अपने डिवाइस (मोबाईल उपकरणों) को सुरक्षित करना

यह संसाधन डिवाइस ट्रैकिंग के सामान्य प्रकारों के विरुद्ध उपकरणों को सुरक्षित करने के लिए कुछ व्यावहारिक प्रथम चरण प्रदान करता है और इसमें कुछ ऐसी कार्रवाइयाँ शामिल हैं ब्लूटूथ, WiFi (वाईफाई) और स्थान साझाकरण बंद करना; अपने उपकरण का नाम बदलना; स्पाइवेयर और ऐप अनुमतियों की जाँच करना; और एक फ़ैक्टरी रीसेट करना।

यह आपके उपकरणों को सुरक्षित रखने के लिए सामान्य युक्तियाँ हैं। अलग उपकरणों के लिए विशेष चरण भिन्न हो सकते हैं और समय के साथ बदल सकते हैं।

iPhones और iPads पर, आप आमतौर पर होम स्क्रीन पर "सेटिंग" टैप कर के, और फिर सर्च बार दिखाने के लिए नीचे की ओर स्वाइप करके एक सेटिंग ढूंढ सकते हैं। (सहायता के लिए, http://tiny.cc/iphonesearch.) देखें।)

android

Android उपकरणों पर, होम स्क्रीन से ऊपर की ओर स्वाइप करें: एक सर्च बार दिखाई देगा जिसमें लिखा होगा "अपना फोन खोजें और अधिक"। खोज बार में वह सेटिंग टाइप करें जिसे आप ढूंढ रहे हैं।

जब आप ब्लूटूथ और WiFi का उपयोग न कर रहे हों तो उन्हें बंद कर दें।

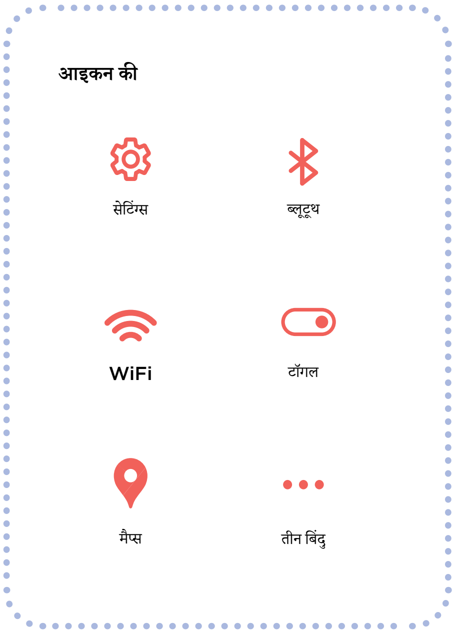
ब्लूटूथ और WiFi आपके उपकरण को अन्य उपकरणों के लिए दृश्यमान बना देते हैं। जब आप उनका उपयोग न कर रहे हों, तो सेटिंग में जाकर या ब्लूटूथ और wifi आइकन पर टैप करके उन्हें बंद करें।

आप अपनी ब्लूटूथ सेटिंग (सेटिंग > ब्लूटूथ) पर भी जा सकते हैं और अपने फोन के साथ जुड़े किसी भी उपकरणों को देख सकते हैं। यदि कोई ऐसा हो जिसे आप न पहचानें, तो उन्हें अलग कर दें।

स्थान साझाकरण बंद करें

यदि आपका फ़ोन बंद हो, तो भी स्थान साझाकरण और "फाइंड माई फ़ोन" जैसे ऐप काम करते रहते हैं, इसलिए आपको उन्हें सेटिंग में बंद करना होगा। iPhone पर, सेटिंग > गोपनीयता > स्थान सेवाएँ को खोलें, या "स्थान सेवाएँ" खोजें, और स्थान साझाकरण को बंद करें।

Android उपकरण पर, मैप्स खोलें, अपनी प्रोफ़ाइल तस्वीर पर और फिर स्थान साझाकरण पर टैप करें। जिस किसी व्यक्ति को आपका स्थान नहीं दिखाई देना चाहिए, उनकी प्रोफ़ाइल तस्वीर पर टैप करें और फिर “बंद करो” पर टैप करें।



©2023 MediaSmarts

अपने उपकरणों का नाम बदलें

भले ही आपने अपने फ़ोन का नाम कभी नहीं बदला हो, उसका तब भी एक नाम होता है जो उसकी पहचान करता है। iPhone पर, सेटिंग्स > सामान्य > अबाउट > नाम पर टैप करें, या "नाम" खोजें, और फिर एक नया नाम प्रविष्ट करें और "हो गया" पर टैप करें।

