نومبر ۲۰۱۴ OUCH!

کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- سوشل انجینئرنگ
- سوشل انجینئرنگ حملوں کی نشاندہی کرنا / روکنا
- مستقبل کے حملوں سے بچنا

سوشل انجینئرنگ

جائزہ

لوگوں کو ایک عام غلط فہمی سائبر حملہ آوروں کے بارے میں یہ ہے کہ وہ لوگوں کے کمپیوٹرز، اکاؤنٹس اور موبائل آلات میں گھسنے کے لیے صرف اعلیٰ درجے کے ہیکنگ ٹولز کا استعمال کرتے ہیں، اس میں سچائی نہیں ہے۔ سائبر حملہ آوروں نے آپ کی معلومات چرانے یا کمپیوٹر ہیک کرنے کا آسان طریقہ آپ سے بات چیت کرکے آپ کو گمراہ کرنا نکالا ہے۔ اس شمارے میں ہم یہ سیکھیں گے کہ کس طرح انسانی حملے، جو کہ سوشل انجینئرنگ حملے کہلاتے ہیں، کیسے کام کرتے ہیں اور آپ کن احتیاطی تدابیر کو اپنا کر خود کو ان سے محفوظ رکھ سکتے ہیں۔

مہمان ایڈیٹر

ایلیسا ٹوریس SANSکی سند یافتہ انسٹرکٹر ہیں- وہ ایڈوانسڈ کمپیوٹر فارنزکس اور انسیڈینٹ رسپانس میں مہارت رکھتی ہیں۔ ان کے صنعت کے تجربے میں انسیڈینٹ ہینڈلر کے طور پر اور ایک داخلی سکیورٹی ٹیم میں ڈیجیٹل فارنزک انویسٹی گیٹر کے طور پر خدمت سر انجام دینا شامل ہے۔ آپ ایلیسا کو ٹوئیٹر پر **@sibertor** کے ذریعے ڈھونڈ سکتے ہیں۔

سوشل انجینئرنگ

سوشل انجینئرنگ، نفسیاتی حملے کی ایک قسم ہے جس میں حملہ آور آپ کو دھوکہ دہی کے ذریعے ایسے کام کروانے کی کوشش کرتا ہے جنہیں وہ آپ کے ذریعے کروانا چاہتا ہے۔ سوشل انجینئرنگ کا وجود ہزاروں سال پرانا ہے، کسی کو دھوکہ دینا کوئی نیا تصور نہیں ہے لیکن سائبر حملہ آوروں نے یہ سیکھ لیا ہے کہ انٹرنیٹ پر اس طریقۂ کار کو اپنانا انتہائی مؤثر ہے اور لاکھوں لوگوں کو ہدف بنانے کے لیے استعمال ہوسکتا ہے۔ سوشل انجینئرنگ کام کس طرح کرتی ہے، یہ سمجھنے کیلئے سب سے آسان ترین طریقہ یہ حقیقی دنیا کی عام مثال ہے۔

آپ کو کسی شخص سے ایک فون کال موصول ہوتی ہے جو کہ کسی کمپیوٹر سپورٹ کمپنی، آپ کی آئی۔ایس۔پی یا شاید مائیکروسافٹ کی ٹیکنیکل سپورٹ کا نمائندہ ہونے کا دعویٰ کرتا ہے- وہ شخص وضاحت کرتے ہوئے بتاتا ہے کہ اُس نے یہ بات محسوس کی ہے کہ آپ کا کمپیوٹر کچھ عجیب برتاؤ کررہا ہے جیسے کہ انٹرنیٹ کو اسکین کرنا یا اسپیم بھیجنا اور یہ کہ اُس کے خیال میں آپ کا کمپیوٹر متاثر ہوچکا ہے- وہ مزید بتاتا ہے کہ اُسے اس مسئلے کی تفتیش اور آپ کے کمپیوٹر کو محفوظ بنانے کا کام سونپا گیا ہے- اُس کے بعد وہ کئی تکنیکی اصطلاحات کا استعمال کرتا ہے اور آپ کو الجھانے والے اقدامات کے ذریعے قائل کرنے کی کوشش کرتا ہے کہ آپ کا کمپیوٹر متاثر ہوچکا ہے۔

مثال کے طور پر وہ آپ کے کمپیوٹر میں کچھ مخصوص فائلز کی جانچ کرنے کا کہہ سکتے ہیں یہ دیکھنے کے لیے کہ آیا وہ فائلز آپ کے کمپیوٹر میں موجود ہیں کہ نہیں اور وہ آپ کو اُنہیں ڈھونڈنے کا طریقہ بھی بتاتے ہیں- جب آپ اُن فائلز کو ڈھونڈ لیتے ہیں تو وہ آپ کو یقین دلاتے ہیں کہ یہ فائلز اس بات کی نشاندہی کرتی ہیں کہ آپ کا کمپیوٹر متاثر ہوچکا ہے جبکہ حقیقت میں یہ فائلز عام سسٹم فائلز سے زیادہ کچھ بھی نہیں ہوتی ہیں جو کہ ہر کمپیوٹر میں پائی جاتی ہیں- ایک بار جب وہ آپ کو دھوکہ دے کر یہ یقین دلانے میں کامیاب ہوجائیں کہ آپ کا کمپیوٹر متاثر ہوگیا ہے تو پھر وہ آپ پر دباؤ ڈالیں گے کہ آپ ایک ویب سائٹ پر جاکر اُن کا سکیورٹی سافٹ ویئر خریدیں یا وہ آپ کے کمپیوٹر کا ریموٹ ایکسس مانگیں گے تاکہ وہ اس مسئلے کو خود حل کرسکیں تاہم جو سافٹ ویئر وہ بیچ رہے ہیں وہ درحقیقت ایک متاثرہ پروگرام ہے۔ اگر آپ اس سافٹ ویئر

سوشل انجینئرنگ

کو خریدتے اور انسٹال کرتے ہیں تو نہ صرف یہ کہ وہ آپ کو بے وقوف بناکر آپ کا اپنا کمپیوٹر متاثر کروادیتے ہیں بلکہ آپ اُنہیں اس کام کے پیسے بھی دیتے ہیں- اگر آپ اپنے کمپیوٹر کو صحیح کروانے کے لیے اُنہیں ریموٹ ایکسس فراہم کرتے ہیں تو درحقیقت وہ اُسکے ذریعے آپکے کمپیوٹر کو متاثر کردیتے ہیں ۔

اس بات کو ذہن میں رکھیں کہ سوشل انجینئرنگ حملے صرف فون کالز تک محدود نہیں ہیں بلکہ وہ کسی بھی ٹیکنالوجی کے ذریعے ہوسکتے ہیں جس میں ای میل کے ذریعے فشنگ حملے، ٹیکسٹ میسیجنگ، فیس بک میسیجنگ، ٹوئیٹر پرپوسٹ یا آن لائن چیٹس شامل ہیں- سب سے اہم چیز یہ ہے کہ آپ کو یہ معلوم ہونا چاہیے کہ آپ کو کس چیز سے بچنا ہے۔

اپنے آپ کو سوشل انجینئرنگ حملوں سے محفوظ رکھنے کے لیے اُن سے بچنے، اُن کی نشاندہی کرنے اور اُنہیں روکنے کے بارے میں سیکھنا مؤثر ترین اقدامات میں سے ایک ہے۔

سوشل انجینئرنگ حملوں کی نشاندہی کرنا / روکنا

سوشل انجینئرنگ سے بچنے کا آسان ترین طریقہ اپنی عقل کا استعمال کرنا ہے- اگر آپ کو کوئی چیز مشتبہ لگ رہی ہو یا صحیح نہیں لگ رہی ہو تو ہوسکتا ہے کہ یہ ایک حملہ ہو- سوشل انجینئرنگ حملے کی چند نشانیاں درجہ ذیل ہیں۔

- کوئی شخص شدید جلد بازی کا احساس پیدا کررہا ہو- اگر آپ کو لگے کہ آپ پر فوری فیصلہ کرنے کا دباؤ ہے تو آپ مشتبہ ہوجائیں ۔
- کوئی آپ سے ایسی معلومات کے بارے میں پوچھ رہا ہے جس کی رسائی اُس تک نہیں ہونی چاہیئے یا اُنہیں اُس کا علم پہلے سے ہونا چاہیئے۔
- کوئی ایسی بات بتائی جارہی ہو کہ وہ سچ نہیں لگ رہی ہو- ایک عام مثال یہ ہے کہ آپ کو مطلع کیا جاتا ہے کہ آپنے لاٹری جیت لی ہے حالانکہ آپنے کبھی اُس میں حصہ ہی نہیں لیا ہو۔

اگر آپ کو لگ رہا ہے کہ آپ کو کوئی سوشل انجینئرنگ حملے کا نشانہ بنا رہا ہے تو آپ اُس شخص سے مزید بات چیت نہیں کریں- اگر کوئی آپ کو فون کال کررہا ہے تو کال کو منقطع کردیں- اگر کوئی آپ سے آن لائن چیٹ کررہا ہے تو آپ اُس کنیکشن کو منقطع کردیں- اگر وہ کوئی ای میل ہے جس پر آپ بھروسہ نہیں کرتے ہیں تو آپ اسے ڈیلیٹ کردیں۔ اگر حملہ آپکے دفتر سے متعلق ہے تو آپ اس بات کی تاکید کرلیں کہ آپ اُس کی اطلاع فوراً اپنے ہیلپ ڈیسک یا انفارمیشن سکیورٹی ٹیم کو کریں-

مستقبل کے سوشل انجینئرنگ حملوں سے بچنا

خوش قسمتی سے کچھ ایسی احتیاطی تدابیر ہیں جن کو اختیار کرکے آپ اپنے آپ کو مستقبل کے سوشل انجینئرنگ حملوں سے بچا سکتے ہیں۔

- **پاس ورڈ کا اشتراک کبھی بھی نہیں کریں:** آپ کو کبھی بھی کوئی تنظیم آپ کا پاس ورڈ پوچھنے کے لیے رابطہ نہیں کرے گی اگر کوئی آپ سے پاس ورڈ پوچھ رہا ہے تو آپ سمجھ جائیں کہ یہ ایک حملہ ہے۔

سوشل انجینئرنگ

- **زیادہ معلومات کا اشتراک نہیں کریں:** حملہ آور کو آپ کے بارے میں جتنی معلومات ہوں گی اتنا ہی اُس کے لیے آپ کو ڈھونڈنا اور اپنی مرضی کے مطابق گمراہ کرنا آسان ہوگا۔ یہاں تک کہ آپ کا چھوٹی سے چھوٹی ذاتی معلومات کا وقتاً فوقتاً اشتراک، آپ کے بارے میں مکمل خاکہ پیش کرسکتا ہے- آپ جتنی کم معلومات کا عوامی اشتراک کریں گے جس میں سوشل میڈیا سائیٹس، مصنوعات کے جائزے یا عوامی فورمز اور میل لسٹس شامل ہیں، آپ پر حملے کے امکانات اُتنے ہی کم ہوں گے۔

- **کانٹیکٹس کی تصدیق کرنا:** بعض دفعہ آپ کو اپنے بینک، کریڈٹ کارڈ کمپنی، موبائل سروس پرووائیڈر یا دوسری تنظیموں کی جانب سے جائز وجوہات کی بناءپر بُلایا جاسکتا ہے- اگرآپ کو ذرا سا بھی شک ہو کہ آیا آپ سے کی گئی معلومات کی درخواست جائز ہے یا نہیں تو آپ اُس درخواست گزار سے اُس کا نام اور فون کا ایکسٹینشن نمبر پوچھ سکتے ہیں- پھر آپ اُس تنظیم کے فون نمبر کا کسی قابلِ اعتماد ذریعے سے معلوم کریں جیسے کہ وہ نمبر جو آپ کے کریڈٹ کارڈ کے پیچھے لکھا ہے، وہ نمبر جو آپ کی بینک اسٹیٹمنٹ پر لکھا ہے یا شاید وہ نمبر جو کمپنی کی ویب سائٹ پر لکھا ہے (اس بات کی تاکید کرلیں کہ اُس ویب سائٹ کا URL آپ اپنے براؤزر میں خود لکھیں) اس طرح جب آپ اُس تنظیم کو کال کرتے ہیں تو آپ کو معلوم ہوتا ہے کہ آپ حقیقت میں اُن ہی سے بات کررہے ہیں- اگرچہ یہ ایک رکاوٹ لگتی ہے لیکن اپنی شناخت اور ذاتی معلومات کی حفاظت کے لیے یہ اضافی قدم بہت اہمیت کا حامل 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 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

سوشل نیٹ ورکنگ کا محفوظ استعمال: http://www.securingthehuman.org/ouch/2013#march2013

دھوکے سے بچنا: http://www.onguardonline.gov/topics/avoid-scams

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

ترجمہ: شعیب ہاشمی