تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- آپ
- پاس ورڈز
- اپڈیٹ کرنا
- بیک اپس

محفوظ رہنے کے لیئے چار اقدامات

جائزہ

ٹیکنالوجی جیسے جیسے ہماری زندگیوں میں اہم کردار ادا کرتی جا رہی ہے ویسے ویسے یہ بہت پیچیدہ بھی ہوتی جا رہی ہے- اِس بات کو مدّنظر رکھتے ہوئے کہ ٹیکنالوجی بہت تیزی سے تبدیل ہوتی ہے، سکیورٹی کی تمام سَفارشات پر عمل کرنا اُلجھن کا باعث ہو سکتا ہے- ایسا لگتا ہے کہ ہمیشہ کوئی نہ کوئی نئی ہدایت آ رہی ہوتی ہے کہ آپ کو کیا کرنا چاہیئے اور کیا نہیں- تاہم، وقت کے ساتھ ساتھ محفوظ رہنے کے طریقے تبدیل ہو سکتے ہیں لیکن آپ چند بُنیادی اقدامات اپنا کر ہمیشہ اپنے آپ کو محفوظ رکھ سکتے ہیں- اِس بات سے قطع نظر کہ آپ کون سی ٹیکنالوجی استعمال کر رہے ہیں یا کہاں استعمال کر رہے ہیں، ہمارا مشورہ ہے کہ آپ مُندرجہ ذیل چار اہم اقدامات کو اپنائیں- آپ مُندرجہ ذیل اقدامات کے بارے میں مزید جاننے کے لیئے اِس نیوز لیٹر کے آخری حصے 'وسائل' سے رُجوع کریں-

مہمان ایڈیٹر

راین جانسن اپنی توجہ اِس بات کو یقینی بنانے پر مرکوز رکھتے ہیں کہ تنظیمیں کسی بھی ناگُزیر خلاف ورزی کی صورتحال سے نمٹنے کے لیئے مُناسب اقدامات کے ساتھ تیار رہیں- اِس کے علاوہ وہ SANS اِنسٹیٹیوٹ میں ایڈوانسڈ نیٹ ورک فارینزکس بھی پڑھاتے ہیں- راین ٹُوئیٹر پر @ForensicRJ کے ذریعے فعّال ہیں-

۱. **آپ**: سب سے پہلے آپ اِس بات کو ذہن نشین کر لیں کہ محض ٹیکنالوجی کا استعمال آپ کو مکمل تحفظ فراہم کرنے کے لیئے کبھی بھی کافی نہیں ہوتا- حملہ آوروں کو یہ بات پتہ چل چُکی ہے کہ سب سے مُشکل ترین سکیورٹی ٹیکنالوجی کو بھی عبُور کرنے کا سب سے آسان طریقہ آپ پر حملہ کرنا ہے- اگر اُنہیں آپ کا پاس ورڈ، کریڈٹ کارڈ یا ذاتی معلومات چاہیئے تو اُن کے لیئے سب سے آسان طریقہ دھوکہ دہی کے ذریعے آپ سے معلومات نکلوانا ہے- مثال کے طور پر وہ آپ کو مائیکروسافٹ کی ٹیکنیکل سپورٹ ٹیم کا نمائندہ بن کر کال کر سکتے ہیں اور یہ دعوہ کر سکتے ہیں کہ آپ کا کمپیوٹر متأثر ہو گیا ہے جبکہ حقیقت میں وہ صرف سائبر مُجرمان ہوتے ہیں جو کہ یہ چاہتے ہیں کہ آپ اُن کو اپنے کمپیوٹر تک رسائی فراہم کر دیں- یہ بھی ہو سکتا ہے کہ وہ آپ کو ای-میل بھیجیں اور آپ کو یہ بتائیں کہ آپ کا کوئی پیکج ارسال نہیں کیا جا سکا اور آپ سے کہیں کہ آپ اُس ای-میل میں دیئے گئے لِنک کو کِلک کر کے اپنے ڈاک کے پتے کی تصدیق کر دیں، درحقیقت وہ آپ کو دھوکہ دہی کے ذریعے مُضر ویب سائٹ پر لے جانا چاہ رہے ہوتے ہیں جس کے ذریعے آپ کا کمپیوٹر ہیک ہو جائے- اسی طرح رینسم ویئر یا سی-ای-او فراڈ جیسے حملے شروع ہوتے ہیں- بِل آخر حملہ آوروں کے خلاف سب سے بہترین دفاع آپ ہیں، آپ مشکوک رہیں- آپ اپنے عام فہم کے استعمال سے زیادہ تر حملوں کی نشاندہی کر سکتے ہیں اور اُنہیں روک سکتے ہیں-

