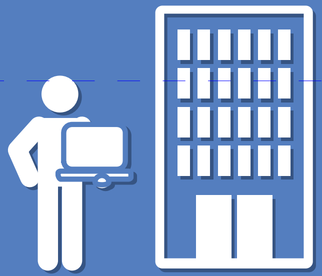
तुम्ही ऑनलाईन सुरक्षीत कसे राहु शकता p. 4

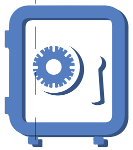
तुमच्या कुटूंबाला आवश्यक सुरक्षीत निवड तयार करा p. 9

गुगल तुम्हाला सुरक्षीत कसे ठेवतो p. 14

तुम्ही ऑनलाईन सुरक्षीत कसे राहु शकता

सुरक्षीत चालु करण्यासाठी बंद करा. इंटरनेट शोध, तयार करणे आणि एक सोबत कार्य करणे यांसाठी भरपुर संधी देतो. वेब वर जास्त काम करण्यासाठी, तुम्हाला स्वतःला सुरक्षीत कसे ठेवायचे याबद्दलचे ज्ञान असायला हवे. तुमच्याकडे जेव्हा नवीन इंटरनेट वापरकर्ता किंवा तज्ञ असतात, तेव्हा येथील सल्ला आणि उपकरणे तुम्हाला वेबवर सुरक्षीतपणे काम करण्यास मदत करू शकतात.





तुमचा पासवर्ड सुरक्षीत ठेवा.

पासवर्ड हा सायबर गुन्ह्यांविरूद्ध बचाव करण्याचा पहिला पर्याय आहे. बळकट पासवर्ड ठेवणे महत्वाचे असते जो तुमच्या प्रत्येक महत्वाच्या अकाऊंटसाठी वेगळा असावा, आणि नियमीतपणे पासवर्ड अद्ययावत करणे ही उत्तम सवय आहे. बळकट पासवर्ड तयार करणे आणि सुरक्षीत रहाणे यांसाठी खालील टिप्सचे पालन करा.

- **अक्षरे, अंक व सिम्बॉल एकत्रीत करा**
- **प्रत्येक संकेतस्थळासाठी वेगळा पासवर्ड वापरा.**

1. इमेल आणि ऑनलाईन बँकींग सारख्या तुमच्या महत्वाच्या अकाऊंटसाठी वेगळा पासवर्ड वापरावा.
2. अंक, अक्षरे आणि सिम्बॉल यांसह असलेला लांब पासवर्ड वापरा.
3. तुम्हाला तुमचा पासवर्ड रिसेट करायचा असल्यास तुमच्या रिकव्हरी इमेल ॲड्रेस वर तुम्हाला इमेल पाठविण्याची सुविधा भरपुर सर्व्हीस देतील, त्यामुळे तुमचा रिकव्हरी इमेल ॲड्रेस अद्ययावत असावा आणि तुम्ही सध्या वापरत असलेल्या अकाऊंट ला जोडलेला असावा याची निश्चीती करा.

केवळ तुम्हालाचा माहिती असावे या म्हणीचा विचार करावा ही एक कल्पना आहे, आणि तुम्हाला लक्षात रहावे यासाठी विशीष्ट संकेतस्थळासोबत त्याला जोडा. तुमच्या इमेल अकाऊंटसाठी, तुम्ही "माझा मित्र टॉम आणि जास्मीन मला दिवसातुन एकदा विनोदी इमेल पाठवतात" अशा प्रकारच्या म्हणीपासुन तुम्ही चालु करू शकता आणि नंतर त्याची पुन्हा रचना करण्यासाठी अंक आणि अक्षरे यांचा वापर करा. "MfT&Jsmafe1ad" हा भरपुर बदल असलेला पासवर्ड आहे. नंतर इतर साईट्स साठी ही प्रक्रिया पुन्हा करा.

ओळख चोर (आयडेंटिटी थेफ्ट) पासुन बचाव करा.

सामान्य योजना माहिती करून क्रिमीनल कर्मचारी तुम्हाला ऑनलाईन धोका आणि आयडेंटिटी थेफ्ट यांपासुन बचाव करण्यास मदत करेल. येथे काही सोप्या टिप्स आहेतः

- **वैयक्तीक माहितीसह शंकास्पद संदेश वाटल्यास त्याला प्रतिसाद देऊ नका.**

1. तुम्हाला शंकास्पद इमेल दिसल्यास, तुमच्या वैयक्तीक किंवा आर्थीक माहितीसाठी तात्काळ संदेश किंवा वेबपेज दिसल्यास त्याला रिप्लाय करू नका.
2. तुम्ही अशा इमेल किंवा चाट मध्ये आल्यास जीथे तुम्हाला विश्वास नाही तेथे तुमचा पासवर्ड टाकु नका.
3. इमेल द्वारे तुमचा पासवर्ड पाठवु नका, आणि इतरांना सुद्धा देऊ नका.

तुम्ही ओळखत असलेल्या एखाद्याकडुन तुम्हाला संदेश मिळाल्यास परंतु तो त्यांच्याकडुन आल्यासारखा वाटत नसल्यास, त्यांचे अकाऊंट सायबरक्रिमीनल मध्ये समाविष्ट आहे ज्यांना तुमच्याकडुन पैसा किंवा माहिती मिळवायचा आहे, तर त्यांना प्रतिसाद देतांना काळजी घ्या, किंवा त्या सर्वांना प्रतिसाद देऊ नका. सामान्य सूचनांमध्ये तुम्हाला त्यांना तात्काळ पैसा देण्याबद्दल विचारण्यात येईल, इतर देशांमध्ये प्रमाणीत असल्याचे किंवा त्यांचा फोन चोरी गेल्याचे सांगुन ते कॉल करू शकत नाहीत असे सांगतील. या संदेशामध्ये तुम्हाला हे सांगीतल्या जाईल की चित्रावर, आर्टीकलवर किंवा व्हिडीयोवर क्लीक करण्यास सांगीतले जाईल, ज्यावरून तुम्हाला एका साईटवर नेल्या जाते आणि तुमची माहिती चोरली जाते. तुम्ही क्लीक करण्याआधी विचार करा!

