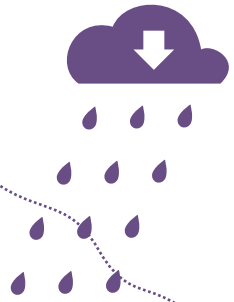
DATA DETOX KIT

اپنے سمارٹ فون کا ڈیٹا کنٹرول کریں

اپنی آنلائن پرائیویسی بڑھانے کے لیے



اگر آپ اس بارے میں سوچیں کہ آپکا ڈیٹا آپکے متعلق دوسروں کو کیا بتاتا ہے، تو شاید یہ کوئی اتنی اہم بات نہ لگے: کسی کو کیا پرواہ کہ آپ کنٹری میوزک کے شوقین ہیں، اپنی ضرورت سے زیادہ جوتے خریدنا پسند کرتے ہیں یا اگلی چھٹیوں کی منصوبہ بندی ایک سال پہلے ہی شروع کر دیتے ہیں؟

مسئلہ اس میں یہ ہے کہ آپکے ڈیٹا کے ساتھ ہو کیا رہا ہے۔ وقت کے ساتھ آپ کی جمع کردہ معلومات گیسا کہ آپکی عادات، نقل و حمل ، تعلقات، ترجیحات اور راز ان لوگوں پر افشاء کیے جاتے ہیں جو ان کو تجزیہ کرتے ہیں اور پھر ان سے منافع کماتے ہیں جیسا کہ بروکرز اور بزنس

جب آپ اس ڈیٹا ڈیٹوکس کو فالو کریں گے تو آپ کو پتا چلے گا کہ یہ سب کیسے ہو رہا ہے اور کیوں ہو رہا ہے۔ تو پھر آپ انٹرنیٹ پر اپنے ڈیٹا ٹریسسز کو کنٹرول کرنے کے لیے عملے اقدامات لینا شروع کر دیں گے۔

آئیے شروع کرتے ہیں۔

4.

اپنے نشانات کو کم کریں

آپکا فون براؤزر آپ کے متعلق بہت ساری معلومات جمع کرتا ہے۔ جیسا کہ آپ کی لوکیشن، آپ کیا تلاش کرتے ہیں یا آپ کون سی ویب سائٹ استعمال کرتے ہیں۔ اور ہو سکتا ہے کہ آپکی یہ انفارمیشن وہ کسی اور کو بھی دے دے۔ آپ کچھ تبدیلیاں کر کے بہت سی معلومات کا کنٹرول حاصل کر سکتے ہیں۔

فون، ٹیبلٹس اور کمپیوٹرز میں پہلے سے انسٹال کیے گئے ویب براؤزرز آتے ہیں جن کے لیے آپ کی پرائیویسی کی اتنی اہمیت نہیں ہوتی۔ اس کی بجائے آپ ایسے براؤزرز ڈاؤن لوڈ اور انسٹال کر سکتے ہیں جو آپ کی ویب ایکٹوٹی کو زیادہ پرائیویٹ رکھتے ہیں اور آپ کی ٹریکرز سے حفاظت کرتے ہیں۔

جاسوس اشتہارات اور نہ نظر آنے والے ٹریکرز سے بچنے کے لیے آپ یہ طریقہ اختیار کر سکتے ہیں, انسٹال uBlock Origin (کے لیے کروم، سفاری اور فائر فاکس) or Privacy Badger (کے لیے کروم، سفاری اور اوپرا کے لیے).