۲. **پاس ورڈز**: اپنی حفاظت کا اگلا قدم اپنے ہر آلہ اور آن لائن اکاؤنٹ کے لیئے مضبوط اور منفرد پاس ورڈ کا استعمال ہے- یہاں اہم الفاظ 'مضبوط' اور 'منفرد' ہیں- ایک مضبوط پاس ورڈ کا مطلب ہے کہ وہ پاس ورڈ جس کا اندازہ با آسانی ہیکرز یا اُن کے خوُدکار پروگرامز نہیں لگا سکتے ہیں- کیا آپ کے لیئے پیچیدہ پاس ورڈز کو یاد رکھنا اور اُنہیں لکھنا مُشکل ہے؟ اس کے بجائے آپ پاس فریز کا استعمال کریں- ایک لفظ استعمال

محفوظ رہنے کے لیۓ چار اقدامات

ان چار اہم اقدامات کو اپنا کر آپ جدید ترین ٹیکنالوجی استعمال کرتے ہوۓ اپنے آپ کو دیرپا تحفّظ فراہم کر سکتے ہیں-

کرنے کے بجاۓ آپ الفاظ کا مجموعہ یا کوئی ایسا جُملہ استعمال کریں جسے یاد رکھنا آسان ہو جیسے کہ «میری کافی کہاں ہے؟» جتنا بڑا جملہ ہوگا، پاس ورڈ اتنا ہی مضبوط ہوگا- ایک منفرد پاس ورڈ کا مطلب ہے کہ ہر آلہ اور آن لائن اکاؤنٹ کے لیۓ مختلف پاس ورڈ استعمال کرنا- اس طرح اگر ایک پاس ورڈ کسی کے ہتّھے چڑھ بھی جاتا ہے تو آپ کے باقی تمام اکاؤنٹس اور آلات محفوظ رہتے ہیں- کیا آپ اپنے تمام مضبوط اور منفرد پاس ورڈز یاد نہیں رکھ سکتے ہیں؟ فکر نہ کریں کیونکہ ہم بھی سب کو یاد نہیں رکھ سکتے ہیں- اس لیۓ ہمارا مشورہ ہے کہ آپ پاس ورڈ مینیجر کا استعمال کریں جو کہ آپ کے اسمارٹ فون یا کمپیوٹر کے لیۓ ایک خصوصی ایپلیکیشن ہے جس کے ذریعے آپ پاس ورڈز کو محفوظ طریقے سے اِنکرپٹڈ شکل میں ذخیرہ کر سکتے ہیں-

آخر میں یہ کہ کسی بھی اکاؤنٹ کی حفاظت کے لیۓ سب سے اہم ترین اقدامات میں سے ایک ٹُو-اسٹیپ ویریفیکیشن کو فعال کرنا ہے- محض پاس ورڈز کا استعمال اکاؤنٹس کی حفاظت کے لیۓ کافی نہیں ہے، اِس لیۓ ہمیں مزید مضبوط حفاظتی اقدامات اُٹھانے پڑیں گے- ٹُو-اسٹیپ ویریفیکیشن کافی مضبوط ہے، وہ آپ کے پاس ورڈ کے علاوہ ایک دوسرا قدم بھی استعمال کرتا ہے جو کہ آیا کوئی ایسی چیز ہوتی ہے جو کہ آپ کے پاس ہوتی ہے (جیسے کہ آپ کے اسمارٹ فون پر بھیجا گیا کوئی کوڈ یا آپ کے اسمارٹ فون میں موجود کسی ایپلیکیشن کی جانب سے نکلا ہُوا کوڈ) یا کوئی ایسی چیز جو آپ میں ہے (بایومیٹریکس)- آپ اِس اختیار کو اپنے ہر ممکنہ اکاؤنٹ پر فعّال کر دیں بشمول پاس ورڈ مینیجر- ٹُو-اسٹیپ ویریفیکیشن، اپنی حفاظت کا شاید واحد بہت اہم قدم ہے اور یہ آپ کی سوچ سے بہت زیادہ آسان ہے-