• शंकास्पद पोस्ट किंवा इमेल ला प्रतिसाद देऊ नका.

• स्कॅम्स टाळण्यासाठी ऑनलाईन व्यवहार संशोधन करा

• तो फार चांगला खरा असल्याचे भासवेल, बहुधा असेच असेलही

स्कॅम्स टाळा.

वेब हे महान ठिकाण असु शकते, परंतु ऑनलाईन असलेल्या प्रत्येकाचा हेतू चांगला नसतो. स्कॅमर्सला टाळण्यासाठी आणि वेबवर सुरक्षीत रहाण्यासाठी येथे तीन सोपे मार्ग आहेत :

1. जवळ भेटवस्तु बाळगणाऱ्यांपासुन सावध रहा. तुम्ही विजेते आहात असे तुम्हाला एखाद्याने सांगीतले आणि तुमच्या खाजगी माहितीसह एखादा अर्ज (फॅार्म) भरण्यास सांगीतला, तर लगेच तो भरण्यासाठी उत्साही होऊ नका. तुम्ही त्यांच्या अर्जामध्ये तुमची माहिती भरणे चालु केली आणि सबमिट बटनवर क्लिक केले नाही, तरिसुद्धा कदाचीत तुम्ही तुमची माहिती त्यांना पाठवत आहात असे होऊ शकते.

2. स्वतःचे संशोधन करा,तुम्ही ऑनलाईन खरेदी करतांना, स्थानीक दुकानातुन काही खरेदी केल्यापेक्षा एखाद्या वस्तुचे मूल्य संशयास्पदरित्या कमी आहे का याचा विचार करा. खरे दिसणारे ऑनलाईन व्यवहार बारकाईने तपासा. खोट्या किंवा फसव्या वस्तु घेऊन कोणालाही स्वतःची फसवणुक करुन घ्यायची नसते.

3. तुम्हाला शंका आल्यास, त्यासोबत सुरक्षीत व्यवहार करा. तुम्हाला जाहीरात किंवा ऑफर यांबद्दल वाईट विचार आले आहेत का? मनातील विचारावर विश्वास ठेवा! केवळ सुरक्षीत, दृष्टिगत केलेल्या आणि विश्वास असलेल्याच साईट्स वरुन खरेदी करा किंवा त्यांच्या जाहीरातींवर क्लिक करा.

• सार्वजनीक किंवा शेयर केलेल्या डिव्हाईसमधुन लॉग–आऊट करा

• आपोआप लॉक करण्यासाठी डिव्हाईसचे सेटींग करा

तुमची स्क्रीन किंवा डिव्हाईस लॉक करा.

तुम्ही कंप्युटर, लॅपटॉप किंवा फोनचा वापर करुन झाल्यावर तुमची स्क्रीन नेहमी लॉक करायला हवी. हा टप्पा फोन्स किंवा टॅबलेटसाठी फारच महत्वाचा आहे, जेथे बहुधा गैरवापर होऊ शकतो आणि तुम्हाला कोणी वापरु नये अशी वाटणारी माहिती लोक शोधु शकतात, तसेच घरच्या संगणकासाठी ते फारच महत्वाचे आहे. समाविष्ट केलेल्या सुरक्षेसाठी, झोपण्याआधी आपोआप लॉक करण्यासाठी तुमच्या डिव्हाईसमध्ये सेटींग करायला हवी.

• आपल्या घरी सुरक्षित एक WPA2 सह राऊटर पासवर्ड

सुरक्षीत नेटवर्कचा वापर करा.

तुम्हाला माहिती नाही किंवा तुमचा विश्वास नाही अशांचा वापर करुन ऑनलाईन असतांना जसेकी तुमच्या लोकल कॅफेवर मोफत वाय–फाय चा वापर न करता फार जास्त काळजी घ्या. सर्व्हीस प्रोव्हायडर त्यांच्या नेटवर्कवर सर्व ट्रॅफीकवर लक्ष ठेवतील, ज्यामध्ये वैयक्तीक माहितीचा समावेश असू शकतो.

जेव्हा तुम्ही सार्वजनीक वाय–फाय नेटवर्कच्या माध्यमातुन जोडल्या जाता, आसपासच्या जागेतील कोणीही तुमचे कनेक्शनकडे आणि वाय–फाय हॉटस्पॉट कडे लक्ष ठेवु शकतो. सार्वजनीक नेटवर्कवर बँकींग किंवा ऑनलाईन खरेदी अशासारख्या महत्वाच्या कृती करणे टाळा.

तुम्ही घरी वाय–फाय चा वापर करत असाल, तुमचे नेटवर्क सुरक्षीत करण्याची निश्चीती करा जेणेकरुन इतर लोक त्याचा वापर करु शकणार नाहीत. तुमच्या वाय–फाय नेटवर्कचा बचाव करण्यासाठी पासवर्ड सेट करा – आणि तुम्ही निवडलेल्या इतर पासवर्ड प्रमाणे, तुम्ही तो लांब असल्याची व त्यामध्ये संख्या, अक्षरे आणि सिम्बॉल असण्याची निश्चीती करावी जेणेकरुन इतर जण सहजतेने तुमचा पासवर्ड ओळखू शकणार नाही. बळकट बचावासाठी तुम्ही तुमचे नेटवर्क कॉन्फीगर करता तेव्हा WPA2 सेटींग निवडा.

