تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- موبائل ایپلیکیشنز کا حصول
- اجازت
- ایپلیکیشنز کو اپڈیٹ کرنا

موبائل ایپلیکیشنز کا محفوظ طریقے سے استعمال

جائزہ

موبائل آلات کو جو چیز مختلف بناتی ہے وہ اس میں استعمال ہونے والی لاکھوں ایپلیکیشنز ہیں جن میں سے ہم کسی کو بھی مُنتخب کر سکتے ہیں- یہ ایپلیکیشنز ہمیں زیادہ فعّال بناتی ہیں، فوری مواصلات اور دوسروں سے چیزوں کا اشتراک کرنے، لوگوں کو تربیت یا تعلیم دینے یا پھر صرف تفریح کا موقع فراہم کرتی ہیں- تاہم ان موبائل ایپلیکیشنز کی طاقت کے ساتھ ساتھ کچھ خطرات بھی لاحق ہیں- آپ مُندرجہ ذیل اقدامات اپنا کر اپنی موبائل ایپلیکیشنز کو باحفاظت استعمال کر سکتے ہیں-

مہمان ایڈیٹر

جاشوا رائٹ کاؤنٹر ہیک میں ٹیکنیکل ڈائریکٹر اور SANS انسٹیٹیوٹ میں سینئر انسٹرکٹر ہیں- وہ SEC575: موبائل ڈیوائس سکیورٹی اینڈ ایتھیکل ہیکنگ، اور ہیکنگ ایکسپوزڈ: وائرلیس کے مصنف ہیں- آپ ان تک ٹوئیٹر پر **@joswr1ght** کے ذریعے رسائی حاصل کر سکتے ہیں-

موبائل ایپلیکیشنز کا حصول

سب سے پہلا قدم اس بات کو یقینی بنانا ہے کہ آپ موبائل ایپلیکیشنز کو محفوظ اور قابلِ بھروسہ جگہ سے ڈاؤن لوڈ کر رہے ہیں- سائبر مُجرمان نے ایسی متاثر ایپلیکیشنز بنانے اور اُنھیں بانٹنے میں مہارت حاصل کر لی ہے جو کہ دیکھنے میں بالکل صحیح لگتی ہیں- اگر آپ ان متاثرہ ایپلیکیشنز میں سے کسی کو اِنسٹال کرتے ہیں تو مُجرمان آپ کے موبائل آلات کا مکمّل کنٹرول حاصل کر سکتے ہیں- ایپلیکیشنز کو معروف اور قابلِ بھروسہ جگہ سے ڈاؤن لوڈ کرنے سے آپ متاثرہ ایپلیکیشن اِنسٹال کرنے کے خطرے کو کم کر دیتے ہیں- آپ کو شاید اس بات کا احساس نہیں ہو لیکن آپ کے موبائل آلہ کا برانڈ آپ کی ایپلیکیشنز کو ڈاؤن لوڈ کرنے کے اختیارات کا تعیّن کرتا ہے-

ایپّل کے آلات جیسے کہ آئی پیڈ یا آئی فون میں آپ ایپلیکیشنز کو صرف ایپّل اپ اسٹور کے ذریعے ڈاؤن لوڈ کر سکتے ہیں- اس کا فائدہ یہ ہے کہ ایپّل موبائل ایپلیکیشنز کو دستیاب کرنے سے پہلے اس کی سکیورٹی کی جانچ پڑتال خود کرتا ہے- ایپّل تمام مُتاثرہ موبائل ایپلیکیشنز کو نہیں پکڑ سکتا ہے لیکن اس مُنظّم ماحول کی وجہ سے مُتاثرہ موبائل ایپلیکیشن اِنسٹال کرنے کے خطرات کو حیرت انگیز طور پر کم کرنے میں مدد ملتی ہے- مزید یہ کہ اگر ایپّل کو اپنے ایپ اسٹور میں کوئی ایسی موبائل ایپلیکیشن ملتی ہے جس کے بارے میں اُسے لگتا ہے کہ وہ مُتاثر ہو گئی ہے تو وہ اُسے جلد وہاں سے ہٹا دیتا ہے- ونڈوز فون میں بھی ایپلیکیشنز کے لیئے یہی طریقہ استعمال ہوتا ہے-

