کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

اس شمارے میں شامل ہے:

- اپنے ٹیبلیٹ کو محفوظ بنانا
- اپنے ٹیبلیٹ کو محفوظ بنائے رکھنا

OUCH!

اپنے نئے ٹیبلیٹ کو محفوظ بنانا

جائزہ

آپ کو نیا ٹیبلیٹ مبارک ہو! یہ ٹیکنالوجی دوسروں سے بات چیت کرنے، آن لائن خریداری کرنے، فلمز دیکھنے، گیمز کھیلنے اور ہزاروں دیگر سرگرمیاں سرانجام دینے کا سہل اور طاقتور زریعہ ہے- کیونکہ ٹیبلیٹ کا آپ کی زندگی کا اہم حصہ بنّے کے امکانات کافی زیادہ ہیں، شاید آپ کے کمپیوٹر کے متبادل کے طور پر، اِس لیۓ اپنی معلومات اور ٹیبلیٹ کے تحفظ کے لیۓ آپ مُندرجہ ذیل اہم اقدامات اٹھا سکتے ہیں-

مہمان ایڈیٹر

لوری روزنبرگ انفارمیشن سکیورٹی سے متعلق تعلیمی مواد بنانے اور ملازمین اور صارفین کو تربیت فراہم کرنے کا وسیع تجربہ رکھتی ہیں اور وہ اس تعلیم کا اشتراک کرنے کے جدید اور مصروُف کُن طریقوں کے بارے میں بہت پُر جوش ہیں- آپ ٹوئیٹر پر اُن تک رسائی @InfoSecLori کے ذریعے حاصل کر سکتے ہیں-

اپنے ٹیبلیٹ کو محفوظ بنانا

آپ کے لیۓ یہ بات شاید حیران کُن ہو کہ آپ کے ٹیبلیٹ کو سب سے زیادہ خطرہ ہیکرز سے نہیں بلکہ مُمکنہ طور پر آپ سے ہے- آپ کے ٹیبلیٹ کے گُم ہونے، کہیں بھُولنے یا اُس کے چوری ہونے کے امکانات، کسی کا اُس کے ہیک کرنے کے امکانات سے کہیں زیادہ ہیں- اپنے ٹیبلیٹ کی حفاظت کے لیۓ سب سے اہم قدم اِسکرین کو لاک کرنے کے خوُدکار نظام کو فعّال کرنا ہے- اِس کا مطلب ہے کہ ہر دفعہ اپنے ٹیبلیٹ کو استعمال کرتے وقت آپ کو پہلے اپنی اسکرین کو ایک مضبوط، سوئپنگ پیٹرن یا اپنی فِنگر پرنٹ کے ذریعے ان لاک کرنا پڑے گا- یہ اِس بات کو یقینی بناتا ہے کہ اگر آپ کا ٹیبلیٹ گم یا چوری ہو جاتا ہے تو کوئی اس میں موجود معلومات تک رسائی حاصل نہیں کر سکے گا اور آپ کی تمام ذاتی معلومات، موبائل ایپلیکیشنز اور کوئی بھی دوسری معلومات محفوظ رہتی ہیں- ایک بار خودکار اسکرین لاک فعّال ہو جائے تو آپ اُسے مزید محفوظ بنانے کے لیۓ مُندرجہ ذیل اقدامات اپنا کر اپنے نئے ٹیبلیٹ کو مزید محفوظ بنا سکتے ہیں:

۱. آپ ایسا سافٹ ویئر انسٹال یا فعّال کریں جس کے ذریعے آپ اپنے ٹیبلٹ کو انٹرنیٹ کے ذریعے دوُر سے ٹریک کر سکتے ہوں۔ اس طرح سے اگر آپ کا ٹیبلٹ گُم یا چوری ہو جاتا ہے تو آپ ممکنہ طور پر انٹرنیٹ کے ذریعے اُس سے مُنسلک ہو سکتے ہیں اور اُس کے مقام کا تعیّن کر سکتے ہیں یا بد ترین صورت میں دُور سے بیٹھ کر اپنی تمام معلومات کو حذف کر سکتے ہیں۔

۲. اپنے ٹیبلٹ کو اپڈیٹ کریں اور خوُدکار اپڈیٹ کو فعّال کر دیں تا کہ وہ ہمیشہ آپریٹنگ سسٹم کا جدید ترین ورژن استعمال کرے۔ حملہ آور سافٹ ویئر میں ہمیشہ کمزوریاں تلاش کر رہے ہوتے ہیں اور وینڈرز انھیں دُرست کرنے کے لیئے تسلسُل کے ساتھ نئی اپڈیٹ اور پیچز جاری کر رہے ہوتے ہیں۔ ہمیشہ جدید ترین آپریٹنگ سسٹم چلانے اور موبائل ایپلیکیشنز کا جدید ترین ورژن استعمال کرنے سے آپ کسی کے لیۓ بھی ٹیبلٹ کو ہیک کرنا بہت مشکل بنا دیتے ہیں۔