अंतीमतः, तुम्ही तुमच्या रूटरला सुरक्षीत करण्यासाठी पासवर्डचा वापर करता याची निश्चीती करा. रूटर डिफॉल्ट पासवर्डचा वापर करण्याऐवजी ज्याची गुन्हेगाराला माहिती असू शकते रूटरसाठी तुमच्या इंटरनेट सर्व्हीस प्रोव्हायडर किंवा रूटरने ज्या सूचना दिल्या त्याचे केवळ पालन करा. गुन्हेगार तुमच्या रूटरचा वापर करु शकत असल्यास, ते तुमची सेटींग बदलु शकतात आणि

• गुगल अकाऊंटसाठी दोन–टप्प्यातील पडताळणी

• तुम्ही शेयर करण्याआधी सेटींग तपासा

तुमची गुगल सुरक्षीतता आणि गोपनियता उपकरणे जाणा.

गुगल सह, तुम्हाला विविध प्रकारची उपकरणे असतात जे तुम्हाला तुमची माहिती गोपनीय आणि सुरक्षीत ठेवण्यासाठी मदत करु शकतात. येथे आपल्या बहुतेक प्रसिद्ध उपकरणांबद्दल माहिती आहे ज्यामुळे गुगल तुमच्यासाठी उत्तम कार्य करु शकतो.

दोन–टप्प्यातील पडताळणी

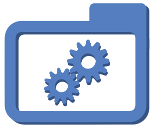
तुमच्या गुगल अकाऊंटची बळकट स्तरावर सुरक्षा ठेवण्यासाठी, आम्ही आमच्या वापरकर्त्यांना दोन–टप्प्यातील पडताळणीची सुविधा देतो. या उपकरणांमध्ये केवळ पासवर्डची आवश्यकता नसुन, विशेष स्तरावरील गुगल अकाऊंटमध्ये लॉग–इन करण्यास पडताळणी कोडची आवश्यकता असते. दोन–टप्प्यातील पडताळणीमुळे गुगल तुम्हाला एक कोड पाठवतो जो तुमच्या फोन मध्ये पाठवला जातो – फारच क्वचीत असे घडते की, अटॅकर ते दोन्ही व तुमचा पासवर्ड यांचा वापर करु शकतील.

गुगल अकाऊंट सेटींग

तुमच्या अकाऊंट सेटींग पेजवर, तुम्ही तुमच्या गुगल अकाऊंटसोबत संबंधित माहिती आणि सेवा बघु शकता आणि तुमची सुरक्षीतता आणि गोपनियता सेटींग बदलु शकता.

यु–ट्युब गोपनियता सेटींग

काहीवेळेला तुम्हाला एखादा छोटासा व्हिडीयो यु ट्युब सह तुमच्या मित्रांच्या लहान गटाला शेयर करायचा असतो किंवा तुमच्यासाठी ठेवायचा असतो. असे असल्यास, तुम्ही व्हिडीयो अपलोड करता तेव्हा तुमचा व्हिडीयो एकतर "अनलिस्टेड" (सर्च रिझल्टमधुन लपलेला, परंतु तुमच्यासोबत लिंक असलेल्या लोकांना दिसणारा) ठेवु शकता किंवा "प्रायव्हेट" (केवळ तुम्हालाच दिसणारा) असे ठेवु शकता.



तुमची गुगल सुरक्षीतता आणि गोपनियता उपकरणे जाणा.

तुमच्या गुगल अकाऊंटमध्ये साठवलेला डेटा हाताळा.

गुगल अकाऊंटमध्ये काय साठवले आहे ते गुगल डॅशबोर्ड दाखवतो व तुमच्या सध्याच्या अकाऊंट कृती सुद्धा पुरवतो. एका केंद्र ठिकाणामधुन, तुम्ही सहजतेने तुमचा डेटा आणि कृती बघु शकता आणि ब्लॉगर, गुगल कॅलेंडर, गुगल डॉक्स, गुगल प्लस आणि यापेक्षाही भरपुर काही सर्व्हीसचा तुम्ही वापर करू शकता.

तुमचे जाहीराती (ॲड्स) प्राधान्य ठरवा.

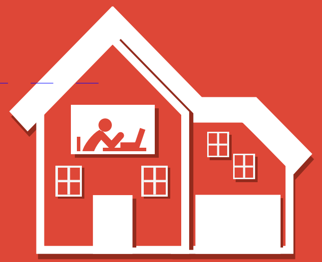
तुम्हाला आवडत असलेल्या व प्रत्येक दिवशी तुम्ही वापरत असलेल्या मोफत ऑनलाईन सर्व्हीसला निधी पुरवण्यामध्ये जाहीरातींची मदत होते. गुगल ॲड्स सेटींगसह, त्या जाहीराती तुमच्यासाठी कशा निवडल्या जातात त्याची तसेच तुमच्या माहितीवर नियंत्रण मिळवणे ज्याची जाहीराती निवडण्यास मदत होते तसेच विशीष्ट जाहीराती ब्लॉक करणे यांची माहिती समजुन घेऊ शकता.

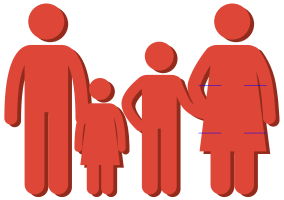
तुम्ही शेयर केलेले कोण बघु शकतो ते ठरवा.