اینڈرائڈ موبائل آلات مُختلف ہوتے ہیں- اینڈرائڈ آپ کو اس معاملے میں کافی لچک دیتا ہے کیونکہ وہ آپ کو موبائل ایپلیکیشن انٹرنیٹ پر کہیں سے بھی ڈاؤن لوڈ کرنے دیتا ہے- تاہم اس سہوُلت کے ساتھ ذمہ داری بھی کافی بڑھ جاتی ہے- آپ کو موبائل ایپلیکیشنز کو ڈاؤن لوڈ اور اِنسٹال کرتے وقت کافی مُحتاط رہنا چاہیئے کیونکہ ان تمام ایپلیکیشنز میں سے سب کا جائزہ نہیں لیا گیا ہوتا ہے- گوُگل بھی ایپّل کی طرح ایک مُنظّم موبائل ایپلیکیشن اسٹور چلاتا ہے جو کہ ‹گوُگل پلے› کہلاتا ہے- آپ جو موبائل ایپلیکیشنز گوُگل پلے سے ڈاؤن لوڈ کرتے ہیں، اُن سب نے بُنیادی سکیورٹی ٹیسٹ پاس کیا ہوتا ہے- اس لیئے

موبائل ایپلیکیشنز کا محفوظ طریقے سے استعمال

ہمارا مشورہ ہے کہ آپ اینڈرائڈ ایپلیکیشنز کو صرف گوگل پلے سے ڈاؤن لوڈ کریں- آپ دوسری ویب سائٹس سے اینڈرائڈ موبائل ایپلیکیشنز اِنسٹال کرنے سے اجتناب کریں کیونکہ کوئی بھی، بشمول سائبر مُجرمان کے، با آسانی مُضر موبائل ایپلیکیشنز بنا سکتے ہیں اور اُسے پھیلا سکتے ہیں اور دھوکہ دہی کے ذریعے آپ کے موبائل آلہ کو مُتاثر کر سکتے ہیں- اضافی تحفّظ کے طور پر جب بھی مُمکن ہو آپ اپنے موبائل آلہ پر اینٹی وائرس اِنسٹال کر دیں-

موبائل ایپلیکیشنز کو محفوظ طریقے سے استعمال کرنے کا سب سے آسان طریقہ اُسے قابلِ بھروسہ جگہ سے انسٹال کرنا، اُس کی اپڈیٹس جب بھی دستیاب ہوں اُنھیں انسٹال کرنا اور ایپلیکیشن کو صرف ضرورت کی اجازت دینا شامل ہے-

اس بات سے قطع نظر کہ آپ کون سا آلہ استعمال کر رہے ہیں، ایک اضافی قدم جو آپ اٹھا سکتے ہیں وہ یہ ہے کہ آپ کوئی بھی بالکل نئی ایپلیکیشن یا ایسی ایپلیکیشن جسے بہت کم لوگوں نے ڈاؤن لوڈ کیا ہے یا جس کے بارے میں بہت کم مثبت تبصرے موجود ہوں، کو اِنسٹال کرنے سے اجتناب کریں- جو ایپلیکیشن جتنا زیادہ عرصے سے دستیاب ہو، اُسے جتنے زیادہ لوگوں نے استعمال کیا ہو اور جس کے بارے میں زیادہ مثبت تبصرے موجود ہوں، اُس پر اُتنا ہی بھروسہ کیا جا سکتا ہے- اس کے علاوہ یہ کہ آپ صرف وہ ایپلیکیشنز اِنسٹال کریں جن کی آپ کو ضرورت ہے اور جسے آپ استعمال کرتے ہیں- آپ اپنے آپ سے سوال کریں کہ کیا آپ کو اس ایپلیکیشن کی ضرورت ہے؟ نہ صرف یہ کہ ہر نئی ایپلیکیشن اپنے ساتھ مُمکنہ طور پر نئے خطرات لے کر آتی ہے بلکہ نئے پرائیویسی مسائل بھی لاتی ہے- اگر آپ کوئی ایپلیکیشن استعمال کرنا چھوڑ دیتے ہیں تو اُسے اپنے موبائل آلہ سے نکال دیں (اگر آپ کو اُس کی ضرورت پڑے تو آپ اُسے کبھی بھی واپس اِنسٹال کر سکتے ہیں)- آخر میں یہ کہ آپ اپنے موبائل آلہ کو کبھی بھی جیل بریک یا رُوٹ نہ کریں- یہ وہ طریقہ ہے جس کے ذریعے آپ غیر منظوُرشُدہ ایپلیکیشنز اِنسٹال کر سکتے ہیں یا پہلے سے موجود خُصوصیات میں تبدیلی کر سکتے ہیں- یہ نہ صرف آپ کے موبائل آلہ کے سکیورٹی کنٹرولز کو نظرانداز کرتا ہے بلکہ اس طرح وارنٹی اور سپورٹ کانٹریکٹس بھی غیر مُتاثر ہو جاتے ہیں-

