کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:
- جائزہ
- پانچ اہم اقدامات

محفوظ رہنے کےلئے پانچ اقدامات

جائزہ

ٹیکنالوجی جس طرح ہماری زندگیوں میں اہمیت حاصل کرتی جا رہی ہے، اتنا ہی پیچیدہ بھی ہوتی جا رہی ہے۔ اس بات کو مدنظر رکھتے ہوئے کہ ٹیکنالوجی تیزی سے تبدیل ہوتی رہتی ہے، حفاظت سے متعلق مشورے الجھن پیدا کر سکتے ہیں۔ ایسا لگتا ہے کہ ہمیشہ کوئی نئی ہدایت موجود ہوتی ہے اس بارے میں کہ آپ کو کیا کرنا چاہیئے اور کیا نہیں۔ اگرچہ محفوظ رہنے کے طریقے وقت کے ساتھ ساتھ تبدیل ہو سکتے ہے، کچھ ایسے بنیادی اقدامات ہیں جنہیں آپ اپنا کر ہمیشہ اپنے آپ کو محفوظ رکھ سکتے ہیں۔ اس بات سے قطع نظر کہ آپ کون سی ٹیکنالوجی استعمال کر رہے ہیں یا کہاں استعمال کر رہے ہیں، ہمارا مشورہ ہے کہ آپ مندرجہ ذیل پانچ اہم اقدامات اپنائیں۔

مہمان ایڈیٹر

لینی ذیلٹسر OUCH کے اس شمارے کے مہمان ایڈیٹر ہیں۔ لینی ، NCR Corp میں اپنی توجہ صارفین کے آئی ٹی آپریشن کی حفاظت پر مرکوز رکھتے ہیں اور SANS انسٹیٹیوٹ میں میل ویر کی روک تھام کے بارے میں تربیت دیتے ہیں۔ لینی ٹوئیٹر پر **@lennyzeltser** کے ذریعے فعال ہیں اور وہ سکیورٹی کے بلاگ **blog.zeltser.com** پہ لکھتے ہیں۔

پانچ اہم اقدامات

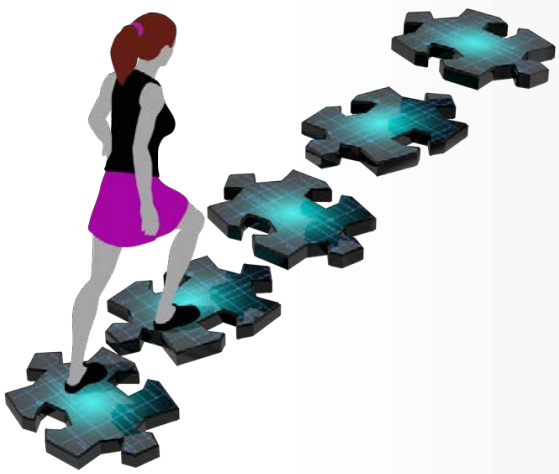
مندرجہ ذیل پانچ میں سے ہر ایک اقدام کا آسان جائزہ لیا گیا ہے۔ ہر اقدام کے بارے میں مزید جاننے کے لئے اس نیوز لیٹر کے آخری حصے «وسائل» میں جائیں۔

۱. **آپ:** سب سے پہلے آپ یہ بات زہن نشین کر لیں کہ محظ ٹیکنالوجی آپ کی مدد نہیں کر سکتی ہے۔ حملہ آوروں نے زیادہ تر سکیورٹی ٹیکنالوجی سے بچنے کا آسان طریقہ آپ پر حملہ کرنا نکالا ہے۔ اگر انہیں آپ کا پاس ورڈ یا کریڈٹ کارڈ چاہیئے ہو تو ان کے لئے سب سے آسان طریقہ آپ کو دھوکہ دے کر معلومات نکلوانا ہے۔ مثال کے طور پر وہ آپ کو مائیکروسافٹ کی ٹیکنیکل سپورٹ ٹیم کا نمائندہ بن کر آپ سے بات کر سکتے ہیں اوریہ دعوہ کرسکتے ہیں کہ آپ کا کمپیوٹر متاثر ہو چکا ہے جبکہ در حقیقت وہ سائبر مجرمان ہوتے ہیں جنہیں صرف آپ کے کمپیوٹر تک رسائی چاہیئے ہوتی ہے یا شاہد وہ آپ کو ای میل بھیجیں کہ آپ کا سامان پہنچایا نہیں جا سکتا ہے اور پھر آپ سے ایک لنک کا دورہ کرنے کا کہیں تاکہ آپ کے پتے کی تصدیق کی جا سکے۔ لیکن حقیقت میں وہ چاہتے ہیں کہ آپ ایک متاثرہ ویب سائٹ کا دورہ کریں جس کے ذریعہ وہ آپ کے کمپیوٹر کو ہیک کر سکیں۔ بلآخر حملہ آور کے خلاف سب سے مضبوط ترین دفاع آپ ہیں۔ آپ مشکوک رہیں کیونکہ عقل کا استعمال کرنے سےآپ زیادہ تر حملوں کو پکڑ سکتے ہیں اور ان کی روک تھام کرسکتے ہیں۔