गुगल प्लस सर्कल तुम्हाला तुमचे मित्र व संपर्क हाताळण्यास मदत करतात. तुम्ही तुमच्या मित्रांना एका सर्कलवर, तुमच्या कुटूंबाला दुसऱ्या सर्कलमध्ये आणि तुमच्या बॉसला वेगळ्य सर्कलमध्ये जसेकी तुम्ही वास्तव जीवनामध्ये करता तसेच ठेवू शकता. त्यानंतर तुम्ही निवडलेल्या योग्य लोकांना कोणत्याही वेळेत तुम्ही गुगल प्लस पोस्ट, युट्युब व्हिडीयो किंवा गुगल लोकल लिस्टींग जाहीराती शेयर करू शकतात.

तुमच्या कुटूंबाला आवश्यक अशा सुरक्षीत निवडी बनवा

पूर्वतयारी करा. पालक किंवा मार्गदर्शक म्हणुन, तुमच्या कुटूंबासाठी काय योग्य आहे किंवा तुमच्या मुलांनी योग्य ते कसे शिकावे हे तुम्हाला माहितीच आहे. बदलत्या ऑनलाईन जगतामधुन नवीन तंत्रज्ञान, गॅजेट आणि सर्व्हीस यांच्या माध्यमातुन जाण्यास तुमच्या कुटूंबाला मदत करण्यासाठी, तुम्हाला प्रात्याक्षीक सल्ल्याची आवश्यकता आहे. त्यामुळे काय कार्य केले जाते त्याकडे लक्ष ठेवण्यासाठी आम्ही सातत्याने जगभरातील सुरक्षा तज्ञ, पालक, शिक्षक आणि समाजातील व्यक्ती यांसोबत बोलत असतो. जबाबदार डिजीटल नागरीकांच्या समाजाला सांभळण्यासाठी आपण एकत्रीतपणे मदत करू शकतो.





कुटूंब सुरक्षेच्या मुलभूत बाबी

व्यस्त पालकांसाठी, तुमच्या कुटूंबाला सुरक्षीत ठेवण्यास मदत कशी करावी यासाठी काही तात्काळ सूचना आहे.

1 तुमच्या कुटूंबासोबत ऑनलाईन सुरक्षेबद्दल बोला.
तंत्रज्ञानाबद्दल तसेच अयोग्य वापराबद्दलची तुमची काळजी यांबद्दल तुमच्या कुटूंबाचे नियम व अपेक्षा यांबद्दल स्पष्ट रहा. आणि सर्वात महत्वाचे म्हणजे, कुटूंबातील सदस्यांना जेव्हा काहीतरी महत्वाचे व कठीण निर्णय घ्यायचे असतात तेव्हा त्यांनी तुमच्यासोबत मोकळेपणाने बोलावे व मार्गदर्शन घ्यावे अशासाठी त्यांना सोयीस्कर वाटु द्या. या चर्चेमुळे त्यांना स्वतः इंटरनेटवर संशोधन करतांना सुरक्षीत वाटु द्या, आणि त्यांना प्रश्न असल्यास त्यांनी कोणाला विचारावे हे त्यांना जाणुन घेऊ द्या.

2 एकत्रीतपणे तंत्रज्ञानाचा वापर करा.
ऑनलाईन सुरक्षा शिकणे हा उत्तम पर्याय आहे, आणि यामुळे तुमच्या कुटूंबासोबत ऑनलाईन सुरक्षा विषयाकडे लक्ष देण्यासाठी संधी निर्माण होते.

3 ऑनलाईन सर्व्हीस आणि साईट्स बद्दल चर्चा करा.
कुटूंब सदस्यांना कोणत्या प्रकारच्या साईट्सला भेट द्यायची आहे आणि प्रत्येक कुटूंब सदस्यासाठी योग्य काय त्याबद्दल बोला.

4 पासवर्ड सुरक्षीत ठेवा.
ऑनलाईन पासवर्ड सुरक्षीत कसा ठेवायचा याबद्दल तुमच्या कुटूंबाला शिकण्यासाठी मदत करा. पालकांसारख्या विश्वास असलेल्या लोकांव्यतिरीक्त इतर कोणाला अशा प्रकारचे पासवर्ड न देण्याची तुमच्या कुटूंब सदस्यांना आठवण द्या. त्यांनी शाळेमधील, कॅफे किंवा लायब्ररी मधील सार्वजनीक कंप्युटर्सवर ऑनलाईन अकाऊंट चालु केल्यास काम झाल्यावर साईन आऊट करण्याची निश्चीती करण्यास सांगा.

5 गोपनियता सेटींग आणि शेयरींग कंट्रोलचा वापर करा.
विचार, फोटो, व्हिडीयो, शेयर करणे तसेच स्टेटस अपडेट करणे व आणखीन भरपुर गोष्टींसाठी भरुपर साईट्स उपलब्ध आहेत. यांपैकी काही सर्व्हीस गोपनियता सेटींग आणि नियंत्रण देतात ज्यामुळे तुम्ही पोस्ट करण्यापुर्वी ती कोण बघु शकतो याचा निर्णय घेण्यास तुम्हाला मदत मिळते. कुटूंबाने सार्वजनीक रित्या ते शेयर करावे किंवा नाही करावे याबद्दल तुमच्या कुटूंब सदस्यांसोबत बोला. कुटूंब व मित्रांबद्दलची वैयक्तीक माहिती गोपनिय ठेवुन त्यांचा आदर करणे, आणि सार्वजनीक शेयर मजकुरामध्ये त्यांचे नाव न घेता त्यांना गोपनिय ठेवणे यांसाठी कुटूंब सदस्यांना मदत करा.