Android उपकरण पर, सेटिंग > फोन के बारे में -> उपकरण नाम पर टैप करें, या "नाम" खोजें, और फिर नया नाम प्रविष्ट करें और "ठीक"पर टैप करें।

स्पाइवेयर के लिए जाँच करें

"स्पाइवेयर" का अर्थ है, ऐसे ऐप जो किसी अन्य व्यक्ति को आपके उपकरण की जासूसी करने का अवसर प्रदान करते हैं। जाँच करें कि क्या कोई ऐसे ऐप मौजूद हैं जिन्हें आप नहीं पहचानते। iPhone पर, होम स्क्रीन पर दाईं ओर स्वाइप करें जब तक आपको ऐप लाइब्रेरी न दिखाई दे।

स्क्रीन के शीर्ष पर स्थित खोज बॉक्स पर टैप करें, फिर ऐप की सूची में स्क्रॉल करते हुए ऐसे सभी ऐप हटा दें जिन्हें आप नहीं पहचानते हैं।

Android उपकरण पर, सेटिंग > ऐप एवं सूचनाएँ > सभी ऐप देखें पर जाएँ, या "ऐप" खोजें।

कुछ ऐसे ऐप भी हैं, जैसे *Certo* और *Incognito* जिनका आप उपयोग कर सकते हैं, जो आपके उपकरण का स्पाइवेयर के लिए स्कैन करेंगे, लेकिन आपको अवगत होना चाहिए कि यह संभावना हो सकती है कि आपके फोन पर स्पाइवेयर अभी भी हो सकता है।

ऐप अनुमतियों की जाँच करें

आप किसी भी ऐप को आपके स्थान जैसी बातें एकत्र करने या साझा करने से भी रोक सकते हैं। iPhone पर, प्रत्येक ऐप क्या साझा कर रहा है, यह देखने के लिए तीन बिन्दु > गोपनीयता एवं सुरक्षा > ऐप गोपनीयता रिपोर्ट पर टैप करें, या "गोपनीयता रिपोर्ट" खोजें। सेटिंग बदलने के लिए प्रत्येक ऐप पर टैप करें।

आइकन की

सेटिंग्स | तीन बिंदु | टॉगल

Android उपकरण पर, Play Store से *DuckDuckGo* ऐप को डाउनलोड करें और फिर उसे खोलें। सेटिंग > ऐप ट्रैकिंग संरक्षण पर टैप करें और फिर टॉगल को दाईं ओर सरकाएँ।

फ़ैक्टरी रीसेट

यदि आपने बाकी सारी चीजें कर चुके हैं और आपको तब भी लगता है कि कोई आपके फ़ोन को ट्रैक कर रहा है, तो आप फ़ैक्टरी रीसेट कर सकते हैं। हालाँकि, इससे आपके फोन पर मौजूद किसी भी सबूत सहित सभी डेटा हटा दिया जाएगा। यदि आप अपना फ़ोन रीसेट करते हैं, तो आप सहेजे गए बैकअप से पुनर्स्थापित नहीं कर सकते हैं क्योंकि जो कुछ भी आपको ट्रैक कर रहा था वह दोबारा लोड हो सकता है: आपको पूरी तरह नए तौर पर आरंभ करना होगा।

यदि आप सुनिश्चित हैं कि आप ऐसा करना चाहते हैं, तो iPhone पर, आप सेटिंग्स > सामान्य > iPhone स्थानांतरित या रीसेट करें पर, और फिर सभी सामग्री और सेटिंग्स मिटाएँ पर टैप कर सकते हैं। इस सेटिंग को ढूंढने के लिए आप "रीसेट" भी खोज सकते हैं।

यदि आपके पास iPhone है तो आप लॉकडाउन मोड को भी चालू कर सकते हैं, जो अधिकांश प्रकार के स्पाइवेयर से आपका बचाव कर सकता है। ऐसा करने से यह भी सीमित हो जाता है कि आप FaceTime और Safari जैसे ऐप्स का कितना उपयोग कर सकते हैं। लॉकडाउन मोड के बारे में अधिक जानकारी के लिए https://support.apple.com/en-ca/HT212650 पर जाएँ।

Android उपकरण पर, पहले सेटिंग्स पर जाएँ और फिर "रीसेट" खोजें। "फ़ैक्टरी रीसेट" या "सभी डेटा मिटाएं" जैसे जैसे परिणाम खोजें और उस पर टैप करें।

MediaSmarts

Financial contribution from

Public Health Agency of Canada | Agence de la santé publique du Canada

सुरक्षित रूप से संचार करना

यह संसाधन ऑनलाइन ट्रैकिंग के सामान्य रूपों से बचने के लिए सुरक्षित रूप से ऑनलाइन संचार करने के लिए कुछ व्यावहारिक प्रथम चरण प्रदान करता है और ऐसी प्रक्रियाओं के बारे में बताता है जैसे खातों से साइन आउट करना, स्थान साझाकरण बंद करना, गोपनीयता सेटिंग्स की समीक्षा करना, और पासवर्ड बदलना।

