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۔)

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۔

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۔

Financial contribution from

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