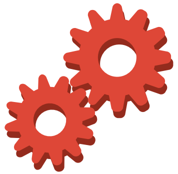
6 वयाची बंधने तपासा :
गुगल सह – भरुपर ऑनलाईन सर्व्हीसेस ला त्यांची सर्व्हीस कोणी वापरावी यासाठी वयाचे बंधन असते. उदा, गुगल अकाऊंट असण्यासाठी आणि गुगल उत्पादनांचा वापर करण्यासाठी तो वापरकर्ता 18 वर्ष किंवा त्यापेक्षा मोठा असावा लागतो. तुमच्या मुलांना अकाऊंट साईन अप करण्यापुर्वी त्या संकेतस्थळाच्या अटी तपासा, आणि कुटूंबाने कोणत्या साईट्स व सर्व्हीस वापरू शकतात याचे काही नियम घातले असतील तर त्याबद्दल सुद्धा मुलांना सांगा.

7 जबादारीने संभाषण करण्यासाठी तुमच्या कुटूंबाला शिकवा
येथे एक उत्तम नियम आहे : एखादी गोष्ट एखाद्याला दिसु नये असे वाटत असल्यास, ते एखाद्याच्या पेजवर लिहु नका, इमेल करू नका, तात्काळ संदेश पाठवु नका किंवा पोस्ट करू नका. तुम्ही ऑनलाईन काय म्हणता त्याबद्दल इतरांना काय वाटते त्याबद्दल बोला, आणि कोणत्या प्रकारचे संभाषण योग्य आहे याबद्दल कुटूंबाचे मार्गदर्शन घ्या.

8 इतर प्रौढ व्यक्ती आणि तज्ञ यांसोबत बोला.
तुमचे मित्र, विस्तारीत कुटूंब, शिक्षक, कोच आणि काऊंसेलर यांसोबत संभाषण खुले ठेवा. तुमच्या साठी अनोळखी असलेले तंत्रज्ञानासारखे क्षेत्र हाताळत असतांना तुमच्या कुटूंब सदस्यांसाठी काय योग्य आहे याचा निर्णय घेण्यासाठी इतर पालक आणि व्यावसायीक जे मुलांसोबत काम करतात त्यांची मदत घेणे सर्वात महान स्त्रोत ठरू शकतो.

9 तुमचा कंप्युटर आणि ओळख यांचा बचाव करा.
तुमच्याकडे क्रोमबुक असेपर्यंत अँटीव्हायरस सॉफ्टवेयरचा वापर करा व त्याला नियमीतपणे अपडेट ठेवा कारण त्याला अँटीव्हायरस ची आवश्यकता भासत नाही. ज्ंसा ूपजी लवनत उिपसल इवनज जीम जलचमे वि चमतेवदंस पदवितउंजपवदकृेनबी ‘ “वबपंस” मबनतपजल दनउइमतए चीवदम दनउइमत वत ‘िवउम ‘ककतमेकृजींज’िवनसक दवज इम चवेजमक वदसपदमण ज्मंबी लवनत उिपसल दवज जव ‘बबमचज पिसमे वत जव वचमद मउंपस ‘जजंबीउमदजे तिवउ नदादवूद चमवचसमण

10 चालुच ठेवा.
सुरक्षीत रहाणे ही एक वेळचीच गोष्ट नाही – ते तंत्रज्ञान आहे, आणि त्याची तुमच्या कुटूंबाची गरज असेल. तुम्ही येणाऱ्या डायलॉगवरच रहाण्याची निश्चीती करा. तुमच्या कुटूंबाच्या मुलभूत नियमांची पुनःस्थापना करा, प्रत्येकाची प्रगती तपासा आणि नियमीत अंतराने ते सेट करा. पालकांना चिंता वाटावी अशा आमच्या भागीदारांना लक्षात आलेल्या काही सामान्य समस्या खाली दिलेल्या आहेत.



वापरण्यास सोपे (इझी–टू–युज) सुरक्षा उपकरणांबद्दल शिका

तुमचे कुटूंब ऑनलाईन काय बघते यावर नियंत्रण करण्यास मदत करण्यासाठी गुगल सुरक्षा वैशिष्ट्यांचा शोध घ्या.

सर्चमधुन कुटूंबाला योग्य परिणाम प्राप्त करा.

गुगल सेफ सर्च सक्षम करुन, तुम्ही भरपुर असा विकसीत मजकुरांमधील काही मजकुर टाळु शकता ज्याला तुम्ही व तुमचे कुटूंब टाळत असते. योग्य परिणाम प्राप्त न झाल्यास, तुम्ही त्याबद्दल गुगल ला सांगु शकता. आम्ही नेहमी आमच्या कन्टेंट फिल्टरला सुधारण्यासाठी कार्य करतो, आणि याप्रकारचा आढावा आपल्याला प्रत्येकासाठी सुरक्षीत शोध करण्यास मदत करु शकतो.

अयोग्य मजकुर बाहेर काढण्यासाठी फिल्टर सेट करा.

तुम्ही यु–ट्युब ब्राऊज करतांना वयाची बंधने असलेले किंवा प्रौढांसाठीचे मजकुर न बघण्यास प्राधान्य देण्याचे ठरवले, तर कोणत्याही यु–ट्युब चा खालचा भाग स्क्रॉल करा आणि सेफ्टी मोड सक्षम करा. सेफ्टी मोड मुळे सर्च, संबंधीत व्हिडीयो, प्लेलीस्ट, शो आणि फिल्म्स यांमधील आक्षेपार्ह मजकुर फिल्टर करु शकता.

शेयर केलेल्या क्रोमबुक्सवरील वापरकर्त्यांवर लक्ष ठेवा.

