اپنی ورچوئل قیمتی انفارمیشن کی حفاظت کریں

آپ کو اپنی آن لائن معلومات کی حفاظت بالکل ویسے ھی کرنی چاھئیے جیسے آپ اپنے گھر میں قیمتی اشیا کی حفاظت کرتے ھیں۔ چاھے وہ آپ کے فنانشل ریکارڈز ھوں آپ کے پاسپورٹ کی سکین کاپی ھوں یا آپ کا ایڈریس اور فون نمبر ھو۔ آپ کو یہ ضرور سوچنا چاھیے کہ آپ اپنی قیمتی ذاتی معلومات کہاں سٹور کر رھے ھیں اور آپ اس کی کیسے حفاظت کر سکتے ھیں

اگر آپ جلدی جلدی کچھ بہتری لانا چاھتے ھیں تو کسی جگہ کافی پر بیٹھ کر، سپاٹ کلین، ایک بہترین خیال ھو سکتا ھے۔ کوئی خاص معلومات جو کہ آپ کی ای میل میں پڑی ھے جیسا کہ آپ کی آئی ڈی کی سکین کاپی، آپ کی بینک معلومات یا آپ کی ھیلتھ انشورنس کو تلاش کر کے ڈلیٹ کرنا ایک آغاز ھو سکتا ھے۔ اگر یہ ایسی معلومات ھیں جن کی آپ کو بعد میں بھی ضرورت پڑ سکتی ھے تو آپ ان کو ڈاؤن لوڈ کر کے اپنے پاس محفوظ کر سکتے ھیں یا آپ ان کے پرنٹ لے سکتے ھیں

ڈیپ کلین زیادہ جامع ھے اور سال میں ایک دفعہ کرنا اچھا ھے۔ آپ کے ای میل اور سوشل میڈیا اکاؤنٹس میں جو کچھ بھی پڑا ھے اسے اپنے کمپیوٹر میں ڈاؤن لوڈ کر لیں اور ایک نئے سٹارٹ کے لیے جو بھی کانٹنٹ آپ کے اکاؤنٹس میں پڑا ھے اسے ڈلیٹ کر دیں۔

صرف ڈلیٹ مت کریں بلکہ اپنے ٹریش اور عارضی فائلز کے فولڈرز کو بھی خالی کریں۔

معلومات آگے بڑھائیں

جب آپ اپنے اکاؤنٹس کو محفوظ بناتے ھیں اپنے پاس ورڈز کو مضبوط بناتے ھیں اور اپنے ڈیٹا کو صاف کرتے ھیں تو آپ کو تو فائدہ ھو گا لیکن وہ لوگ جو آپ کے ساتھ آن لائن رابطے میں ھوتے ھیں وہ بھی آپ کی وجہ سے تھوڑے محفوظ ھو جاتے ھیں۔

جب آپ اپنی ای میل اور سوشل میڈیا اکاؤنٹس کو صاف کر رھے ھوں تو یہ بھی سوچیں کہ ایسا کیا آپ اور صاف کر سکتے ھیں جس سے آپ کے دوستوں اور ساتھ کام کرنے والے ساتھیوں کی مدد ھوسکتی ھے۔ جیسا کہ اپنی بہن کے بینک اکاؤنٹس کی تفصیلات ، اپنے آفس کا کی کوڈ یا اپنے بیٹے کے پاسپورٹ کی سکین کاپی کچھ ایسے ریکارڈز ھو سکتے ھیں جو آپ کے لیے دردسر بنا سکتے ھیں اگر وہ کسی غلط بندے کے ھاتھ لگ جائیں۔

اسے آگے بڑھائیے۔اپنی ڈیجیٹل سیکورٹی بڑھانا آپ کے لیے بہت آسان ھے اور ایسا آپ کچھ سٹیپس اٹھا کے کر سکتے ھیں۔ اس ڈیٹا ڈیٹوکس باکس کو اپنے دوستوں، خاندان کے لوگوں سے ، اور ساتھ کام کرنے والوں کے ساتھ شیئر کریں اور ان کی مدد کریں ان کی عادات اس طرح بدلنے میں جس طرح ان کو ٹھیک لگے۔

