اپنی ڈیوائسز کی حفاظت کرنا

یہ وسیلہ ڈیوائس ٹریکنگ کی عام قسموں کے خلاف ڈیوائس کو محفوظ بنانے کے لیے کچھ ابتدائی عملی اقدامات فراہم کرتا ہے اور اس میں ان اعمال کا احاطہ کیا گیا ہے جیسے کہ بلوٹوتھ، وائی فائی اور مقام شیئرنگ کو آف کرنا؛ اپنی ڈیوائس کا نام تبدیل کرنا؛ اسپائی ویئر اور ایپ کی اجازتوں کو چیک کرنا؛ اور فیکٹری ری سیٹ کرنا۔

یہ آپ کی ڈیوائس کو محفوظ رکھنے کے سلسلے میں عام تجاویز ہیں۔ مختلف ڈیوائسز کے لیے درست اقدامات مختلف ہوسکتے ہیں اور یہ وقت کے ساتھ بدل سکتے ہیں۔

آئی فونز اور آئی پیڈز پر، آپ عام طور پر ہوم اسکرین پر موجود "ترتیبات" پر ٹیپ کرکے ایک ترتیب تلاش کرسکتے ہیں، پھر تلاش کا بار دیکھنے کے لیے نیچے سوائپ کرسکتے ہیں۔ (مدد کے لیے، دیکھیں http://tiny.cc/iphonesearch۔)

اینڈرائڈ ڈیوائسز پر، ہوم اسکرین سے اوپر کی جانب سوائپ کریں: ایک تلاش والا بار ظاہر ہوگا جس میں یہ کہا گیا ہے "کہ اپنا فون اور بہت کچھ تلاش کریں"۔ تلاش والے بار میں وہ ترتیب ٹائپ کریں جسے آپ تلاش کر رہے ہیں۔

جب آپ بلوٹوتھ اور وائی فائی استعمال نہ کر رہے ہوں تو انہیں بند کردیں

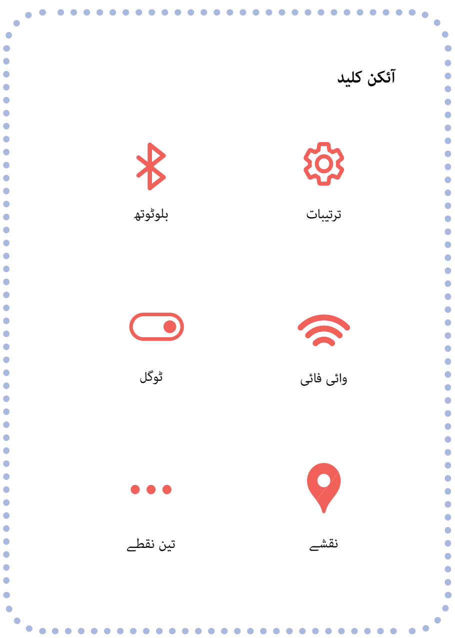
بلوٹوتھ اور وائی فائی آپ کی ڈیوائس کو دوسری ڈیوائسز کے لیے مرئی بناتا ہے۔ جب آپ انہیں استعمال نہ کر رہے ہوں تو، ترتیبات میں جا کر یا بلوٹوتھ اور وائی فائی آئیکنز پر ٹیپ کرکے انہیں بند کردیں۔

آپ اپنی بلوٹوتھ کی ترتیبات (ترتیبات > بلوٹوتھ) پر بھی جا سکتے ہیں اور اپنے فون کے ساتھ جڑی ہوئی کسی بھی ڈیوائسز کو تلاش کرسکتے ہیں۔ اگر کوئی ایسا ملتا ہے جسے آپ نہیں پہچان پاتے ہیں تو، ان کی جوڑی ہٹادیں۔

مقام شیئرنگ کو بند کریں

مقام شیئرنگ اور "میرا فون تلاش کریں" جیسی ایپس آپ کے فون کے بند ہونے پر بھی کام کرتی ہیں، لہذا آپ کو انہیں ترتیبات میں جاکر بند کرنا ہوگا۔ آئی فون پر، ترتیبات > رازداری > مقام کی سروسز کھولیں، یا "مقام کی سروسز" تلاش کریں اور مقام شیئرنگ کو بند کردیں۔

اینڈرائیڈ ڈیوائس پر، نقشے کھولیں، اپنی پروفائل کی تصویر پر اور پھر مقام شیئرنگ پر ٹیپ کریں۔ کسی بھی ایسے شخص کی پروفائل تصویر پر ٹیپ کریں جنہیں آپ کے مقام کو نہیں دیکھنا چاہیے اور پھر "روکیں" پر ٹیپ کریں۔



©2023 MediaSmarts

اپنی ڈیوائسز کی حفاظت کرنا

اپنی ڈیوائسز کا نام تبدیل کریں

خواہ آپ نے کبھی بھی اپنے فون کا نام تبدیل نہ کیا ہو، تب بھی ممکن ہے کہ کوئی اس کی شناخت کرلے۔ آئی فون پر، ترتیبات > عمومی > کے بارے میں > نام پر ٹیپ کریں، یا "نام" تلاش کریں، پھر نیا نام درج کریں اور "ہوگیا" پر ٹیپ کریں۔

اینڈرائیڈ ڈیوائس پر، ترتیبات > فون کے بارے میں > ڈیوائس کا نام پر ٹیپ کریں، یا "نام" تلاش کریں، پھر نیا نام داخل کریں اور "ٹھیک ہے" پر ٹیپ کریں۔

اسپائی ویئر کی جانچ کریں

"اسپائی ویئر" سے مراد ایسی ایپس ہیں جو کسی اور کو آپ کی ڈیوائس کی جاسوسی کرنے دیتی ہیں۔ یہ دیکھنے کے لیے چیک کریں کہ آیا ایسی کوئی ایپس ہیں جنہیں آپ نہ پہچانتے ہوں۔ آئی فون پر، اس وقت تک ہوم اسکرین پر دائیں جانب سوائپ کریں جب تک کہ آپ کو ایپ لائبریری نظر نہ آئے۔

اسکرین کے اوپری حصے میں تلاش والے باکس پر ٹیپ کریں، پھر ایپس کی فہرست میں اسکرول کریں اور ایسی کسی بھی چیز کو ہٹا دیں جسے آپ نہ پہچانتے ہوں۔

اینڈرائیڈ ڈیوائس پر، ترتیبات > ایپس اور نوٹیفیکشنز > تمام ایپس دیکھیں پر جائیں، یا "ایپس" تلاش کریں۔

Certo اور *Incognito* جیسی ایپس بھی ہیں جسے آپ استعمال کرسکتے ہیں جو آپ کی ڈیوائسز کو اسپائی ویئر کے لیے اسکین کرے گی، لیکن آپ کو معلوم ہونا چاہیے کہ ہمیشہ اس بات کا امکان رہتا ہے کہ اسپائی ویئر اب بھی آپ کے فون میں موجود ہوسکتا ہے۔

ایپ کی اجازتوں کو چیک کریں

آپ کسی بھی ایپ کو اپنے مقام جیسی چیزوں کو جمع کرنے یا اس کا اشتراک کرنے سے بھی روک سکتے ہیں۔ آئی فون پر، یہ دیکھنے کے لیے کہ ہر ایک ایپ کون سی چیز شیئر کررہی ہے، یا "رازداری کی رپورٹ" تلاش کرنے کے لیے تین نقطے > رازداری اور سیکیورٹی > ایپ کی رازداری کی رپورٹ پر ٹیپ کریں۔ ترتیبات کو تبدیل کرنے کے لیے ہر ایپ پر ٹیپ کریں۔

اینڈرائیڈ ڈیوائس پر، پلے اسٹور سے *DuckDuckGo* ایپ ڈاؤن لوڈ کریں اور پھر اسے کھولیں۔ ترتیبات > ایپ ٹریکنگ پروٹیکشن پر ٹیپ کریں اور پھر ٹوگل کو دائیں طرف سلائیڈ کریں۔

فیکٹری ری سیٹ کرنا

اگر آپ نے باقی سب کچھ کرلیا ہے اور پھر بھی لگتا ہے کہ کوئی آپ کے فون کو ٹریک کررہا ہے تو، آپ فیکٹری ری سیٹ کرسکتے ہیں۔ تاہم، یہ آپ کے فون پر موجود کسی بھی ثبوت سمیت تمام ڈیٹا کو حذف کردے گا ۔ اگر آپ اپنے فون کو ری سیٹ کرتے ہیں تو، آپ محفوظ شدہ بیک اپ سے اسے دوبارہ اسٹور نہیں کرسکتے ہیں کیونکہ جس بھی چیز کو ٹریک کیا جارہا تھا وہ واپس سے لوڈ ہو سکتا ہے: آپ کو اسے پھر سے شروع کرنا ہوگا۔

