تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- پانچ آسان اقدامات
- دوسروں کے گھر جا کر اپنے بچّوں کی حفاظت کرنا

دوُسروں کو اُن کی حفاظت میں مدد فراہم کرنا

جائزہ

ہم میں سے کئی لوگ ٹیکنالوجی کے محفوظ استعمال سے کافی آرامدہ محسوس کرتے ہیں- تاہم ہو سکتا ہے کہ آپ کے خاندان کے باقی افراد اتنا آرامدہ محسوس نہ کریں- درحقیقت ہو سکتا ہے کہ وہ اس سے متعلق کچھ الجھن کا شکار ہوں، ڈرے ہوئے ہوں یا شاید اس سے خوفزدہ ہوں- اس طرح ان لوگوں کے آج کل کے سائبر حملہ آوروں کا نشانہ بننے کے امکانات بڑھ جاتے ہیں- سائبر سکیورٹی کو ڈراونا نہیں ہونا چاہیئے، اگر آپ بنیادی باتوں کو سمجھیں گے تو یہ کافی آسان لگے گا- اکثر اوقات انہیں آپ جیسے رہبر کی رہنمائی چاہیئے ہوتی ہے جو کہ انہیں بنیادی باتیں سمجھنے میں مدد فراہم کرے-

مہمان ایڈیٹر

رینڈی مارچینی (ٹوئیٹر: **@randymarchany**) ورجینیا ٹیک کے سیسو (CISO) اور SANS انسٹیٹیوٹ میں سرٹیفائیڈ انسٹرکٹر ہیں-

پانچ آسان اقدامات

آپ مندرجہ ذیل پانچ آسان اقدامات کو اپنا کر دوسروں کو ان کے خوف سے نجات دلا سکتے ہیں تاکہ وہ جدید ٹیکنالوجی کا محفوظ اور احسن طریقے سے استعمال کر سکیں- ان تمام اقدامات سے متعلق مزید معلومات کے لیئے آپ اس نیوز لیٹر کے آخری حصّے ‹وسائل› کو رجوع کریں-

۱. **سوشل انجینئرنگ**: سوشل انجینئرنگ ایک عام تکنیک ہے جو کہ سائبر حملہ آور استعمال کرتے ہیں لوگوں کو دھوکہ دہی یا بیوقوف بنا کر ایسے کام کروانے کے لیئے جو کہ آپ کو نہیں کرنے چاہیئے جیسے کہ اپنے پاس ورڈ کا اشتراک کرنا، کمپیوٹر کو متاثر کرنا یا حسّاس معلومات کا اشتراک کرنا- یہ کوئی نئی چیز نہیں ہے، جعلساز اور دھوکےباز لوگ ہزاروں سالوں سے موجود ہیں- فرق صرف اتنا ہے کہ اب برے لوگ ان چیزوں کا اطلاق انٹرنیٹ پر کر رہے ہیں- آپ دوسروں کی مدد اس طرح سے کر سکتے ہیں کہ آپ انہیں سوشل انجینئرنگ حملوں کی سب سے عام علامات کے بارے میں بتائیں جیسے کہ اگر کوئی کسی کام کے لیئے بہت عجلت کا احساس دلا رہا ہو، جب کوئی ایسی بات بتا رہا ہو جو آپ کو نا قابل یقین لگ رہی ہو یا جب کوئی سائبر حملہ آور آپ کے سامنے آپ کا کوئی جاننے والا بن کر بات کر رہا ہوں لیکن اس کے پیغامات سے بالکل بھی نہیں لگ رہا ہو کہ یہ وہی شخص ہے- آپ ان کے ساتھ سوشل انجینئرنگ حملوں کی مثالوں کا اشتراک کریں جیسے کہ فشنگ ای میلز یا مشہور زمانہ مائیکروسافٹ کی ٹیکنیکل سپورٹ کی فون کالز- اگر کچھ اور نہیں تو کم از کم اس بات کو یقینی بنائیں کہ آپ کے گھر والے اس بات کو اچھّی طرح سے سمجھ جائیں کہ انہیں اپنا پاس ورڈ کسی کو نہیں دینا یا کسی کو کہیں باہر سے اپنے کمپیوٹر تک رسائی نہیں دینی ہے-

۲. **پاس ورڈز**: مضبوط پاس ورڈز اپنے آلات اور آن لائن اکاؤنٹس، دونوں کی حفاظت کا سب سے اہم ذریعہ ہیں- آپ اپنے خاندان کے افراد کو مضبوط پاس ورڈز بنانے کا طریقہ بتائیں- ہمارا مشورہ ہے کہ آپ پاس ورڈ کے لیئے پاس فریزیز کا استعمال کریں کیونکہ انہیں لکھنا اور یاد رکھنا بہت ہی آسان ہے- پاس فریزیز مختلف الفاظ سے مل کر بنے پاس ورڈز ہوتے ہیں- اس کے علاوہ آپ پاس ورڈ مینیجر انسٹال کرنے اور استعمال کرنے میں ان کی مدد کریں-

دوُسروں کو اُن کی حفاظت میں مدد فراہم کرنا

آپ ان پانچ آسان اقدامات کے ذریعے دوسروں کو ٹیکنالوجی کے بہترین اور محفوظ استعمال میں مدد کر سکتے ہیں-

یہاں یہ بات اہم ہے کہ آپ اپنے تمام آلات اور اکاؤنٹس کے لیۓ منفرد پاس ورڈ بنائیں- اگر ان کے لیۓ پاس ورڈ مینیجر کا استعمال مشکل ہے تو آپ انہیں اپنے پاس ورڈز کو کسی جگہ پر لکھنا اور اسے محفوظ جگہ پر ذخیرہ کرنا سکھائیں- آخری بات یہ کہ اپنے اہم اکاؤنٹس کے لیۓ آپ ٹو اسٹیپ ویریفیکیشن (جو کہ ٹو فیکٹر آتھنٹیکیشن بھی کہلاتی ہے) کو فعّال کر دیں- ٹو اسٹیپ ویریفیکیشن اپنے اکاؤنٹس کو محفوظ رکھنے کے سب سے مؤثر ترین طریقوں میں سے ایک ہے-

۳. **پیچنگ**: اپنے سسٹمز کو تازہ ترین اور مکمّل اپڈیٹ رکھنا اپنے آلات کو محفوظ رکھنے کے بنیادی طریقوں میں سے ایک ہے- اس کا اطلاق صرف کمپیوٹرز اور موبائل آلات پر ہی نہیں ہوتا بلکہ ان تمام آلات پر ہوتا ہے جو کہ انٹرنیٹ سے منسلک ہوتے ہیں جیسے کہ گیمنگ کنسولز، تھرما میٹرز اور شاید لائٹس اور اسپیکرز بھی- اس بات کو یقینی بنانے کا سب سے آسان طریقہ خودکار اپڈیٹنگ کو فعّال کرنا ہے-

۴. **اینٹی وائرس**: لوگوں سے غلطیاں سرزد ہو جاتی ہیں، ہم کبھی کبھی ایسے لنکس پر کلک کر دیتے ہیں یا ایسی چیزیں انسٹال کر دیتے ہیں جو کہ ہمارے سسٹمز کو متاثر کر سکتی ہیں جو کہ ہمیں نہیں کرنی چاہیۓ- اینٹی وائرس کو ہماری ان غلطیوں سے حفاظت کے لیئے ڈیزائن کیا گیا ہے- اینٹی وائرس حالانکہ تمام میلویئر کو نہیں روک سکتا ہے لیکن یہ سب سے عام حملوں کا پتہ لگانے اور انہیں روکنے میں مدد گار ثابت ہوتا ہے- آپ اس بات کو یقینی بنائیں کہ آپ کے گھر کے کمپیوٹرز میں اینٹی وائرس انسٹال ہے اور اس کا موجودہ ورژن چل رہا ہے اور یہ بھی کہ وہ فعّال ہے- مزید یہ کہ آج کل کے اینٹی وائرس سولیوشنز میں کچھ اور سکیورٹی ٹیکنالوجی بھی موجود ہوتی ہے جیسے کہ فائر والز اور براؤزر پروٹیکشن-

۵. **بیک اپس**: جب سب کچھ ناکام ہو جاتا ہے تو بیک اپس ہی وہ واحد طریقہ رہ جاتا ہے جس کے ذریعے آپ اپنی غلطیوں یا سائبر حملوں، جیسے کہ رینسم ویئر، سے ریکوؤر کر سکتے ہیں- آپ اس بات کو یقینی بنائیں کہ آپ کے گھر والوں اور دوستوں کے پاس خودکار بیک اپ سسٹم موجود ہے- اکثر کلاؤڈ پر آسان ترین حل موجود ہوتے ہیں جو کہ آپ کے آلات کا ہر گھنٹے یا جب بھی آپ کسی فائل میں تبدیلی کرتے ہیں، اس کا بیک اپ لے لیتے ہیں- یہ حل نہ صرف معلومات کا بیک اپ لینا آسان بنا دیتے ہیں بلکہ انہیں ریکوؤر کرنا بھی آسان بنا دیتے ہیں-