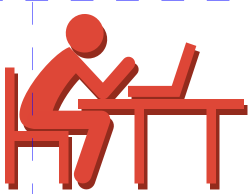
तुमच्या कुटूंबाच्या वेब कृतींवर लक्ष ठेवण्यास तुम्ही नेहमी तेथे असु शकत नाही. तुम्ही त्यांच्यासोबत खोलीमध्ये असु शकणार नाही अशा ठिकाणी, गुगल क्रोम हाच त्यांचा लक्ष ठेवणारा वापरकर्ता असतो. हे वैशिष्ट्य सक्षम असल्यास, तुम्ही वापरकर्ता काही विशीष्ट साईट्सला भेट देऊ शकतात, परवानगी देऊ शकतात किंवा ब्लॉक करु शकतात अशांचा आढावा घेणे या बाबी तुमचे कुटूंब सदस्य करु शकतात व तुम्ही त्याकडे लक्ष ठेवु शकता.

मान्यताप्राप्त ॲप्स आणि गेम्सच्या वापरावर मर्यादा.

तुमच्या सर्व स्टफ शेयर करण्याशिवाय तुमच्या टॅबलेटला शेयर करायचे आहे का? ॲंड्रॉईड व्हर्जन 4.3 आणि त्यापेक्षा जास्त व्हर्जनवर, तुम्ही तुमच्या टॅबलेट वर असलेल्या वैशिष्ट्ये आणि मजकुराच्या वापरावर मर्यादा घालु शकता.

वयानुसार योग्य ॲप्स निवडण्यासाठी ॲप रेटींग वापरा.

मुव्हीज प्रमाणे, रेटींग कडे बघता तुमच्या कुटूंबासाठी गुगल प्ले ॲप्स योग्य असल्याचे तुम्ही ठरवु शकता. कमी समज, मध्यम समज व जास्त समज असलेले सर्वजणांच्या स्तराप्रमाणे तुम्ही फिल्टरींग लेवल ठरवु शकता आणि साध्या पिन कोड (अपघाताने फिल्टर अक्षम झाल्यास इतर वापरकर्त्यांना ठेवणे) ने फिल्टरींग लेवल लॉक करु शकता.



तुमच्या कुटूंबाला त्यांची ऑनलाईन प्रतिष्ठा प्राप्त करण्यासाठी गुगल सुरक्षा उपकरणे शोधुन द्या.

अनावश्यक कमेंट किंवा टॅग थांबवा.

तुम्हाला एखाद्याची गुगल प्लस वरील पोस्ट बघायची नसल्यास, तुम्ही त्याचया प्रोफाईलवर जाऊन आणि रिपोर्ट/ब्लॉक (व्यक्तीचे नाव) निवडुन त्याला ब्लॉक करु शकता. तुम्ही विशीष्ट पोस्टला तुमच्या स्ट्रीममध्ये जास्त काळ बघु शकणार नाही.

तुमच्या व्हिडीयोबद्दल चाटरवर नियंत्रण मिळवा.

तुमच्या यु–ट्युब चॅनलवर कमेंटमध्ये बदल करणे सोपे आहे. तुम्ही एखाद्या व्यक्तीकडुन किंवा तुम्ही त्यांचा अभ्यास करण्यापुर्वी काही किवर्ड सह कमेंट हटवण्याचे निवडू शकता.

गुन्हेगार यु ट्युब वापरकर्त्यांना ब्लॉक करा.

तुम्हाला एखाद्याची व्हिडीयो किंवा चॅनल वरील कमेंट आवडली नाही, तर तुम्ही त्याला यु ट्युब वर ब्लॉक करु शकता. ते बराच काळापर्यंत तुमच्या स्टफवर कमेंट करु शकणार नाहीत किंवा तुम्हाला खाजगी संदेश पाठवु शकणार नाहीत.

तुमच्या डिव्हाईसवर नजर ठेवा.

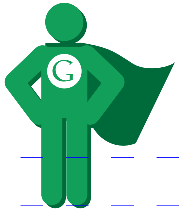
तुमचे अकाऊंट सुरक्षीत ठेवण्यासाठी तुमची स्क्रीन लॉक करणे हे केवळ महत्वाचे काम नसुन,सभोवतालचे लोक तुमचा फोन स्नूप करण्याचा प्रयत्न करत असल्यास त्यांना तसे करु न देणे सुद्धा महत्वाचे आहे. तुम्ही तुमचा फोन किंवा टॅबलेट वरील स्क्रीन लॉक करण्यासाठी पिन, पासवर्ड किंवा पॅटर्न निवडू शकता.

गुन्हेगारी मजकुराचा रिपोर्ट करा.

गुगल प्लस, यु ट्युब, किंवा ब्लॉगरवर एखाद्याने अयोग्य कमेंट टाकल्यास तुम्ही त्याचा रिपोर्ट करु शकता. गुगल ला स्पष्ट अशी कन्टेंट धोरणे आहेत जी साईट्स वर काय करणे योग्य आहे किंवा नाही याची माहिती देतात, त्यामुळे तुम्हाला आमच्या धोरणांचे उल्लंघन करत असलेल्या कमेंट आढळल्यास, तुम्ही त्याच्या पडताळणीसाठी त्याची आमच्याकडे नोंद करु शकता. आम्ही चोवीस तासांत त्याचा अभ्यास करतो, आणि तो मजकुर काढुन टाकु शकतो तसेच ज्यांनी धोरणांचे उल्लंघन केले त्यांच्या अकाऊंटवर मर्यादा घालु शकतो किंवा शट डाऊन करु शकतो.