کی مدد سے
Firefox

کا ایک پروجیکٹ
TACTICAL TECH

DATA DETOX KIT

اپنی سیٹنگز کو شفٹ کریں

اپنے ڈیٹا کو محفوظ بنانے کے لیے

اگر انٹرنیٹ صرف اسلئے ھوتا کہ یہاں ڈائناسور کاسٹیوم پہنے ھوئے کتوں کی تصویریں شیئر کی جائیں، تو پاس ورڈز کی کوئی ضرورت نہ ھوتی۔ لیکن انٹرنیٹ ایسی جگہ ھے جہاں آپ اپنے بل پے کرتے ھیں اور اپنا ووٹ رجسٹر کرواتے ھیں۔

تو جب آپ آن لائن اپنی قیمتی چیزوں کے متعلق سوچتے ھیں اور ان کو انٹرنیٹ پر شیئر کرتے ھیں اور انہیں اپنی ڈیوائیسز میں سٹور کرتے ھیں تو آپ ان کو اس طرح محفوظ کیوں نہیں بناتے جیسے آپ اپنی چابیوں یا بٹوے کو محفوظ بناتے ھیں؟

ایک آسان سا طریقہ ھے کہ آپ دوسروں کو آن لائن اپنی چیزوں تک نہ پہنچنے دیں اور وہ یہ ھے کہ آپ ان کو اپنا پاس ورڈ کا اندازہ نہ لگانے دیں۔ بہت سے لوگوں کو آپ کے اکاونٹس تک رسائی کے لیے کوئی زیادہ خاص مہارت کی ضرورت نہیں ھوتی وہ چند اندازے لگا کر آپ کے اکاونٹس تک پہنچ سکتے ھیں یا کوئی آٹومیٹڈ پروگرام اس کے لیے استعمال کر سکتے ھیں۔

اور جب وہ کسی ایک اکاونٹ تک رسائی حاصل کرلیتے ھیں تو وہ ان دوسرے اکاونٹس کے لیے بھی اس پاس ورڈ کو استعمال کر کے آپ اور آپ کی عادات کے متعلق معلومات حاصل کر سکتے ھیں یا آپ کے اکاونٹ کو اپنے قبضے میں لے سکتے ھیں یا آپ کی شناخت کو اپنے لیے استعمال کر سکتے ھیں۔

آپ جیسے اس ڈیٹا ڈیٹوکس کو فالو کریں گے تو آپ ایسے پریکٹیکل سٹیپس جان سکیں گے جو آپ کی آن لائن سیکورٹی میں اضافہ کریں گے۔

تو ائیے آغاز کرتے ھیں

datadetoxkit.org
#datadetox

1.

اپنے ڈیجیٹل دروازے کو بند کریں

اگر کوئی آپ کے فون میں گھسنے کی کوشش کر رہا ہو تو سکرین لاک، پاس ورڈز، پیٹرنز، فنگر پرنٹس یا فیس آئی ڈی اس کے خلاف آپ کے سب سے بہترین ڈیفینسز ہیں۔ ہو سکتا ہے کہ ان جیسی بہت سی اقسام موجود ہوں لیکن آپ کے لیے کون سا لاک ٹھیک ہے یہ جاننا بہت مشکل ہے۔

کسی بھی لاک کا ہونا لاک کے نہ ہونے سے بہت بہتر ہے۔ اور کچھ لاکس دوسرے لاکس سے بہت بہتر ہیں بلکل ایسے ہی جیسے آپ کے دروازے کے کچھ لاکس دوسروں سے بہتر ہوتے ہیں۔ اس وقت دستیاب تمام لاکس میں سے منفرد اور لمبے پاس ورڈز سب سے زیادہ طاقتور ہوتے ہیں۔ اس کا مطلب یہ ہے کہ اگر آپ اپنے فون کو پاس ورڈ سے کھولتے ہیں تو اس میں الفاظ، ہندسے، اور سپیشل کریکٹرز ہونے چاہیے

چلیں اگر آپ اپنے فون کو استعمال کرنے کے لیے سوائپ کے ذریعے ان لاک کرتے ہیں تو آہستہ آہستہ آپ اپنے موبائل کی سیکورٹی کو لمبے پاس ورڈ کے ذریعے بڑھا سکتے ہیں۔ یا اگر آپ پیٹرن لاک کا استعمال کرتے ہیں تو پیٹرن کو لمبا کرنا کیسا رہے گا۔ کیا آپ 1234 کو اپنے پن کے طور پر استعمال کرتے ہیں تو پاس ورڈ کو سات مختلف عدد تک کرنا اور یاد رکھنا کیسا رہے گا۔

ایک چھوٹی سی تبدیلی سے آپ اپنی ڈیوائس کا زیادہ کنٹرول حاصل کر سکتے ہیں۔.