यह आपके उपकरणों को सुरक्षित रखने के लिए सामान्य युक्तियाँ हैं। अलग उपकरणों के लिए विशेष चरण भिन्न हो सकते हैं और समय के साथ बदल सकते हैं।

iPhones और iPads पर, आप आमतौर पर होम स्क्रीन पर "सेटिंग" टैप कर के, और फिर सर्च बार दिखाने के लिए नीचे की ओर स्वाइप करके एक सेटिंग ढूंढ सकते हैं। (सहायता के लिए, http://tiny.cc/iphonesearch.) देखें।)

android

Android उपकरणों पर, होम स्क्रीन से ऊपर की ओर स्वाइप करें: एक सर्च बार दिखाई देगा जिसमें लिखा होगा "अपना फोन खोजें और अधिक"। खोज बार में वह सेटिंग टाइप करें जिसे आप ढूंढ रहे हैं।

सभी खातों से साइन आउट करना

कुछ ऐप के मामले में आप एक से अधिक उपकरण पर साइन इन हो सकते हैं। *Facebook* पर सभी जगह साइन आउट ऐसे किया जाता है: तीन बिंदु पर टैप करें और फिर सेटिंग, फिर "पासवर्ड एवं सुरक्षा" और फिर "अकाउंट सेंटर" पर। "पासवर्ड एवं सुरक्षा" पर टैप करें और फिर "आप कहाँ लॉग इन हैं" पर टैप करें।

अब आपको अपने सभी *Facebook*, *Instagram* या *WhatsApp* खाते दिखाई देंगे। आप किन उपकरणों में लॉग इन हो, यह देखने के लिए प्रत्येक पर टैप करें, और फिर उन सभी के लिए "लॉग आउट" पर टैप करें जो आपका फ़ोन नहीं है।

©2023 MediaSmarts

सोशल मीडिया में स्थान साझाकरण बंद करें

यह महत्वपूर्ण है यदि आप *Snapchat* का उपयोग करते हैं, जोकि दर्शाता है कि आप मैप पर कहाँ हैं। ऐसा करने के लिए, *Snapchat* खोलें और अपने प्रोफ़ाइल आइकन पर टैप करें। इसके बाद ऊपर दाईं ओर तीन लंबवत बिंदु पर टैप करें और स्क्रॉल करते हुए नीचे “कौन कर सकता है...” अनुभाग पर जाएँ। यदि आप "मेरा स्थान देखें" पर टैप करते हैं तो एक पॉप-अप दिखाई देगा जिसमें लिखा होगा "घोस्ट मोड"। इसको को “चालू” पर टॉगल करें।

Facebook या *Instagram* पर, आप सेटिंग > गोपनीयता > लोकेशन सर्विसेज पर टैप करके और फिर उसके निकट टॉगल पर टैप करके स्थान को बंद कर सकते हैं। अधिकांश अन्य सोशल नेटवर्क इसे “गोपनीयता” या “सुरक्षा” जैसी सेटिंग के भीतर इस प्रकार के स्थानों पर रखते हैं।

गोपनीयता सेटिंग्स की समीक्षा करें

आपके सभी सोशल नेटवर्क खातों में गोपनीयता सेटिंग होते हैं, जिन्हें आप आमतौर पर सेटिंग्स और फिर "गोपनीयता," "गोपनीयता एवं सुरक्षा" या "दर्शक" जैसे कुछ सेटिंग टैप करके पहुँच सकते हैं। यह सुनिश्चित करें कि यह केवल वही दिखाने के लिए सेट किया हुआ है जो आप मित्रों पर पोस्ट करते हैं।

क्लाउड स्टोरेज पर पासवर्ड बदलें

यदि आप अपनी तस्वीरों या वीडियो के लिए *iCloud* या *Google Drive* जैसे किसी क्लाउड स्टोरेज का उपयोग करते हैं, तो सुनिश्चित करें कि आपने पासवर्ड बदल दिया है ताकि कोई अन्य व्यक्ति इस तक न पहुँच सके।

Financial contribution from
Public Health Agency of Canada
Agence de la santé publique du Canada

सुरक्षित रूप से ब्राउज़ करना

यह संसाधन ऑनलाइन ट्रैकिंग के सामान्य रूपों से बचने के लिए सुरक्षित रूप से ऑनलाइन ब्राउज़ करने के लिए कुछ व्यावहारिक प्रथम चरण प्रदान करता है, और गोपनीयता-केंद्रित ब्राउज़रों का उपयोग करने, निजी/गुप्त ब्राउज़िंग, इतिहास साफ़ करना, और गुमनाम ईमेल और मजबूत पासवर्ड के साथ साइन इन करने जैसी प्रक्रियाओं के बारे में बताता है।