دوسروں کے گھر جا کر بچّوں کی حفاظت کرنا

اگر آپ ٹیکنالوجی سے مطمئن ہیں تو اس بات کا قوی امکان ہے کہ آپ نے نہ صرف اپنی حفاظت کی ہے بلکہ اپنے بچّوں کی بھی حفاظت میں ان کی مدد کی ہے- تاہم جب بچّے کسی ایسے رشتے دار یا دوست کی طرف جاتے ہیں جو کہ خود اس ٹیکنالوجی سے مطمئن نہیں ہیں، جیسے کہ دادا، دادی، نانا، نانی، تو ہو سکتا ہے کہ یہ لوگ بچّوں کی بہترین حفاظت سے متعلق آپ کی توقّع پر پورا نہ اتریں-

- **قواعد و ضوابط**: آپ اس بات کو یقینی بنائیں کہ اگر آپ نے بچّوں کے لیئے سکیورٹی سے متعلق کوئی قواعد و ضوابط بنائے ہیں یا آپ کی ان سے کچھ توقّعات ہیں تو دوسروں کو بھی ان کے بارے میں پتہ ہو- مثال کے طور پر کیا کوئی ایسا اصول ہے جو یہ بیان کرے کہ بچّے کتنی دیر آن لائن رہ سکتے ہیں، کس سے بات کر سکتے ہیں یا کون سی گیمز کھیل سکتے ہیں یا نہیں کھل سکتے ہیں؟ آپ اس بات پر ہمارا بھروسہ

دوُسروں کو اُن کی حفاظت میں مدد فراہم کرنا

کریں کہ آپ بچّوں پر آسرہ نہیں کریں کہ وہ رشتےداروں کو یہ قواعد و ضوابط سمجھائیں گے- ایک طریقہ یہ ہے کہ آپ قواعد و ضوابط کی ایک شیٹ بنا دیں اور اس کا اشتراک ان رشتےداروں سے کر دیں جن کے ہاں بچّے زیادہ جاتے ہیں-

- **کنٹرول**: اگر کوئی بچّہ ٹیکنالوجی کو اپنے سرپرستوں سے زیادہ بہتر سمجھتا ہے تو ہو سکتا ہے کہ وہ اس کا فائدہ اٹھائے- مثال کے طور پر بچّے اپنے دادا، دادی کے کمپیوٹر کے ایڈمنسٹریٹو حقوق مانگ سکتے ہیں اور پھر اس کے بعد وہ جو چاہیں کر سکتے ہیں جیسے کہ کوئی ایسی گیم انسٹال کر سکتے ہیں جسے آپ نہیں چاہتے ہیں کہ وہ کھیلیں- آپ اس بات کو یقینی بنائیں کہ آپ کے رشتےدار اس بات کو سمجھتے ہوں کہ انہیں آپ کے بچّوں کو قائم شدہ حقوق سے زیادہ اختیار نہیں دینا ہے-

آخری بات یہ کہ آپ لوگوں کو OUCH! نیوز لیٹر جیسے وسائل کو سبسکرائب کرنے کی تجویز دیں تاکہ وہ اپنے طور پر چیزیں سیکھتے رہیں- یہ نیوز لیٹر ہر مہینے ۲۰ زبانوں میں شائع ہوتا ہے- آپ https://securingthehuman.sans.org/ouch کے ذریعے سائن اپ کر سکتے ہیں-

مزید جانیئے

آخری بات یہ کہ آپ لوگوں کو OUCH! نیوز لیٹر جیسے وسائل کو سبسکرائب کرنے کی تجویز دیں تاکہ وہ اپنے طور پر چیزیں سیکھتے رہیں- یہ نیوز لیٹر ہر مہینے ۲۰ زبانوں میں شائع ہوتا ہے- آپ securingthehuman.sans.org/ouch/archives کے ذریعے سائن اپ کر سکتے ہیں-

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

پاس فریزیز: https://securingthehuman.sans.org/ouch/2017#april2017

پاس ورڈ مینیجر: https://securingthehuman.sans.org/ouch/2017#september2017

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

بیک اپ اور ریکؤری: https://securingthehuman.sans.org/ouch/2017#august2017

آج کل کے آن لائن بچّوں کی حفاظت کرنا: https://securingthehuman.sans.org/ouch/2017#may2017

ترجمہ: شعیب ہاشمی

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