اگر آپ واقعی میں اسے آئی فون پر کرنا چاہتے ہیں تو، آپ ترتیبات > عمومی > منتقلی یا آئی فون ری سیٹ کریں پر ٹیپ کرسکتے ہیں، پھر تمام مواد اور ترتیبات کو مٹا سکتے ہیں۔ آپ اس ترتیب کو تلاش کرنے کے لیے "ری سیٹ" کو بھی تلاش کرسکتے ہیں۔

اگر آپ کے پاس آئی فون ہے تو آپ لاک ڈاؤن موڈ کو بھی آن کرسکتے ہیں، جو زیادہ تر قسموں کے اسپائی ویئر سے آپ کی حفاظت کرتا ہے۔ یہ اس چیز کو بھی محدود کرتا ہے کہ آپ فیس ٹائم اور سفاری جیسے ایپس کو کتنا استعمال کرسکتے ہیں۔ لاک ڈاؤن موڈ کے بارے میں مزید جاننے کے لیے https://support.apple.com/en-ca/HT212650 دیکھیں۔

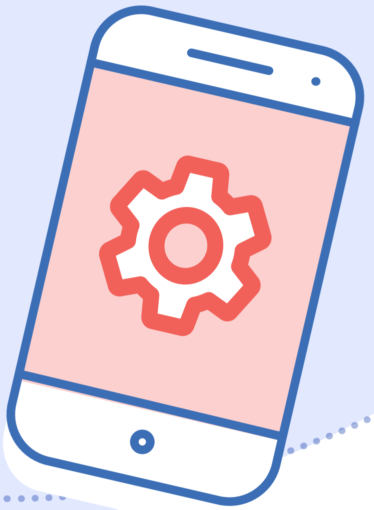
اینڈرائیڈ ڈیوائس پر، ترتیبات پر جا کر شروعات کریں، پھر "ری سیٹ" تلاش کریں۔ "فیکٹری ری سیٹ" یا "تمام ڈیٹا مٹا دیں" جیسے نتیجے تلاش کریں اور اس پر ٹیپ کریں۔

Financial contribution from

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

محفوظ طریقے سے مواصلات کرنا

یہ وسیلہ آن لائن ٹریکنگ کی عام قسموں سے بچنے کے لیے محفوظ طریقے سے آن لائن مواصلت کرنے کی خاطر کچھ ابتدائی عملی اقدامات فراہم کرتا ہے اور کارروائیوں کا احاطہ کرتا ہے جیسے کہ اکاؤنٹس سے سائن آؤٹ ہونا، مقام کے اشتراک کو بند کرنا، رازداری کی ترتیبات پر نظرثانی کرنا اور پاس ورڈ تبدیل کرنا۔



یہ آپ کی ڈیوائس کو محفوظ رکھنے کے سلسلے میں عام تجاویز ہیں۔ مختلف ڈیوائسز کے لیے درست اقدامات مختلف ہوسکتے ہیں اور یہ وقت کے ساتھ بدل سکتے ہیں۔

آئی فونز اور آئی پیڈز پر، آپ عام طور پر ہوم اسکرین پر موجود "ترتیبات" پر ٹیپ کرکے ایک ترتیب تلاش کرسکتے ہیں، پھر تلاش کا بار دیکھنے کے لیے نیچے سوائپ کرسکتے ہیں۔ (مدد کے لیے، دیکھیں http://tiny.cc/iphonesearch۔)

android

اینڈرائڈ ڈیوائسز پر، ہوم اسکرین سے اوپر کی جانب سوائپ کریں: ایک تلاش والا بار ظاہر ہوگا جس میں یہ کہا گیا ہے "کہ اپنا فون اور بہت کچھ تلاش کریں"۔ تلاش والے بار میں وہ ترتیب ٹائپ کریں جسے آپ تلاش کر رہے ہیں۔

تمام اکاؤنٹس سے سائن آؤٹ کریں

آپ ایک سے زیادہ ڈیوائسز پر کچھ ایپس میں سائن ان ہوسکتے ہیں۔ فیس بُک پر ہر جگہ سائن آؤٹ ہونے کا طریقہ یہ ہے: تین نقطے پر اور پھر ترتیبات پر، اس کے بعد "پاس ورڈ اور سیکیورٹی" اور پھر "اکاؤنٹس سینٹر" پر ٹیپ کریں۔ "پاس ورڈ اور سیکیورٹی" پر اور پھر "جہاں آپ لاگ ان ہیں" وہاں ٹیپ کریں۔