2.

ٹھیک والے پاس ورڈ کا انتخاب کریں

ایک اچھا پاس ورڈ بنانا بہت آسان ہے ۔آپ کو صرف چند بنیادی اصول اختیار کرنے ہیں۔ ا پاس ورڈ کو:

لمبا ہونا چاہیے: آپ کا پاس ورڈ کم از کم آٹھ ہندسوں پر مشتمل ہونا چاہیے۔ اگر سولہ سے بیس ہندسوں پر مشتمل ہو تو اور اچھا ہے۔

منفرد ہو: آپ کا ہر سائٹ جو آپ استعمال کرتے ہیں ان کے لیے پاس ورڈ مختلف ہونا چاہیے

بے ترتیب: آپ کے پاس ورڈ کو آسا ن نہیں ہونا چاہیے جس کا آسانی سے اندازہ لگایا جا سکے۔ اس کی کوئی منطقی ترتیب نہیں ہونی چاہیے۔ یہاں پاس ورڈ مینجرز آپ کے بہت کام آسکتے ہیں

سب سے مضبوط پاس ورڈ حروف، نمبرز اور خصوصی علامات کا مجموعہ ہوتا ہے۔ اس وقت بھی نصیحت یہی ہے کہ آپ ایک مضبوط ایسا پاس ورڈ بنائیں جس کے متعلق اندازہ لگانا مشکل ہو۔ بدقسمتی سے کچھ پاس ورڈ سسٹم خصوصی علامات کے استعمال کی اجازت نہیں دیتے۔ لیکن پھر بھی حروف اور اعداد پر مشتمل پاس ورڈ چھوٹے پاس ورڈ سے بہت بہتر ہے۔

مثالی طور پر آپ کو اپنے پاس ورڈز کو بنانے اور سٹور کرنے کے لیے ، مخصوص پاس ورڈ مینجرز کا استعمال کرنا چاہیے۔ کچھ پاس ورڈ مینجرز ایپلیکیشنز کا بنیادی keePassXC اور Passwordجیسا کہ 1 مقصد آپ کے لاگ ان کی معلومات اور دوسرے حساس ڈیٹا کی حفاظت کرنا ہے۔

3.

ایک اور چابی کا اضافہ کریں

دو یا زیادہ عناصر پر مشتمل تصدیق کے مراحل کا مطلب ہے کہ اگر کسی کو آپ کا پاس ورڈ معلوم بھی ہو جائے تو ان کے پاس وہ اضافی معلومات نہیں ہوگی جس سے وہ لاگ ان کر سکیں۔

جو ویب سائٹس یا ایپلیکیشنز آپ استعمال کرتے ہیں ان کی سیکورٹی سیٹنگز کا جائزہ لیں کہ کیا آپ یہ اضافی سیکورٹی اختیار کر سکتے ہیں کہ نہیں۔ جو سب سے زیادہ اہم ہیں ان سے شروع کر لیں۔ کوئی بھی فنانس کے متعلق ایپلیکیشن یا کوئی سروسز جیسا کہ ای میل جسے آپ اپنے اکاؤنٹ کو ریکور کرنے کے لیے استعمال کرتے ہیں۔

DATA DETOX KIT

فیس بک:

menu ←
سیٹنگز ←
سیکورٹی اور لاگ ان ←
ٹو فیکٹر ایتھنٹیکیشن اختیار کریں

سائن ان کریں
myaccount.google.com ←
سیکورٹی←
سٹیپ ویریفکیشن 2 ←
شروع کریں

ٹپ: جب آپ سیکورٹی کے لیے تصدیق کی ایک اضافی پرت لگا رہے ہوں گے تو یہ تصدیق کرنے کے لیے کہ یہ آپ ہی ہیں ایک دوسرا طریقہ اختیار کرنا ہو گا۔ اپنے فون پر موصول ہونے والے ایس ایم ایس کے ذریعے اس تصدیقی عمل سے گریز کریں ہو سکتا ہے کہ آپ اپنا فون گم کر بیٹھیں۔ ۔ ای میل کے ذریعے تصدیق کرنا زیادہ قابل اعتماد طریقہ ہے۔