اجازت

ایک بار جب آپ قابلِ بھروسہ جگہ سے موبائل ایپلیکیشن اِنسٹال کر دیں تو اس بات کو یقینی بنائیں کہ آپ نے اُسے محفوظ طریقے سے کنفیگر کیا ہے اور وہ آپ کی پرائیویسی کی حفاظت کر رہا ہے- آپ موبائل ایپلیکیشن کو اپنے آلہ میں کسی قسم کی بھی رسائی فراہم کرنے سے پہلے ضرور سوچیں کہ: کیا آپ اُس ایپلیکیشن کو اُس کی مانگی گئی اجازت دینا چاہتے ہیں؟ کیا اُس ایپلیکیشن کو اُس اجازت کی ضرورت ہے بھی؟ مثال کے طور پر کُچھ ایپلیکیشنز ‹جیو-لوکیشن› کا استعمال کرتی ہیں- اگر آپ ایسی کسی ایپلیکیشن کو اپنے محّلِ وقوُع کی ہمیشہ معلوُمات فراہم کرنا چاہتے ہیں تو اس کا مطلب ہے کہ آپ اُس ایپلیکیشن کے خالق کو اپنی مُکمّل نقل و حرکت کو ٹریک کرنے کی اجازت دے رہے ہیں جس کے نتیجے میں ہو سکتا ہے کہ وہ آپ کی معلوُمات دوُسروں کو بیچ دے- اگر آپ اُنہیں اجازت نہیں دینا چاہتے ہیں تو اُن کی طرف سے مانگی گئی اجازت کی تمام درخواستوں کو رد کر دیں یا کوئی دوسری ایسی ایپلیکیشن ڈھوُنڈیں جو کہ آپ کی ضروریات پوری کرتی ہو- یہ بات ہمیشہ یاد رکھیں کہ آپ کے پاس بہت اختیارات ہیں-

موبائل ایپلیکیشنز کا محفوظ طریقے سے استعمال

ایپلیکیشنز کو اپڈیٹ کرنا

موبائل ایپلیکیشنز کو بھی بالکل آپ کے کمپیوٹر اور موبائل آلہ کے آپریٹنگ سسٹم کی طرح اپڈیٹ اور تازہ ترین رکھنے کی ضرورت ہوتی ہے- مُجرمان مُسلسل ایپلیکیشنز میں کمزوریاں تلاش کر رہے ہوتے ہیں- وہ پھر اِن کمزوریوں کا فائدہ اُٹھانے کے لیۓ حملے تخلیق کرتے ہیں- جو لوگ آپ کی ایپلیکیشن تخلیق کرتے ہیں وہ اِن کمزوریوں کی تصحیح اور آپ کے آلات کو محفوظ رکھنے کے لیۓ اپڈیٹس بھی جاری کرتے ہیں- آپ جتنا زیادہ اپڈیٹس کے بارے میں جانچ کریں گے اور اُنھیں اِنسٹال کریں گے، اُتنا ہی بہتر ہوگا- زیادہ تر آلات آپ کو موبائل ایپلیکیشنز میں خوُدکار طور پر اپڈیٹ کو کنفیگر کرنے کی سہولت فراہم کرتے ہیں- ہمارا مشورہ ہے کہ آپ اِس سیٹنگ کا ضرور استعمال کریں- اگر یہ مُمکن نہیں ہے تو ہمارا مشورہ ہے کہ آپ اپنی موبائل ایپلیکیشنز میں ہر دو ہفتے بعد اپڈیٹس کی جانچ کریں- آخری بات یہ کہ جب آپ کی ایپلیکیشنز اپڈیٹ ہو جائیں تو آپ اِس بات کو یقینی بنائیں کہ آپ نے اُس میں مانگی گئی کسی بھی نئی اجازت کی تصدیق کر لی ہے-

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 securingthehuman.sans.org/ouch/archives (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:

سوشل انجینئرنگ: https://securingthehuman.sans.org/ouch/2017#january2017

اپنے موبائل آلہ کو تلف کرنا: https://securingthehuman.sans.org/ouch/2016#december2016

اپنے نئے ٹیبلٹ کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#january2016

OUCH آرکائیوز اور ترجُمے: https://securingthehuman.sans.org/ouch/archives

موبائل آلہ کی سکیورٹی کا کورس: https://sans.org/sec575

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

ترجمہ: شعیب ہاشمی