اب آپ کو اپنے تمام فیس بُک، انسٹاگرام یا واٹس ایپ اکاؤنٹس نظر آئیں گے۔ یہ دیکھنے کے لیے ہر ایک پر ٹیپ کریں کہ آپ کون سی ڈیوائسز میں لاگ ان ہیں اور پھر ہر ایک کے لیے "لاگ آؤٹ" پر ٹیپ کریں جو آپ کا فون نہیں ہے۔

سوشل میڈیا میں مقام شیئرنگ کو بند کردیں

اگر آپ اسنیپ چیٹ استعمال کرتے ہیں تو ایسا کرنا ضروری ہے، جو یہ دکھاتا ہے کہ نقشے پر آپ کہاں موجود ہیں۔ ایسا کرنے کے لیے، اسنیپ چیٹ کھولیں اور اپنے پروفائل آئیکن پر ٹیپ کریں۔ اس کے بعد اوپر دائیں جانب تین عمودی نقطے پر ٹیپ کریں اور نیچے "یہ کون کر سکتا ہے..." سیکشن پر اسکرول کریں۔ اگر آپ "میرا مقام دیکھیں" پر ٹیپ کرتے ہیں تو ایک پاپ اپ ظاہر ہوگا جس پر "گھوسٹ موڈ" نظر آتا ہے۔ اسے "آن" پر ٹوگل کریں۔

فیس بُک یا انسٹاگرام پر، آپ ترتیبات > رازداری > مقام کی سروسز پر ٹیپ کرکے مقام کو بند کرسکتے ہیں اور پھر اس کے پاس ٹوگل پر ٹیپ کرسکتے ہیں۔ زیادہ تر دوسرے سوشل نیٹ ورکس اسے "رازداری" یا "تحفظ" جیسی ترتیبات کے اندر اسی طرح کی جگہوں پر رکھتے ہیں۔

رازداری کی ترتیبات کا جائزہ لیں

آپ کے تمام سوشل نیٹ ورک اکاؤنٹس میں رازداری کی ترتیبات ہوتی ہیں، جن تک آپ عام طور پر ترتیبات پر ٹیپ کرکے اور پھر "رازداری،" "رازداری اور سیکیورٹی" یا "سامعین" جیسی کسی چیز پر ٹیپ کر کے رسائی حاصل کرتے ہیں۔ اس بات کو یقینی بنائیں کہ یہ صرف یہ دکھانے کے لیے تیار ہے کہ آپ دوستوں کو کیا پوسٹ کرتے ہیں۔

کلاؤڈ اسٹوریج پر پاس ورڈز تبدیل کریں

اگر آپ اپنی تصاویر یا ویڈیوز، جیسے کہ آئی کلاؤڈ یا گوگل ڈرائیو کے لیے کوئی کلاؤڈ اسٹوریج استعمال کرتے ہیں تو، یہ یقینی بنائیں کہ آپ نے پاس ورڈ تبدیل کردیا ہے تاکہ کوئی اور اس تک رسائی حاصل نہ کرسکے۔

آئکن کلید

- تین نقطے
- ترتیبات
- تین عمودی نقطے
- ٹوگل

Financial contribution from

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

Digital Smarts

محفوظ طریقے سے براؤز کرنا

یہ وسیلہ آن لائن ٹریکنگ کی عام قسموں سے بچنے کے لیے محفوظ طریقے سے آن لائن براؤزنگ کرنے کی خاطر کچھ ابتدائی عملی اقدامات فراہم کرتا ہے اور کارروائیوں کا احاطہ کرتا ہے جیسے کہ رازداری پر مرکوز براؤزرز کا استعمال کرنا، نجی/ نامعلوم حیثیت میں براؤزنگ، ہسٹری صاف کرنا اور گمنام ای میلز اور مضبوط پاس ورڈز کے ساتھ سائن ان کرنا۔

یہ آپ کی ڈیوائس کو محفوظ رکھنے کے سلسلے میں عام تجاویز ہیں۔

مختلف ڈیوائسز کے لیے درست اقدامات مختلف ہوسکتے ہیں اور یہ وقت کے ساتھ بدل سکتے ہیں۔

آئی فونز اور آئی پیڈز پر، آپ عام طور پر ہوم اسکرین پر موجود "ترتیبات" پر ٹیپ کرکے ایک ترتیب تلاش کرسکتے ہیں، پھر تلاش کا بار دیکھنے کے لیے نیچے سوائپ کرسکتے ہیں۔ (مدد کے لیے، دیکھیں http://tiny.cc/iphonesearch۔)

android

اینڈرائڈ ڈیوائسز پر، ہوم اسکرین سے اوپر کی جانب سوائپ کریں: ایک تلاش والا بار ظاہر ہوگا جس میں یہ کہا گیا ہے "کہ اپنا فون اور بہت کچھ تلاش کریں"۔ تلاش والے بار میں وہ ترتیب ٹائپ کریں جسے آپ تلاش کر رہے ہیں۔