गुगल तुमच्या बचावासाठी कशी मदत करतो

इंटरनेट ही फार महान गोष्ट आहे. परंतु ऑफलाईन जगताप्रमाणेच, ऑनलाईन असलेल्या प्रत्येकाचा हेतू चांगलाच असतो असे नाही. गुगल तुमच्या खाजगीपणा व सुरक्षीतता यांचा फार गंभीरतेने विचार करते. आम्ही प्रत्येक वर्षी दशलक्ष रूपयांची गुंतवणुक करतो आणि तुमच्या माहितीला गोपनीय ठेवण्यासाठी जगातील तज्ञ व्यक्तींची नेमणुक करतो. ते तुमच्या माहितीला सुरक्षीत आणि संरक्षीत ठेवण्यावर भर देतात, आणि तुम्हाला सायबर गुन्हेगारांपासुन एक पाऊल लांबच ठेवतात.
गुगल तुम्हाला आयडेंटिटी थेफ्ट, खाजगी धोखा आणि ऑनलाईन स्कॅम्स यांपासुन बचाव करण्यास मदत करण्यासाठी मेहनत करतो, जेणेकरून तुमच्या कंप्युटरचे रक्षण होण्यास मदत होते, आणि इंटरनेटला सुरक्षीत ठिकाण बनवल्या जाऊ शकते. तुम्ही स्वतःला आणि तुमच्या कुटूंबाला ऑनलाईन सुरक्षीत ठेवण्यासाठी आम्ही तुम्हाला काही उपकरणे आणि ज्ञान देतो. आणि आम्ही सातत्याने तुमच्या वतीने लढत देण्यासाठी गुंतवणुक करत आहोत आणि सुधारणा करत आहोत.



आम्ही आयडेंटिटी थेफ्ट विरूद्ध लढा देण्यास मदत करतो.

तुम्हाला आयडेंटिटी थेफ्टपासुन सुरक्षीत ठेवण्यासाठी आणि तुमचे गुगल अकाऊंट सुरक्षीत व संरक्षीत ठेवण्याची निश्चीती करण्यासाठी गुगल विविध प्रकारच्या तंत्रज्ञानांचा वापर करतो.

दोन टप्प्यातील पडताळणी

तुमच्या गुगल अकाऊंटची बळकट स्तरावर सुरक्षा ठेवण्यासाठी, आम्ही आमच्या वापरकर्त्यांना दोन–टप्प्यातील पडताळणीची सुविधा देतो. या उपकरणांमध्ये केवळ पासवर्डची आवश्यकता नसुन, विशेष स्तरावरील गुगल अकाऊंटमध्ये लॉग–इन करण्यास पडताळणी कोडची आवश्यकता असते.
दोन–टप्प्यातील पडताळणीमुळे गुगल तुम्हाला एक कोड पाठवतो जो तुमच्या फोन मध्ये पाठवला जातो – फारच क्वचीत असे घडते की, अटॅकर ते दोन्ही व तुमचा पासवर्ड यांचा वापर करू शकतील.

इन्क्रीप्शन

तुमची वैयक्तीक माहिती अटॅकर आणि स्नूप कडुन सुरक्षीत ठेवणे यांसाठी गुगल भरपुर पाऊले उचलतो. डिफॉल्ट पद्धतीने, आम्ही तुमचा कंप्युटर व गुगल यांमध्ये जीमेल कनेक्शन इन्क्रीप्ट करतो, ज्यामुळे इतरांकडुन स्नूप केली जाणारी तुमची गुगल कृती सुरक्षीत केली जाऊ शकते. आम्ही आणखीन एक संरक्षण करतो ज्याला सेशन–वाईड एसएसएल इन्क्रीप्शन म्हणतात, जे तुम्ही गुगल ड्राईव्ह आणि इतर सर्व्हीसमध्ये साईन इन केल्यावर डिफॉल्ट असते.

आम्ही तुमचा कंप्युटर आणि डिव्हाईस स्वच्छ ठेवण्यास मदत करण्यासाठी काम करतो.

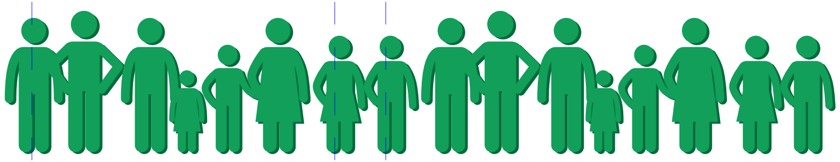
तुम्ही मालवेयर पासुन तुमच्या कंप्युटरला सुरक्षीत करू शकता, परंतु तुम्हाला सुरक्षीत ठेवण्यामध्ये गुगल सुद्धा फार मेहनत घेतो. तुमची माहिती आणि डिव्हाईस सुरक्षीत ठेवण्यासाठी आमच्याकडे चोवीस तास कार्य करणारे शेकडो सुरक्षा तज्ञ आहेत.

मालवेयर टाळण्यासाठी तुम्हाला मदत करत आहे

गुगल सर्च प्रमाणे, तुमच्या प्रश्नांची उत्तरे देण्यासह साईट्ससाठीच्या वेव सोबतच, आम्ही अशा साईट्स शोधतो ज्या वापरकर्त्यांसाठी धोकादायक नाहीत किंवा त्यामध्ये मालवेयर नाही. प्रत्येक दिवशी आम्ही अशा असुरक्षीत साईट्सच्या 10,000 पेक्षा जास्त साईट्स शोधतो, आणि आम्ही 14 दशलक्ष गुगल सर्च परिणाम आणि 300,000 डाऊनलोडमध्ये अशाप्रकारच्या सूचना दाखवलेल्या आहेत, आमच्या वापरकर्त्यांना सांगतो आहे की, अशा विशीष्ट संकेतस्थळ किंवा लिंक मागे काहीतरी शंकास्पद असू शकते.

तुमचा मोबाईल डिव्हाईस सुरक्षीत ठेवण्यास तुम्हाला मदत करत आहे

गुगल अँड्रॉईड सॉफ्टवेयर चालवत असलेल्या स्मार्टफोन्स ला धोका कमी करण्यासाठी सारखीच जागा असते. अँड्रॉईडला ला हे सुद्धा आवश्यक असते की, गुगल प्ले स्टोअरमधील प्रत्येक ॲपला तुमच्या डिव्हाईसमध्ये वापर करण्यासाठी कोणत्या प्रकारची माहिती आवश्यक असते, जेणेकरून तुम्ही त्या ॲपवर विश्वास ठेवता किंवा नाही ते कळते. आपण हानीकारक ॲप्स ब्लॉक करणे किंवा काढण्यासाठी आपोआप गुगल प्ले स्कॅन करू शकतो. काही अँड्रॉईड फोनसाठी तुम्ही कोठेही इन्स्टॉल केलेले असले तरिसुद्धा, आमची गुगल अप्लीकेशन सर्व्हीस हानीकारक अप्लीकेशनसाठी तपास करेल.



आम्ही प्रत्येकासाठी इंटरनेट सुरक्षीत बनवत आहोत.

वापरकर्त्यांना सुरक्षीत करणे ही सर्वांची जबाबदारी आहे. प्रत्येकजण उत्तम सुरक्षीत तंत्रज्ञान व तंत्रांचा वापर करेल तेव्हा ते उत्तम ठरते.

निपुणता आणि टुल्स शेयर करणे

तुमची सुरक्षीतता आमच्यासाठी महत्वाची असल्यामुळे तुम्ही कोणती सर्व्हीस किंवा उत्पादन वापरत आहात हे आमच्यासाठी महत्वाचे नसुन, आम्ही इतर कंपनीसोबत सापडलेल्या वाईट साईट्स आणि लिंक बद्दल माहितीची देवाण–घेवाण करतो, जेणेकरून ते त्यांच्या वापरकर्त्यांना सुद्धा मदत करू शकतात. एकत्रीतपणे काम करून व एकमेकांना मदत करून, संपुर्ण वेब जास्त सुरक्षीत रहाते.

वापरकर्ते आणि संकेतस्थळ मालक यांसोबत संभाषण करणे

आम्ही आमचे वापरकर्ते व त्यांची माहिती यांना सुरक्षीत करण्यासाठी काम करत असल्यामुळे, आम्ही काहीवेळेला कृतींचे असामान्य पॅटर्न शोधतो व संशोधन करतो. प्रत्येक दिवशी आम्ही अशा 10,000 असुरक्षीत साईट्सचा शोध लावतो. आम्ही दररोज अशा हजारो संकेतस्थळ मालकांना संदेश पाठवतो ज्यांच्या संकेतस्थळांना हल्ला होण्यापासुन धोका असतो, ज्यामुळे ते त्यांच्या साईट्स स्वच्छ करू शकतात.

सुरक्षीत संघटनांसोबत भागीदारी करणे

गुगल हा असंख्य संघटनांचा एक भाग आहे जो कंपन्यांना त्यांच्या वापरकर्त्यांना सुरक्षीत ठेवण्यास मदत करतो. उदा, आम्ही मालवेयर किंवा इतर वाईट सॉफ्टवेयर यांचा समावेश असलेल्या संकेतस्थळाला स्वच्छ करणे, थांबवणे व त्याची गंभीरता कमी करणे यांद्वारे वेब सुरक्षीत करण्यासाठी StopBadware.org सोबत भागीदारी केलेली आहे व त्यांना मदत केली आहे.

स्टीकर्स!

तुम्हाला ऑनलाईन सुरक्षीत व संरक्षीत रहाण्यासाठी मदत करत असलेल्या 15 टीप्स. अधिक सुरक्षा टीप्स साठी, भेट द्या www.google.com/safetycenter.

तुम्ही शेयर करण्याआधी विचार करा

सुरक्षीत ब्राऊजरचा वापर करा.

थांबा आणि

तुमच्या माहितीचा ऑनलाईन बॅकअप घ्या

अयोग्य मजकुराची दखल घ्या

संवेदनशील माहिती इमेल ने पाठवु नका

बळकट पासवर्डचा वापर करा

तुमची इमेल सेटींग माहिती करून घ्या. दुर्लक्ष करू नका.

सार्वजनीक व शेयर केलेल्या कंप्युटरवर लॉग आऊट करा.

तुमच्या डिव्हाईसला रिमोट वाईप कसे करायचे ते शिका.

ऑनलाईन सूचना!

तुमचे रूटर सुरक्षीत करा

शंकास्पद संदेशाला रिप्लाय करू नका.

विश्वसनीय स्त्रोतांकडुनच सॉफ्टवेयर इंस्टॉल करा.

तुमचे अकाऊंट सुरक्षीत ठेवा. 2–टप्प्यातील पडताळणी करा.

भागीदार बनण्यासाठी व अधिक माहितीसाठी, भेट द्या www.google.com/safetycenter.

ऑनलाईन सुरक्षीत कसे रहावे याबद्दल अधिक माहिती जाणुन घेण्यासाठी, भेट द्या
www.google.com/safetycenter.

© 2014 Google Inc. All rights reserved, Google, the Google logo, Android, Blogger, Chromebook, Gmail, Google Calendar, Google Chrome, Google Dashboard, Google Docs, Google Drive, Google Local Listing Ads, Google Play, Google SafeSearch, Google+ and YouTube are trademarks or registered trademarks of Google Inc.
All other company and product names may be trademarks of the respective companies with which they are associated.