اور اپنی پرائیویسی کو بڑھانے کے لیے آپ کچھ ایکسٹراچیزیں بھی ڈاؤن لوڈ کر سکتے ہیں۔ یہ چھوٹے چھوٹے آسانی سے انسٹال ہونے والے پروگرامز ہوتے ہیں جو آپ کی آن لائن ایکٹوٹی کو زیادہ پرائیویٹ کرتے ہیں۔

یہ یقینی بنانے کے لیے کہ جہاں تک ہو سکے آپ کے ویب سائٹس کے ساتھ کنکشن HTTPS محفوظ ہے , انسٹال یہ ایک ایسی :Everywhere براؤزر ایکسٹنشن ہے جو کہ یہ یقینی بناتی ہے کہ کچھ اہم ویب سائٹس کے ساتھ آپ کی کمیونیکشن خفیہ اور محفوظ رہے۔ اگر آپ سفاری استعمال کر رہے ہیں اور آپکو یہ فیچر چاہیے تو آپ اپنے سرچ انجن کی ڈیفالٹ سیٹنگز کو نان گوگل پراڈکٹس جیسا کہ ڈک ڈک گو ہے اس پر سیٹ کر دیں یہ آپ کو خود بخود خفیہ کنیکشنز کی طرف لے جائے گا

5.

خود کو اور دوسروں کو ان ٹیگ کریں

کیا آپ نے کبھی اپنے کسی دوست کو تصویروں اور پوسٹس میں ٹیگ کر کے ان کا ڈیٹا بڑھانے میں حصہ ڈالا ہے؟

ان کا ڈیٹا لوڈ (اور اپنے ضمیر کا بوجھ) کم کرنے کے لیے ان کو جتنی تصویروں اور پوسٹس سے انٹیگ کر سکتے ہیں کریں

یہ چیز اپنے دوستوں ، خاندان اور ساتھی ورکرز کو بھی بتائیں کہ وہ ڈیٹا کے دوسروں کے ہاتھ لگنے سے کیسے روک سکتے ہیں۔ اگر ہم سب مل کر اپنے ڈیٹا ٹریسز کو کنٹرول کریں تو ہم ایک دوسرے کی ڈیٹا ڈیٹوکس کرنے میں مدد کر سکتے ہیں۔

کا ایک پروجیکٹ TACTICAL TECH

کی مدد سے Firefox

datadetoxkit.org
#datadetox

1.

اپنی ڈیوائس کا نام بدلیں

کسی نا کسی موقع پر آپ نے وائی فائی یا بلوٹوتھ کے لیے اپنے فون کو کوئی نام دیا ہوگا یا ہو سکتا ہے کہ فون سیٹ اپ کے دوران یہ نام خود بخود ہی بن گیا ہو

اس کا مطلب ہے کہ اس فون کا نام وائی فائی نیٹ ورک کے مالک یا اگر آپ کا بلوٹوتھ آن ہے تو اس ایریا میں اور جس کے بلوٹوتھ آن ہیں ان سب کو نظر آ رہا ہے

آپ جب کسی کیفے، ایسٹورانٹ یا ائرپورٹ پر جاتے ہیں تو اپنا نام نہیں پکارنا شروع کر دیتے آپ کے فون کعو بھی ایسا نہیں کرنا چاہیے۔

آپ اپنے فون کے نام کو کچھ ایسا رکھ سکتے ہیں جو آپ کی شخصیت کو بہت کم ظاہر کرتا ہو اور منفرد بھی ہو۔

آپ ایسا اس طرح کر سکتے ہیں

آئی فون

چینج آئی فون نیم ← سیٹنگز
جنرل ← اباؤٹ ←
چینج دی نیم

اینراءڈ

وائی فائی کا نام بدلیں ← سیٹنگز
وائی فائی ← menu ←
ایڈوانس / مور فیچرز ←
وائی فائی ڈائریکٹ ←
ری نیم ڈیوائس

چینج بلوٹوتھ نیم ← سیٹنگز
بلوٹوتھ ←
بلوٹوتھ آن کریں اگر بند ہے ←
ری نیم ڈیوائس ← menu ←
بلوٹوتھ بند کریں

2.