۲. **اپڈیٹ کرنا:** آپ اس بات کی تاکید کرلیں کہ آپ کے کمپیوٹرز، موبائل آلات، ایپلیکیشنز اور باقی تمام چیزیں جو نیٹ ورک سے متعلق ہیں، ان میں سافٹ ویئر کا جدید ترین ورژن چل رہا ہو۔ سائبر مجرمان مسلسل آپ کی استعمال کردہ ٹیکنالوجی میں نقس تلاش کر رہے ہوتے ہیں۔ جب وہ یہ کمزوری تلاش کرتے ہیں تو کچھ خاص پروگرامز کے ذریعے ان کا فائدہ اٹھاتے ہوئے آپ کے زیراستعمال کسی بھی ٹیکنالوجی کو

محفوظ رہنے کےلئے پانچ اقدامات

ہیک کرلیتے ہیں جس میں نیٹ ورک، آپ کا کمپیوٹر اور موبائل آلات شامل ہیں۔ دراصل وہ کمپنیز جن کی ٹیکنالوجی آپ استعمال کررہے ہوتے ہیں وہ اس ٹیکنالوجی کو تازہ ترین رکھنے کے لئے سخت محنت کرتی ہیں۔ ایک بار جب کسی کمزوری کا پتہ چل جائے تو وہ اسے صحیح کرنے کے لئے اسکا پیچ (patch) تخلیق کرتے ہیں اور اسے عوامی سطح پرشائع کرتے ہیں۔ اس بات کو یقینی بنا کر کہ آپ کے کمپیوٹرز اور موبائل آلات میں یہ اپ ڈیٹس موجود ہیں، آپ معروف خطرات کے امکان کو محدود کردیتے ہیں جس کی وجہ سے کسی کے لئے بھی آپ کو ہیک کرنا بہت مشکل ہو جاتا ہے۔ تازہ ترین سافٹ ویئر سے ہم آہنگ ہونے کے لئے جب بھی ممکن ہو، خودکار اپڈیٹ کو فعال کردیں۔ یہ اصول تقریباً ہر اس ٹیکنالوجی پر لاگو ہوتے ہیں جو نیٹ ورک سے منسلک ہوتی ہے جس میں انٹرنیٹ سے منسلک ٹی۔وی،بے بی مانیٹر، گھر کے راؤٹرز، گیمنگ کنسول یا شاید کبھی کبھی آپ کی گاڑی بھی شامل ہے۔ اگر آپ کے کمپیوٹر کا آپریٹنگ سسٹم، موبائل آلہ یا آپ کے زیر استعمال کسی بھی ٹیکنالوجی کی سپورٹ دستیاب نہیں ہے یا وہ مزید اپ ڈیٹ حاصل نہیں کر سکتی ہے تو ہمارا مشورہ ہے کہ آپ نیا ورژن حاصل کریں جس کی سپورٹ ممکن ہو۔



ان پانچ اہم اقدامات کو اپنا کر آپ جدیدترین ٹیکنالوجی کا استعمال کرتے ہوئے اپنے آپ کو لمبے عرصے تک محفوظ رکھ سکتے ہیں۔

۳. **پاس ورڈ:** اپنے آپ کو محفوظ رکھنے کا اگلا قدم اپنے ہر ایک آلہ، آن لائن اکاؤنٹ اور ایپلیکیشنز کے لئے مضبوط اور منفرد پاس ورڈ کا استعمال کرنا ہے- یہاں اہم الفاظ مضبوط اور منفرد ہیں- ایک مضبوط پاس ورڈ کا مطلب ہے کہ ایسا پاس ورڈ جس کا ہیکرز یا انکے خود کار پروگرامز آسانی سے اندازہ نہیں لگا سکیں۔ ایک لفظ کے پاس ورڈ کے بجائے آپ لمبے پاس ورڈ کا استعمال کریں جس میں کچھ خصوصی حروف اور اعداد اچھے اقدامات کے طور پر شامل ہوں۔ اس طرح اگر آپ کا کوئی ایک پاس ورڈ گم یا چوری ہو جاتا ہے تو آپ کے باقی تمام اکاؤنٹس اور آلات محفوظ رہتے ہیں۔ کیا آپ تمام مضبوط منفرد پاس ورڈ یاد نہیں رکھ سکتے ہے؟ پریشان مت ہوں، ہم بھی اتنے سارے پاس ورڈ یاد نہیں رکھ سکتے ہیں۔ اس لئے ہمارا مشورہ ہے کہ آپ پاس ورڈ مینیجر استعمال کریں جو کہ آپ کے اسمارٹ فون یا کمپیوٹر کے لئے ایک ایسی مخصوص ایپلیکیشن ہے جو آپ کے تمام پاس ورڈز کو محفوظ طریقے سے انکرپشن کے ذریعے ذخیرہ کرتی ہے۔ آخر میں یہ کہ اگر آپ کا کوئی بھی اکاؤنٹ ٹو-اسٹیپ ویری فیکیشن کی ہمایت کرتا ہے تو ہمارا پرزور مشورہ ہے کہ آپ اسے ہمیشہ فعال رکھا کریں کیونکہ یہ آپ کے اکاؤنٹ کی حفاظت کے لیےمضبوط ترین طریقوں میں سے ایک ہے۔

۴. **انکرپشن:** ہمارا چوتھا مشورہ انکرپشن کا استعمال ہے۔ انکرپشن اس بات کو یقینی بناتا ہےکہ صرف آپ یا آپکہ بااعتماد لوگ آپ کی معلومات تک رسائی حاصل کر سکتے ہیں۔ معلومات دو جگہ پر انکرپٹ ہو سکتی ہیں۔ ایک اس وقت جب وہ ساکت ہوں اور دوسرا اس وقت جب وہ متحرک ہوں۔ ساکت معلومات کو انکرپٹ کرنے کا مطلب ہے کہ معلومات کی اس وقت حفاظت کرنا جب وہ فائل کے طور پر محفوظ ہوں جیسے کہ آپ کی ہارڈ ڈسک یا یو۔ایس۔بی اسٹک پر- زیادہ تر آپریٹنگ سسٹم آپ کی معلومات کو فل ڈسک انکرپشن جیسی خصوصیات کے ذریعے خود کار طور پر انکرپٹ کرنے کی سہولت مہیا کرتے ہیں- ہمارا مشورہ ہے کے جب بھی ممکن ہو، آپ اسے فعال کردیں- متحرک معلومات کو انکرپٹ کرنے کا مطلب ہے کہ معلومات کو آپ کے کمپیوٹر یا آلہ سے کسی دوسرے کمپیوٹر یا آلہ پر منتقلی کے دوران

محفوظ رہنے کےلئے پانچ اقدامات

انکرپٹ کرنا جیسا کہ آن لائن بینکنگ کے دوران- براؤزنگ کے دوران انکرپشن کے فعال ہونے کی تصدیق کا ایک آسان طریقہ یہ ہے کے آپ اس بات کو یقینی بنائیں کہ جس ویب سائیٹ کا آپ دورہ کر رہے ہیں اس کا ایڈریس «https:» سے شروع ہو رہا ہو اور اس کے بالکل ساتھ بند تالے (پیڈلاک) کی تصویر ہو۔

۵. **بیک اپ:** بعض دفعہ آپ چاہے جتنا بھی احتیاط کر لیں، آپ کا کوئی آلہ یا اکاؤنٹ متاثر ہوسکتا ہے۔ اگر ایسا ہوتا ہے تو آپ کے پاس اس بات کو یقینی بنانے کے لئے کہ آپ کا کمپیوٹر یا موبائل آلہ میل ویئر سے پاک ہے، صرف ایک طریقہ جاتا ہے اور وہ یہ کہ آپ اپنے کمپیوٹر یا موبائل آلے کو پوری طرح وائپ کردیں اور شروع سے اس کی تعمیر نو کریں- ہو سکتا ہے کہ حملہ آور متاثرہ کمپیوٹر پر آپ کو اپنی ذاتی تصاویر اور دوسری محفوظ معلومات تک رسائی حاصل کرنے سے روک دے۔ آپ کے پاس واحد حل یہ رہ جاتا ہے کے آپ بیک اپ کے ذریعے اپنی تمام ذاتی معلومات کو بحال کریں۔ آپ اس بات کی یقین دہانی کرلیں کہ آپ باقاعدگی سے کسی بھی اہم معلومات کا بیک اپ لیتے رہیں اور اس بات کی بھی تصدیق کر لیں کہ آپ اس کے ذریعے معلومات کو بحال کر سکتے ہیں۔ زیادہ تر آپریٹنگ سسٹمز اور موبائل آلات خودکار بیک اپس کی حمایت کرتے ہیں۔

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں، OUCH! archives تک رسائی حاصل کریں اور SANS سیکیورٹی سے مزید آگاہی کے لئے اس ویب سایٹ 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 کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

ای میل فشنگ حملے:	http://www.securingthehuman.org/ouch/2013#february2013
اپنے ٹیبلٹ کو محفوظ رکھنا:	http://www.securingthehuman.org/ouch/2013#december2013
مضبوط پاس ورڈز:	http://www.securingthehuman.org/ouch/2013#may2013
پاس ورڈ مینیجرز:	http://www.securingthehuman.org/ouch/2013#october2013
ٹو اسٹیپ ویریفیکیشن:	http://www.securingthehuman.org/ouch/2013#august2013
انکرپشن:	http://www.securingthehuman.org/ouch/2014#august2014
بیک اپس:	http://www.securingthehuman.org/ouch/2013#september2013

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

ترجمہ: شعیب ہاشمی