رازداری پر مرتکز براؤزر استعمال کریں

فائر فاکس اور *DuckDuckGo* جیسے براؤزر کو رازداری کو ذہن میں رکھتے ہوئے تیار کیا گیا ہے، تاکہ وہ آپ کو جتنا ممکن ہو کم سے کم ٹریک کریں۔ اپنی ڈیوائس کے ساتھ آنے والے براؤزر کے بجائے ان میں سے کسی ایک کو استعمال کرنے کی کوشش کریں۔

نجی یا نامعلوم حیثیت میں براؤزنگ

زیادہ تر براؤزر میں نجی یا نامعلوم حیثیت والا موڈ ہوتا ہے۔ یہ موڈ براؤزر کو اسے خود سے ریکارڈ کرنے سے روکتا ہے کہ آپ کون سی سائٹس پر گئے ہیں، لیکن یہ ان سائٹوں (یا آپ کے انٹرنیٹ فراہم کنندہ، یا آپ کی ڈیوائس پر موجود دیگر ایپس) کو یہ ریکارڈ کرنے سے نہیں روکتا ہے کہ آپ کیا کرتے ہیں۔

آئکن کلید

ترتیبات

نجی یا گمنام موڈ

محفوظ طریقے سے براؤز کرنا

اپنی ہسٹری صاف کریں

"ہسٹری" تلاش کریں۔ اگر آپ کے پاس گوگل اکاؤنٹ ہے تو، آپ اپنی گوگل اور یوٹیوب کی ہسٹری بھی صاف کرسکتے ہیں۔ myactivity.google.com پر جائیں اور "ویب اور ایپ کی سرگرمی"، "مقام کی ہسٹری" اور "یوٹیوب کی ہسٹری" کو بند کردیں۔

سفاری پر اپنے براؤزر کی ہسٹری صاف کرنے کے لیے، ترتیبات پھر سفاری > ہسٹری اور ویب سائٹ کا ڈیٹا صاف کریں پر ٹیپ کریں، یا "ویب سائٹ" ڈیٹا تلاش کریں۔

گمنام ای میل کے ساتھ سائن ان کریں

بہت ساری ویب سائٹیں اور سروسز آپ سے سائن اپ کرنے کے لیے ای میل پتہ طلب کرتی ہیں۔ اگر آپ کو تصدیقی لنک پر کلک کرنے کی ضرورت نہیں ہے تو، آپ Sharklasers.com پر بنایا گیا جعلی ای میل پتہ استعمال کرسکتے ہیں۔

آپ ایک مفت، نجی اور محفوظ پروٹون میل پتہ بھی بنا سکتے ہیں تاکہ آپ کو ایسا پتہ استعمال نہ کرنا پڑے جسے کوئی اور پہچان سکتا ہو۔

مضبوط پاس ورڈز استعمال کریں

آپ کسی یادگار جملے (جیسے کہ "مجھے کیلے پسند ہیں") سے شروع کرکے اور پھر کچھ حروف کو نمبروں یا علامات میں تبدیل کرکے ایک مضبوط پاس ورڈ بنا سکتے ہیں (جیسے کہ ستارے یا فجائیہ نشانات تاکہ یہ L1keBan@nas! کی طرح بن سکے)۔

لیکن مختلف اکاؤنٹس کے لیے ایک ہی پاس ورڈ استعمال نہ کریں۔ اپنے مرکزی ای میل اکاؤنٹ کے لیے مختلف مضبوط پاس ورڈ استعمال کرنا خاص طور پر ضروری ہے، کیونکہ اکاؤنٹ کی بازیابی کے ای میلز وہاں بھیجے جائیں گے۔ آپ *1Password* جیسے پاس ورڈ مینیجر بھی استعمال کرسکتے ہیں۔ اگر آپ ایسا کرتے ہیں تو، اس بات کو یقینی بنائیں کہ آپ اس کے لیے جو پاس ورڈ استعمال کرتے ہیں وہ مضبوط اور آپ کے دیگر تمام پاس ورڈز سے مختلف ہوں۔

آئکن کلید

ترتیبات

نجی یا گمنام موڈ

Financial contribution from

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

MediaSmarts