اپنی لوکیشن کے نشانات مٹائیں

ہو سکتا ہے آپ کو ایسا لگتا ہو کہ آپ کی لوکیشن کے متعلق ڈیٹا بے ترتیب سی معلومات ہیں لیکن اگر ان ساری معلومات کو اکٹھا دیکھا جائے تو یہ آپ کے متعلق بہت اہم معلومات کی آگاہی دے سکتی ہیں جیسا کہ آپ کی کیا عادتیں ہیں، آپ کہاں رہتے ہیں، کہاں کام کرتے ہیں اور کہاں اپنے دوستوں کے ساتھ جانا پسند کرتے ہیں۔ اسی لیے لوکیشن کے متعلق معلومات کے حاصل کرنے کے لیے کمپنیز اور ڈیٹا بروکرز بے چین رہتے ہیں۔

ہو سکتا ہے کہ یہ کہنا بہت نارمل ہو کہ میپ ایپلیکشن کو یہ رسائی ہے کہ جان سکے کہ آپ کہاں ہیں لیکن آپ شاید یہ دیکھ کر حیران ہو جائیں کہ آپ نے کتنی زیادہ ایپلی کیشنز کو اپنی لوکیشن جاننے کی اجازت دی ہوئی ہے

آپ ہر ایپلیکشن کی پرمیشنز میں جا کر لوکیشن سروسز کو بند کر سکتے ہیں۔ ایسی ایپلیکیشنز تلاش کریں جنہیں سروسز کی فراہمی کے لیے لوکیشنز جاننے کی ضرورت نہ ہو۔

:اینڈرواڈ

سیٹنگز←
ایپس←
ہر ایپلیکیشن کے حوالے سے اپنی لوکیشن سروسز کی ایکسس مینج کریں

:آئی فون

سیٹنگز←
پرائیویسی←
لوکیشن سروسز ←
ہر ایپلیکیشن کے حوالے سے اپنی لوکیشن سروسز کی ایکسس مینج کریں

:اینڈرونڈ

سیٹنگز←
ایپس←
اس ایپ کو سلیکٹ کریں جو آپ صاف کرنا چاہتے ہیں
ان انسٹال

آئی فون: کسی ایک ایپلیکیشن کو اس وقت دبائیں جب تک وہ لرزنا شروع نہ کر دے اور ہر ایپ کے اوپر والے لیفٹ کارنر میں کراس کا نشان ظاہر نہ ہو جائے ایپ کو ڈلیٹ کرنے کے لیے ایپ کے اوپر ظاہر ہونے والے کراس کے نشان کو دبائیں فون کو واپس نارمل کرنے کے لیے ہوم کا بٹن دبائیں

3.

اپنی ایپلیکیشنز کو صاف کریں

آپ کی سوشل میڈیا ایپس، گیمز اور موسم کے متعلق معلومات دینے والی ایپس آپکا ڈیٹا اکھٹا کرنے میں انٹرسٹڈ ہوتی ہیں اور وہ ہو سکتا ہے کہ آپکا بہت سا ڈیٹا اکٹھا بھی کر رہی ہوں ایسی بہت سی ایپلیکیشنز جو آپکے فون میں ہیں اور آپ نے ان کا کبھی استعمال کیا ان سے چھٹکارا پانا آپ کے لیے فائدہ مند ہو سکتا ہے۔

اس سارے عمل سے آپ اپنے فون میں کچھ جگہ بنا سکتے ہیں۔ آپ کا ڈیٹا استعمال کم ہو سکتا ہے۔ اور فون کی بیٹری لائف بڑھ سکتی ہے۔ اس سے فون کی اووراَل پرفارمنس بڑھتی ہے۔

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۔

DATA DETOX KIT

ڈیفالٹ سیٹنگز سے چھٹکارا حاصل کریں

اپنی ڈیجیٹل خیریت کو بڑھانے کے لیے

آپ یہ کیسے یقینی بنا سکتے ہیں کہ آپ کا کسی ڈیوائس پر گزارا گیا وقت واقعی ایک کوالٹی ٹائم ہے؟

آپ کا کسی ایپ یا ویب سائٹ کی طرف جھکاؤ آپ کا قصور نہیں ہے ۔ آپ یقین کریں یا نہ کریں آپ کی پسندیدہ ایپس اور ویب سائٹس ڈیزائن ہی اس طرح کی گئی ہیں کہ آپ مسلسل ان کا استعمال کرتے رہیں۔ ان کا ہر فیچر، رنگ اور ان میں استعمال کردہ آوازیں سب اس طرح استعمال کی جاتی ہیں کہ آپ اس ایپ یا ویب سائٹ سے جڑے رہیں اور واپس آتے رہیں۔

آپ اپنی آن لائن اور آف لائن زندگی میں ایک صحتمند توازن جاننا چاہتے ہیں؟ تو ڈیٹا ڈیٹوکس کا یہ والا حصہ اسی متعلق ہے۔ جہاں سے آپ کو ٹھیک لگے وہیں سے آغاز کریں اور پھر رفتہ رفتہ سلسلے کو آگے بڑھائیں۔ آئیے شروع کرتے ہیں۔

اپنی آواز پہنچائیں اور اسے یقینی بنائیں

ے امکانات بڑھ جاتے ہیں کہ وہ اپنے کام کو بدلیں۔اگر آپ ایسی ویب سائٹس یا ایپس کے عادی اور قائل کرنے والے ڈیزائنز یا مس انفارمیشن سے ناخوش ہیں جنہیں آپ استعمال کرتےہیں تو آپ انہیں ای میلز بھیج سکتے ہیں یا ان کے ٹویٹس لکھ سکتے ہیں اور انہیں بتا سکتےہیں آپ ان کے اس کام سے اتفاق نہیں کرتے۔ جب کمپنیوں پر ان کے سب سے قیمتی اثاثے یعنی ان کے گاہکوں کی طرف سے پریشر آتا ہے تو اس ک

اگر آپ کو محسوس ہوتا ہے کہ آپ کے فیڈبیک پر زیادہ توجہ نہیں دی جا رہی تو آپ ایک بہت پائیدار کام کر سکتے ہیں اور وہ یہ کہ آپ کوئی دوسری ویب سائٹ یا ایپلیکیشن استعمال کریں۔ اگر آپ نے کسی ویب سائٹ یا ایپلیکیشن جو کہ آپ استعمال کرتے ہیں کے متعلق بتایا ہے کہ آپان سے کسی وجہ سے ناخوش ہیں اور آپ اس کو استعما؛ کرنا چھوڑ دیں اور بہت سارے لوگ یہ کام کریں تو کوئی وجہ نہیں کہ وہ اس کو نوٹس نہ کریں

اس کو بھیلائیں

دوسرں تک پہنچائیں یہ ایک ایسی ٹپ ہے جو ہم بآسانی بھول جاتے ہیں لیکن اس کا بہت زیادہ اثر ہو سکتا ہے۔ اپنے دوستوں اور ساتھ کام کرنے والوں کو ان چیزوں کے متعلق بتائیں جو آپ نے نوٹس کی ہیں اور ان سے بھی درخواست کریں کہ وہ اس ڈیٹوکس کا حصہ بنیں

ہر کوئی فون کے ساتھ اپنی عادات کو ٹھیک رکھنے میں مشکل کا سامنا کرتا ہے۔ اہم یہ ہے کہ آپ ایسے طریقے ڈھونڈ سکیں جو آپ کو ٹھیک لگیں اور آپ کے لائف سٹائل کے مطابق بھی ہوں۔ آپ تجربات جاری رکھیں جب تک کہ آپ کو ایسا طریقہ نہ مل جائے جو آپ کے لیے ٹھیک ہو ۔ اس کے بعد اپنی عادات کو وقت کے ساتھ آنے والی تبدیلیوں کے ساتھ ہم آہنگ کریں۔ ایسا کوئی ایک سلوشن دستیاب نہیں ہے جو سب کے لیے ٹھیک ہو۔ اور آخر میں اپنی ٹیکنالوجی چوائسز کے متعلق دوسروں کو بتائیں۔ مثال کے طور پر آپ رات آٹھ بجے کے بعد ہر روز میسجز ایپس پر دستیاب نہیں ہوں گے کیونکہ آپ سکرین فری روٹین کا آغاز کر رہے ہیں۔ اپنی فیملی اور دوستوں کو بتائیں تا کہ وہ میسجز کی بجائے آپ کو کال کر سکیں۔ ڈائیلاگ کو جاری رکھیں اور سوالات پوچھتے رہیں اس طرح آپ ایک متوازن زندگی گزار سکتے ہیں جو کہ آپ کو سوٹ کرتی ہے۔

datadetoxkit.org
#datadetox

کی مدد سے Firefox

کا ایک پروجیکٹ TACTICAL TECH

1.