यह आपके उपकरणों को सुरक्षित रखने के लिए सामान्य युक्तियाँ हैं।
अलग उपकरणों के लिए विशेष चरण भिन्न हो सकते हैं और समय के साथ बदल सकते हैं।

iPhones और iPads पर, आप आमतौर पर होम स्क्रीन पर "सेटिंग" टैप कर के, और फिर सर्च बार दिखाने के लिए नीचे की ओर स्वाइप करके एक सेटिंग ढूंढ सकते हैं। (सहायता के लिए, http://tiny.cc/iphonesearch.) देखें।)

Android उपकरणों पर, होम स्क्रीन से ऊपर की ओर स्वाइप करें: एक सर्च बार दिखाई देगा जिसमें लिखा होगा "अपना फोन खोजें और अधिक"। खोज बार में वह सेटिंग टाइप करें जिसे आप ढूंढ रहे हैं।

ऐसे ब्राउज़र का उपयोग करें जो गोपनीयता को महत्वता देते हैं।

Firefox और *DuckDuckGo* जैसे ब्राउज़र गोपनीयता को ध्यान में रखकर डिज़ाइन किए गए हैं, इसलिए वे आपको कम-से-कम ट्रैक करते हैं। अपने उपकरण के साथ आए ब्राउज़र के स्थान पर उनमें से किसी एक को आज़माएँ।

निजी या गुमनाम ब्राउज़िंग

अधिकांश ब्राउज़रों में निजी या गुमनाम मोड होता है। यह मोड ब्राउज़र को आपके द्वारा देखी गई साइटों को रिकॉर्ड करने से रोकता है, परंतु यह उन साइटों (या आपके इंटरनेट प्रदाता, या आपके उपकरण पर अन्य ऐप) को रिकॉर्ड करने से नहीं रोकता है कि आप क्या कर रहे हैं।

आइकन की

निजी या गुमनाम मोड

सेटिंग्स

©2023 MediaSmarts

सुरक्षित रूप से ब्राउज़ करना

अपना इतिहास साफ़ करें

"इतिहास" खोजें। यदि आपका *Google* खाता है, तो आप अपना Google और *YouTube* इतिहास भी साफ़ कर सकते हैं। **myactivity.google.com** पर जाएँ और “वेब एवं ऐप गतिविधि”, “स्थान इतिहास” और “YouTube इतिहास” को बंद कर दें।

Safari पर अपना ब्राउज़र इतिहास साफ़ करने के लिए, सेटिंग्स पर टैप करें, फिर Safari > इतिहास और वेबसाइट डेटा साफ़ करें पर टैप करें, या "वेबसाइट डेटा" खोजें।

एक गुमनाम ईमेल से साइन इन करें

कई वेबसाइट और सेवाएँ साइन अप करने के लिए आपको एक ईमेल पता प्रदान करने की माँग करती हैं। यदि आपको सत्यापन लिंक पर क्लिक करने की आवश्यकता नहीं है, तो आप **Sharklasers.com** पर बनाए गए नकली ईमेल पता का उपयोग कर सकते हैं।

आप एक निःशुल्क, निजी और सुरक्षित *Protonmail* ईमेल पता भी बना सकते हैं, ताकि आपको किसी ऐसे पता का उपयोग न करना पड़े जिसे कोई और पहचान सके।

मजबूत पासवर्ड का उपयोग करें

आप एक यादगार वाक्यांश (जैसे "मुझे केले पसंद हैं") से आरंभ करके और फिर कुछ अक्षरों को संख्याओं या वर्णों (जैसे तारांकन या विस्मयादिबोधक चिह्न भी) इसे !L1keBan@nas बना सकते हैं।

परंतु अलग-अलग खातों के लिए एक ही पासवर्ड का उपयोग न करें। यह अत्यंत महत्वपूर्ण है कि अपने मुख्य ईमेल खाते के लिए एक अलग मजबूत पासवर्ड का उपयोग करें, क्योंकि खाता पुनर्प्राप्ति के ईमेल वहीं भेजे जाएँगे। आप *1Password* जैसे पासवर्ड मैनेजर का भी उपयोग कर सकते हैं। यदि आप ऐसा करते हैं, तो उह सुनिश्चित करें कि इसके लिए आप जिस पासवर्ड का उपयोग कर रहे हैं वह मजबूत है और आपके अन्य सभी पासवर्ड से अलग है।

आइकन की

निजी या गुमनाम मोड

सेटिंग्स

MediaSmarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada