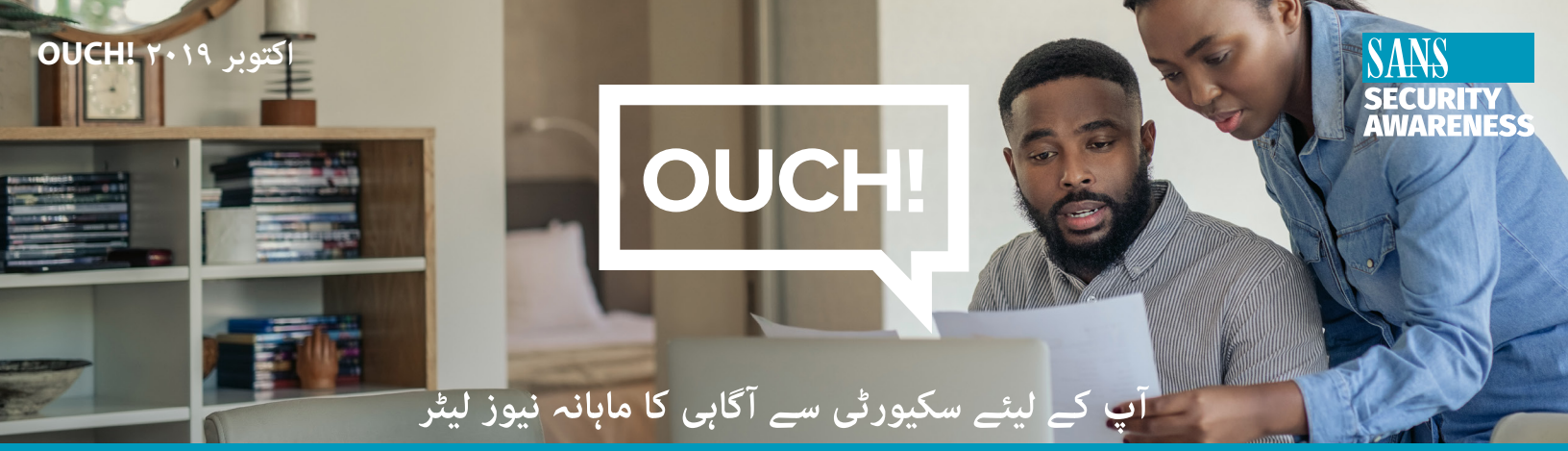

SANS SECURITY AWARENESS

OUCH!

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

محفوظ رہنے کے چار آسان طریقے

جائزہ

ٹیکنالوجی کا زیادہ سے زیادہ اور محفوظ استعمال مشکل اور مبہم ہو سکتا ہے- تاہم اس بات سے قطع نظر کہ آپ کون سی ٹیکنالوجی استعمال کر رہے ہیں یا کیسے استعمال کر رہے ہیں، آپ مندرجہ ذیل چار آسان اقدامات اپنا کر اپنے آپ کو محفوظ رکھ سکتے ہیں-

۱- آپ: اس بات کو آپ اچھی طرح سے ذہن نشین کر لیں کہ صرف ٹیکنالوجی آپ کی مکمّل طور پر حفاظت نہیں کر سکتی ہے اور سب سے بہترین دفاع آپ خود ہی ہیں- حملہ آوروں کو یہ بات معلوم ہے کہ انہیں ان کے مطلب کی معلومات حاصل کرنے کے لیئے سب سے آسان طریقہ آپ کو ہدف بنانا ہے نہ کہ آپ کے کمپیوٹر یا دوسرے آلات کو- اگر اُنہیں آپ کا پاس ورڈ، کریڈٹ کارڈ نمبر یا آپ کے کمپیوٹر تک رسائی حاصل کرنی ہے تو وہ کوشش کریں گے کہ آپ کو عُجلت کا احساس دلا کر اور دھوکہ دہی کے ذریعے معلومات نکلوا لیں- مثال کے طور پر وہ آپ کو مائیکروسافٹ کی ٹیکنیکل سپورٹ کا نمائندہ بن کر کال کر سکتے ہیں اور یہ دعوہ کر سکتے ہیں کہ آپ کا کمپیوٹر وائرس سے متاثر ہو چکا ہے، جبکہ حقیقت میں وہ سائبر مُجرمان ہوتے ہیں جن کا ہدف آپ کے ذریعے آپ کے کمپیوٹر تک رسائی حاصل کرنا ہوتا ہے- یہ بھی ہو سکتا ہے کہ وہ آپ کو ای میل کے ذریعے مُتنبّہ کریں کہ آپ کا بھیجا ہوا سامان اپنی منزل تک نہیں پہنچ سکا اس لیئے آپ ای میل میں فراہم کردہ لنک کے ذریعے اپنے ڈاک کے پتے کی تصدیق کریں- درحقیقت وہ آپ کو بیوقوف بنا کر آپ کو ایک وائرس سے متاثرہ ویب سائٹ پر جانے کا کہہ رہے ہوتے ہیں تاکہ وہ آپ کے کمپیوٹر کو ہیک کر سکیں- بلآخر ان حملہ آوروں کے خلاف آپ خود ہی سب سے بہترین دفاع ہیں- آپ اپنی عقل سلیم استعمال کرتے ہوئے اس طرح کے حملوں کی شناخت کر سکتے ہیں اور اُن سے بچ سکتے ہیں-

۲- پاس فریزیز: جدید کمپیوٹنگ کی رفتار نے آٹھ حُروف پر مشتمل پاس ورڈ کو فرسودہ اور کمزور بنا دیا ہے- جب کوئی سائٹ آپ کو پاس ورڈ بنانے کے لیئے کہتی ہے تو آپ کو چاہیئے کہ آپ ایک مضبوط اور مُنفرد پاس ورڈ بنائیں- پاس فریز، پاس ورڈ کی ایسی قسم ہے جس میں الفاظ کا ایسا سلسلہ (جُملہ) استعمال ہوتا ہے جسے یاد رکھنا آسان ہوتا ہے، جیسے کہ «bee honey bourbon rain»- آپ کا پاس فریز (جُملہ) جتنا طویل ہو گا، اتنا ہی مضبوط ہو گا- ایک منفرد پاس فریز کا مطلب ہے کہ آپ اپنے ہر آلہ یا آن لائن اکاؤنٹ کے لیئے مختلف پاس ورڈ استعمال کرتے ہیں- اس طرح اگر آپ کا ایک پاس فریز کسی کے ہاتھ لگ بھی جاتا ہے تو آپ کے باقی تمام اکاؤنٹس اور آلات محفوظ رہتے ہیں- کیا آپ اپنے تمام پاس فریزز یاد نہیں رکھ سکتے ہیں؟ اس صورت میں آپ پاس ورڈ مینیجر کا استعمال کریں، جو کہ آپ کے تمام پاس فریزیز کو محفوظ طریقے سے انکرپٹڈ شکل میں ذخیرہ کرنے کا ایک خصوصی پروگرام ہے (اس کے علاوہ بھی مزید بہت زبردست خصوصیات شامل ہوتی ہیں)-

ایک اور اہم قدم آپ یہ اٹھا سکتے ہیں کہ آپ ٹُواسٹیپ ویریفیکیشن (جو کہ ٹُو فیکٹر یا ملٹی فیکٹر اوتھنٹیکیشن بھی کہلاتا ہے) کو فعّال کر دیں- یعنی اس طرح آپ کے پاس کسی اکاؤنٹ میں لاگ اِن ہونے کے لیئے دو عنصر درکار ہوتے ہیں،پہلا عنصر پاس ورڈ ہوتا ہے اور

دوسرہ عنصر آپ کے اسمارٹ فون پر بھیجا گیا کوڈ یا کسی مخصوص ایپلیکیشن کے ذریعے نکالا گیا کوڈ- ٹو اسٹیپ ویریفیکیشن کو فعّال کرنا اپنے آن لائن اکاؤنٹس کی حفاظت کا سب سے اہم ترین قدم ہے اور اس کا استعمال آپ کی سوچ سے بھی زیادہ آسان ہے-

۳- اپڈیٹ کرنا: آپ اس بات کی یقین دہانی کر لیں کہ آپ کے ہر کمپیوٹر، ہر موبائل آلہ، ہر پروگرام اور ایپلیکیشن میں سافٹ ویئر کا جدید ترین ورژن چل رہا ہے- سائبر حملہ آور آپ کے استعمال میں موجود آلات کے سافٹ ویئر میں مسلسل نئی کمزوریاں تلاش کرتے رہتے ہیں- جب بھی انہیں نئی کمزوریاں نظر آتی ہیں تو وہ مخصوص پروگرامز کے ذریعے آپ کے آلات کو ہیک کرنے کی کوشش کرتے ہیں- دوسری طرف آپ کے آلات میں موجود سافٹ ویئرز بنانے والی کمپنیز مسلسل ان کمزوریوں کی تصحیح کرنے کی کوشش کرتی رہتی ہیں اور ان سے متعلق اپڈیٹس جاری کرتی رہتی ہیں- ان اپڈیٹس کو فوری طور پر اپنے کمپیوٹرز اور موبائل آلات میں انسٹال کرنے سے کسی کے لیئے بھی آپ کو ہیک کرنا بہت مشکل ہو جاتا ہے- تازہ ترین اپڈیٹس حاصل کرنے کا سب سے آسان طریقہ خودکار اپڈیٹ کو فعّال کرنا ہے- یہ اصول نیٹ ورک سے منسلک ہر ٹیکنالوجی پر لاگو ہوتا ہے جس میں انٹرنیٹ سے منسلک ٹی وی، بےبی مانیٹرز، سکیورٹی کمرہ، گھر کے راؤٹر، گیمنگ کنسولز اور ممکنہ طور پر آپ کی گاڑی بھی شامل ہے-

٤- بیک اپ اور ریکوری: بعض اوقات ایسا ہوتا ہے کہ آپ جتنی مرضی احتیاط کر لیں آپ ہیک ہو جاتے ہیں- اس صورتحال میں آپ کے لیئے اپنی ذاتی معلومات تک رسائی حاصل کرنے کا واحد طریقہ بیک اپ کے ذریعے انہیں ری اسٹور کرنا رہ جاتا ہے- اس لیئے آپ اہم معلومات کا باقاعدگی سے بیک اپ لیتے رہا کریں اور اس بات کی بھی تصدیق کر لیا کریں کہ آپ اس بیک اپ کے ذریعے ان اہم معلومات کو ری اسٹور کر سکتے ہیں- زیادہ تر آپریٹنگ سسٹمز اور موبائل آلات میں خودکار طور پر ایکسٹرنل ڈرائیو یا کلاؤڈ پر بیک اپس لینے کی سہولت موجود ہوتی ہے-

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۔

مہمان مُدیر

اسٹیو اینسن SANS کے سند یافتہ انسٹرکٹر ہیں اور دنیا بھر کی آئی ٹی سکیورٹی ٹیمز اور حکومتوں کو سکیورٹی بہتر بنانے سے متعلق تربیت فراہم کرتے ہیں- اسٹیو ایک کتاب لکھ رہے ہیں جس کا عنوان ہے «اپلائڈ انسیڈنٹ رسپانس»- اس کے علاوہ وہ سکیورٹی کے پیشہ وروں کے لیئے www.AppliedIncidentResponse.com مفت وسائل بھی فراہم کرتے ہیں-

وسائل:

سوشل انجینئرنگ: https://www.sans.org/u/W3G
مخصوص ذاتی جعلسازی: https://www.sans.org/u/W3Q
پاس ورڈز کو آسان بنانا: https://www.sans.org/u/W3V
کیا آپ کے پاس بیک اپ موجود ہے؟: https://www.sans.org/u/W40