لمحے میں موجود رھیں

ہ ٹپ اس سے قدرے مشکل ھے جتنی یہ سنائی دیتی ھے۔ اس کے لیے آپ کو روزانہ پریکٹس چاھیے۔ یہ بالکل ایسے ھی ھے جیسے آپ کو اپنے دماغ کے کسی خلیے کو مضبوط بنانے کے لیے روزانہ پریکٹس کرنی پڑے۔ آپ جو ٹیکنالوجی استعمال کرتے ھیں اس کے ساتھ اپنے بنتے تعلق کو جاننا شروع کر سکتے ھیں۔

آپ اپنے فون کے ساتھ کتنا وقت گزارتے ھیں؟

اگر آپ جواب سے ناخوش ھیں تو ایسی سیٹنگز اور سٹریٹیجیز موجود ھیں جن کی مدد سے آپ ٹیک استعمال پر اپنا کنٹرول بڑھا سکتے ھیں۔

اگر آپ کا مقصد یہ ھے کہ آپ فیس بک، انسٹاگرام اور سنیپ چیٹ پر کم وقت گزارنا چاھتے ھیں تو ان ایپس کی سیٹنگز اور پرمیشنز میں تبدیلی آپ کی مدد کر سکتی ھے۔ کچھ ایپس جیسے کہ انسٹاگرام آپ کو آپشن دیتے ھیں جہاں ایپ آپ کو یاد دھانی کرواتی ھے کہ آپ اپنے روزانہ استعمال کا وقت پورا کر چکے ھیں۔

:انسٹاگرام
پروفائل←
menu ←
سیٹنگز ←اکاؤنٹ←
آپ کی ایکٹوٹی←
روزانہ کا ریمائنڈر لگائیں

اگر آپ کو لگتا ھے کہ آپ کے فون کی کی رنگ بیل یا فلیش آپ کی گفتگو میں خلل ڈال رھی ھے تو آپ اپنے فون کو عارضی طور پر سائلنٹ پر بھی لگا سکتے ھیں اور اس کی سکرین کو الٹا رکھ سکتے ھیں یا اپنی پتلون کی جیب میں رکھ سکتے ھیں جہاں وہ آپ کی نظروں سے دور ھو۔

2.

ڈیزائن ٹرکس پہچانیں

ڈارک پیٹرنز ایسے ڈیزائن ھوتے ھیں جو کہ انسانی نفسیات کا استعمال کرتے ھوئے انہیں کچھ کرنے پر اکسانے ، کچھ خریدنے یا یا ضرورت سے زیادہ ذاتی معلومات دینے پر اکساتے ھیں جتنی کہ وہ دینا چاھتے یا سوچتے ھیں۔ اس طرح کے ڈیزائن میں کچھ مخصوص رنگوں کا استعمال ، بٹنوں کی جگہ کا تعین ،غیر واضح عبارت، یا نامکمل معلومات کا استعمال ھوتا ھے۔ بعض اوقات یہ طریقے بالکل واضح ھوتے ھیں لیکن کچھ دفعہ ان کو پہچاننا مشکل ھوتا ھے۔ آپ نے ان میں کچھ طریقوں کو کسی سبسکرپشن یا آن لائن خریداری کے دوران نوٹس کیا ھوگا۔

آپ بہت سے ایسے کام کر سکتے ھیں جن کی مدد سے آپ ان ایپس سے آگے نکل سکتے ھیں۔

یہ جانیں کہ کب آپ کو کسی جانب مائل کیا جا رھا ھے۔ سب سے پہلا کام یہ ھے کہ آپ کو ان طریقوں کا پتا ھو جن کی مدد سے یہ کام کیا جاتا ھے۔ ان مختلف طریقوں کے متعلق پڑھیں اور ان کو اختیار کریں

سکرین شاٹس لیں اور شیئر کریں جب بھی آپ کو کوئی ایسا قائل کرنے والا ڈیزائن نظر آئے تو اس کا سکرین شاٹ لیکر اپنے دوستوں کے ساتھ شیئر کریں۔ اس میں سے ذاتی قسم کی معلومات خارج کر دیں۔ آپ کمپنیز کو بھی کہہ سکتے ھیں کہ وہ اپنی اس طرح کے طریقے بدلیں۔

پرسکون رھیں اگر کسی پرچیز پیج پر کوئی کاؤنٹ ڈاؤن کلاک چل رھا ھے تو خود سے یہ ضرور پوچھیں کہ کیا یہ اتنا ھی ارجنٹ ھے۔ اگر آپ کسی کلک بٹن پر خود کو کلک کرتا پاتے ھیں جبکہ آپ ایسا کرنا بھی نہیں چاھتے تو اس کلک بٹن کے الفاظ یا اس سروس کے رنگوں پر غور کریں جو آپ نے استعمال کئے ھیں۔ اگر آپ کنفیوز محسوس کر رھے ھیں تو یہ مت سمجھیں کہ یہ آپ کی غلطی ھے۔ ویب سائٹ یا ایپ کی طرف سے استعمال کردہ الفاظ پر غور کریں کیونکہ ھو سکتا ھے وہ غیرواضح ھوں۔

3.

میڈیا میں زیادہ رھیں

جیسا کہ آپ یہ سیکھ سکتے ھیں کہ آپ ایسے فیچرز اور ڈیزائن پر برتری کیسے حاصل کر سکتے ھیں جو آپ کو سکرولنگ اور کلکنگ کی طرف راغب کرتے ھیں ایسے ھی آپ ایسی خبروں اور پوسٹس جو آپ کو گمراہ کرتی ھیں کے متعلق زیادہ اچھا سمجھ سکتے ھیں۔

اب تک ھو سکتا ھے کہ آپ مس انفارمیشن اور فیک نیوز کے متعلق سن چکے ھوں گے۔ اگر آپ تنقیدی سوالات پوچھنے کی عادت بنا لیں تو مس انفارمیشن سے بچ سکتے ھیں اور خاص طور پر ایسی خبروں کے متعلق جو بہت زیادہ حیران کن ھو اور ان کا سچ ھونا ناممکنات میں سے ھوں۔ آپ ان کے متعلق زیادہ چوکس اور ھوشیار رہ سکتے ھیں۔

آخرکار آپ ان خبروں کے حقیقی یا جھوٹا ھونے کی تصدیق کرنا چاھیں گے خاص طور پر اگر آپ ان خبروں کو اپنے دوستوں یا خاندان کے لوگوں کے ساتھ شیئر کرنا چاہ رھے ھیں۔ آپ یہ چند سوالات پوچھ سکتے ھیں

یہ خبر کس ویب سائٹ سے لی گئی ھے؟ یہ خبر کس نے اور کب لکھی ھے؟ ھیڈلائن کے علاوہ باقی آرٹیکل میں کیا بات کی گئی ھے؟ اس خبر میں وہ کس سورس کا حوالہ دے رھے ھیں؟

اگر آپ سمجھتے ھیں کہ یہ مس انفارمیشن ھے اور آپ اس کے پھیلاؤ کو روکنا چاھتے ھیں تو زیادہ تر پلیٹ فارمز پر اس کو رپورٹ کرنے کی سہولت ھوتی ھے۔ آپ شاید اس بارے میں بھی فیصلہ کرنا چاھیں کہ آپ اس اکاوئنٹ کو فالو کرنا جاری رکھنا چاہ رہ رھے ھیں یا نہیں