۳. آپ اپنے ٹیبلٹ کو پہلی مرتبہ کنفِگر کرتے وقت پوری توجّہ دیں خُصوصاً پرائیویسی اختیارات پر۔ آپ کے ٹیبلٹ کے بڑے پرائیویسی مسائل میں سے ایک یہ ہے کہ دوسرے لوگ آپ کے مقام کو ٹریک کر سکتے ہیں اور آپ کے مقام کا پتہ لگا سکتے ہیں۔ ہمارا مشورہ ہے کہ

اپنے نئے ٹیبلیٹ کو محفوظ بنانا

آپ اپنے مقام کی ٹریکنگ کو تمام ایپلیکیشنز کے لیئے غیرفعّال کر دیں، پھر صرف اُن ایپلیکیشنز کے لیئے فعّال کریں جن کے لیئے آپ کو اُس کی ضرورت ہے۔ کُچھ ایپلیکیشنز کے لیئے آپ کے مقام کو ٹریک کرنا ضروری ہوتا ہے جیسے کہ نقشے کی ایپلیکیشنز کے لیئے یا کسی مقامی ریسٹورنٹ تلاش کرنے کے لیئے، لیکن آپ کی زیادہ تر ایپلیکیشنز کو حقیقی وقت میں مقام کی معلومات کی ضرورت نہیں ہوتی ہے۔

۴. زیادہ تر ٹیبلٹس اور ایپلیکیشنز آپ کی معلومات کو کلاؤڈ پر ذخیرہ کرتی ہیں۔ آپ اس بات کی یقین دہانی کر لیں کہ آپ اس بات کو سمجھتے ہیں کہ آپ کی معلومات کہاں ہیں اور اس کی حفاظت کس طرح ہو رہی ہے۔ مثال کے طور پر آپ کبھی بھی نہیں چاہیں گے کہ آپ کی ذاتی تصاویر کا اشتراک، مکمل محل وقوع کی معلومات کے ساتھ انٹرنیٹ پر ہو اور ساری دنیا انھیں دیکھ لے۔ آپ کلاؤڈ پر کسی بھی قسم کی معلومات کے اشتراک کو غیرفعّال کر دیں اور صرف اس وقت فعّال کریں جب آپ کسی مخصوص چیز کا اشتراک کرنا چاہیں۔

۵. ۵۔ٹیبلٹس آپ کی ایپلیکیشنز کو دوسرے آلات، جیسے کہ اسمارٹ فون یا لیپ ٹاپ، کے ساتھ بہت تیزی سے سنکرونائز کرتے ہیں۔ سنکرونائزیشن ایک بہت ہی حیرت انگیز خصوصیت ہو سکتی ہے لیکن اُن ایپلیکیشنز یا خصوصیات کے بارے میں محتاط رہیں جنھیں آپ سنکرونائز کرنے کی اجازت دیتے ہیں۔ اگر آپ کی سنکرونائزیشن فعّال ہے تو آپ یہ دیکھ کر حیران نہ ہوں کہ آپ نے کن جگہوں کا دورہ کیا ہے اور جو ٹیبز آپ نے اپنے ٹیبلٹ کے براؤزر میں بنائے ہیں وہ آپ کے دفتر کے براؤزر پر نظر آرہے ہیں۔

اپنے ٹیبلٹ کو محفوظ بنانے کا بہترین طریقہ اسکرین لاکنگ کو فعّال کرنا، پرائیویسی سیٹینگز کا جائزہ لینا اور اپنےٹیبلٹ کو اپڈیٹ رکھنا ہے۔

اپنے ٹیبلیٹ کو محفوظ بنائے رکھنا

ایک دفعہ آپ کا ٹیبلٹ محفوظ ہو جائے تو آپ کو اس بات کی یقین دہانی کرنی پڑے گی کہ یہ اس طرح ہی محفوظ رہے۔ آپ مندرجہ ذیل اقدامات اپنا کر اپنے ٹیبلٹ کو لمبے عرصے تک محفوظ رکھ سکتے ہیں۔