۳. **اپڈیٹنگ**: آپ اس بات کو یقینی بنائیں کہ آپ کے کمپیوٹرز، موبائل آلات، ایپلیکیشنز اور کوئی بھی ایسی چیز جو کہ انٹرنیٹ سے مُنسلک ہوتی ہے، اُس میں سافٹ ویئر کا جدید ترین ورژن چل رہا ہو- سائبر مُجرمان آپ کے زیراستعمال آلات کے سافٹ ویئر میں مُسلسل نئی کمزوریوں کی تلاش میں رہتے ہیں- جب اُنھیں نئی کمزوریاں ملتی ہیں تو وہ خاص پروگرامز کے ذریعے اُس کا فائدہ اُٹھاتے ہوۓ آپ کے زیراستعمال آلات کو ہیک کر لیتے ہیں- دُوسری جانب جو تنظیمیں ان آلات کے لیۓ سافٹ ویئر تخلیق کرتی ہیں، وہ مُسلسل اُن کمزوریوں کو سُدھارنے میں لگی رہتی ہیں اور اُس کی اپڈیٹس شائع کرتی رہتی ہیں- آپ اپنے کمپیوٹرز اور موبائل آلات میں ان اپڈیٹس کو انسٹال کر کے اس بات کو یقینی بناتے ہیں کہ اُن آلات پر کسی کا بھی ہیک کرنا بہت مُشکل ہو جائے- اپنے آپ کو جدید ترین ورژن پر برقرار رکھنے کے لیۓ جب بھی مُمکن ہو آپ خوُدکار اپڈیٹ کو فعّال کر دیں- یہ اصل نیٹ ورک سے مُنسلک کسی بھی ٹیکنالوجی پر لاگوُ ہوتا ہے جس میں انٹرنیٹ سے مُنسلک ٹی-وی، بےبی مانیٹرز، گھر کے راؤٹرز، گیمنگ کنسولز یا مستقبل قریب میں شاید آپ کی گاڑی بھی شامل ہو گی- اگر آپ کے آپریٹنگ سسٹمز یا آلات پُرانے ہیں اور وہ سکیورٹی کی جدید ترین اپڈیٹس حاصل کرنے سے قاصر ہیں تو ہمارا مشورہ ہے کہ آپ اُنھیں اُن نئے آپریٹنگ سسٹمز یا آلات سے تبدیل کر دیں جو کسی بھی نئی اپڈیٹ کو حاصل کرنے کی صلاحیت رکھتے ہوں-

محفوظ رہنے کے لیۓ چار اقدامات

۴. **بیک اپس**: بعض دفعہ ایسا ہوتا ہے کہ آپ جتنا بھی محتاط ہو جائیں، آپ ہیک ہو سکتے ہیں- اگر یہ صورتحال ہے تو اس میں آپ کو اپنے کمپیوٹر یا آلہ کو میلویئر سے بچانے کا اکثر صرف ایک ہی اختیار رہ جاتا ہے اور وہ یہ کہ آپ اُس کمپیوٹر یا آلہ کو مُکمّل طور پر وائپ کر دیں اور اُسے شرُوع سے بنائیں- ہو سکتا ہے کہ حملہ آور ہیک کۓ ہوۓ سسٹم سے آپ کو اپنی ذاتی فائلز، تصاویر اور دوُسری معلومات تک رسائی سے بھی روک دے- اکثر اپنی تمام ذاتی معلومات کو ری-اسٹور کرنے کا واحد طریقہ اپنی معلومات کا بیک-اپ لینا ہوتا ہے- آپ اِس بات کو یقینی بنائیں کہ آپ باقاعدگی سے تمام اہم معلوُمات کا بیک-اپ لیتے رہیں اور اُسے ری-اِسٹور کر کے اُس کی توثیق کرتے رہیں- زیادہ تر آپریٹنگ سِسٹمز اور موبائل آلات خوُدکار بیک-اپس کی حمایت کرتے ہیں- اِس کے علاوہ ہمارا مشورہ ہے کہ آپ اپنے بیک-اپس کو کلاؤڈ پر یا آف-لائن اسٹور کریں تاکہ سائبر حملہ آوروں سے بچا جا سکے-

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:

فشنگ: https://securingthehuman.sans.org/ouch/2015#december2015

پاس ورڈ مینیجرز: https://securingthehuman.sans.org/ouch/2015#october2015

ُو-اسٹیپ ویریفیکیشن: https://securingthehuman.sans.org/ouch/2015#september2015

پاس فریزز: https://securingthehuman.sans.org/ouch/2015#april2015

بیک اپس: https://securingthehuman.sans.org/ouch/2015#august2015

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

ترجمہ: شعیب ہاشمی