- آپ اپنے ٹیبلٹ کو کبھی بھی جیل بریک یا ہیک نہیں کریں۔ اس طرح سے کئی سکیورٹی کنٹرولز نظرانداز ہو جاتے ہیں اور آپ کے ٹیبلٹ میں حملوں کے خطرات کہیں زیادہ بڑھ جاتے ہیں۔
- آپ صرف وہ ایپلیکیشنز ڈاؤن لوڈ کریں جن کی آپ کو ضرورت ہے اور اس بات کی بھی یقین دہانی کر لیں کہ آپ صرف قابل اعتماد ذریعے سے ڈاؤن لوڈ کررہے ہیں۔ ‹آئی پیڈز› کے لیئے آپ صرف ‹آئی ٹیونز› کے ذریعے ایپلیکیشنز ڈاؤن لوڈ کریں۔ ایپّل ان تمام ایپلیکیشنز کو ‹آئی ٹیونز› پر دستیاب کرنے سے پہلے ان کی جانچ پڑتال کرتا ہے۔ اینڈرائڈ کے لیئے ہمارا مشورہ ہے کہ آپ صرف ‹گُوگل پلے› کے ذریعے ایپلیکیشنز ڈاؤن لوڈ کریں اور ‹ایمیزون ٹیبلٹ› کے لیئے ہمارا مشورہ ہے کہ آپ صرف ‹ایمیزون ایپ اسٹور› کے ذریعے ہی ایپلیکیشنز ڈاؤن لوڈ کریں۔ آپ جبکہ دوسری سائٹس سے بھی ایپلیکیشنز ڈاؤن لوڈ کر سکتے ہیں لیکن اُن ایپلیکیشنز کی جانچ پڑتال نہیں ہوئی ہوتی ہے اور ہو سکتا ہے کہ یہ متاثر بھی ہوں۔ آخر میں یہ کہ اس بات سے قطع نظر کہ آپ اپنی ایپلیکیشن کہاں سے

اپنے نئے ٹیبلیٹ کو محفوظ بنانا

حاصل کرتے ہیں، اگر آپ اسے فعّال طور استعمال نہیں کر رہے ہیں یا آپ کو اس کی مزید ضرورت نہیں ہے تو ہمارا مشورہ ہے کہ آپ اسے اپنے ٹیبلٹ سے حذف کردیں۔

- جب آپ نئی ایپلیکیشن انسٹال کر رہے ہوتے ہیں تو اِس بات کی یقین دہانی کر لیں کہ آپ اس کی پرائیویسی اختیارات کا جائزہ لے لیں اور اسے مقرر کر دیں بالکل اسی طرح جس طرح آپ نے ابتدائی طور پر ٹیبلیٹ کنفِگر کیا تھا- کسی بھی ایپلیکیشن کو کتنی رسائی دینی ہے، اِس بارے میں آپ محتاط رہیں- مثال کے طور پر وہ ایپلیکیشن جسے آپ نے ابھی ڈائون لوڈ کیا ہے، کیا اسے آپ کے تمام دوستوں اور روابط کی معلومات تک رسائی کی ضرورت ہے؟ اگر آپ کسی ایپلیکیشن کی مطلوبہ اجازت سے غیر مطمئن ہیں تو آپ کسی ایسی ایپلیکیشن کو ڈھونڈیں جو آپ کی ضروریات پوری کرتی ہوں- مزید یہ کہ آپ باقاعدگی سے ایپلیکیشن کی اجازت کی جانچ پڑتال کرتے رہیں اور اِس بات کو یقینی بنائیں کہ وہ تبدیل نہیں ہو رہی ہیں-

آپ کا ٹیبلٹ ایک ایسا مضبوط آلہ ہے جسے ہم چاہتے ہیں کہ آپ استعمال کریں اور لطف اندوز ہوں- صرف ان چند آسان اقدامات کو اپنا کر آپ اپنے نۓ ٹیبلٹ کو لمبے عرصے تک محفوظ بنا سکتے ہیں-

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو ‘لائک’ کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

موبائل ایپلیکیشنز کا محفوظ طریقے سے استعمال:	https://www.securingthehuman.org/ouch/2015#january2015
پاس فریزز:	https://www.securingthehuman.org/ouch/2015#april2015
کلاؤڈ کا محفوظ طریقے سے استعمال:	https://www.securingthehuman.org/ouch/2014#september2014
اپنے موبائل آلہ کو تلف کرنا:	https://www.securingthehuman.org/ouch/2014#june2014
SANS کی آج کی سکیورٹی تجاویز:	https://www.sans.org/tip_of_the_day.php

OUCH! کی ا شاعتSANS Secure The Human Programکے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 4.0 License کے تحت تقسیم کرنے کی اجازت ہوتی ہے۔ آپ اس نیوز لیٹر کو تقسیم سکتے ہیں اگر آپ اس کا حوالہ دیں ، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لئے استعمال کریں ۔ ترجمے اور مزید معلومات کے لئےouch@securethehuman.orgپر رابطہ کریں

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپٹزنر، کارمن رولی ہارڈی۔

ترجمہ: شعیب ہاشمی

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus