تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- سوشل انجینئرنگ کیا ہے؟
- سوشل انجینئرنگ حملوں کی شناخت کرنا / اُنہیں روکنا

سوشل انجینئرنگ

جائزہ

سائبر حملہ آوروں سے متعلق زیادہ تر لوگوں کو ایک عام غلط فہمی یہ ہے کہ وہ لوگوں کے کمپیوٹرز اور اکاؤنٹس ہیک کرنے کے لیئے صرف اعلیٰ درجے کے ٹولز اور تکنیک کا استعمال کرتے ہیں- یہ بات دُرست نہیں ہے- سائبر حملہ آوروں نے یہ بات جان لی ہے کہ آپ کی معلومات چوری کرنے، اکاؤنٹس ہیک کرنے یا آپ کے سسٹم کو متاثر کرنے کا سب سے آسان طریقہ لوگوں سے دھوکہ دہی کے ذریعے کوئی غلطی سرزد کروانا ہے- اس نیوز لیٹر میں آپ اِن حملوں، جو کہ سوشل انجینئرنگ کہلاتے ہیں، کے بارے میں جانیں گے کہ یہ کام کیسے کرتے ہیں اور اِن سے آپ اپنی حفاظت کیسے کر سکتے ہیں-

مہمان ایڈیٹر

جمیز لاین (**@jameslyne**)، SANS کے سندیافتہ انسٹرکٹر اور سوفوز میں تحقیق کے عالمی سربراہ ہیں- وہ سائبر مُجرمان کی جدید ترین تخلیقات کو ریورس انجینئر کرتے ہیں- وہ SANS میں ‹میٹااِسپلوائٹ› (SEC580) اور ‹سوشل انجینئرنگ› (SEC567) کے کورسز کے مُصنّف ہیں-

سوشل انجینئرنگ کیا ہے؟

سوشل انجینئرنگ ایک نفسیاتی حملہ ہے جس میں ایک حملہ آور آپ سے دھوکہ دہی کے ذریعے کوئی ایسا کام کروا دیتا ہے جو آپ کو نہیں کرنا چاہیئے- سوشل انجینئرنگ کا تصوّر نیا نہیں ہے، یہ ہزاروں سالوں سے موجود ہے- اس کا تصوّر بالکل ایک دھوکےباز یا دغاباز کی طرح ہے- سائبر حملہ آوروں کے لیئے آج کی ٹیکنالوجی اس لیئے زیادہ مؤثر ہے کیونکہ آپ انہیں جسمانی طور پر نہیں دیکھ سکتے ہیں، وہ با آسانی کوئی بھی بھیس بدل کر یا اپنی مرضی سے کوئی بھی بن کر، دنیا بھر میں لاکھوں لوگوں، جن میں آپ بھی شامل ہیں، کو نشانہ بنا سکتے ہیں- اس کے علاوہ سوشل انجینئرنگ حملے کئی سکیورٹی ٹیکنالوجیز کو پار کر سکتے ہیں- آپ ان حملوں کو باآسانی سمجھنے اور اپنے آپ کو محفوظ رکھنے کے لیئے ان دو مثالوں پر غور کریں-

آپ کو کسی کی فون کال آتی ہے اور وہ یہ کہتا ہے کہ وہ کسی کمپیوٹر سپورٹ کمپنی، ‹آئی ایس پی› یا شاید مائیکروسافٹ ٹیکنیکل سپورٹ سے بات کر رہا ہے- کالر آپ کو بتاتا ہے کہ آپ کا کمپیوٹر انٹرنیٹ پر متواتر اسکیننگ کر رہا ہے اور اُن کا خیال ہے کہ وہ متاثر ہو چکا ہے اور اسے آپ کے کمپیوٹر کو محفوظ بنانے کی ذمہ داری سونپی گئی ہے- پھر وہ مختلف تکنیکی اصطلاحات استعمال کر کے آپ کو مبہم اقدامات کے ذریعے اس بات پر قائل کرنے کی کوشش کرتا ہے کہ آپ کا کمپیوٹر متاثر ہو گیا ہے- مثال کے طور پر وہ آپ کو کمپیوٹر میں کچھ مخصوص فائلز تلاش کرنے کا کہہ سکتا ہے اور وہ آپ کو انہیں ڈھونڈنے میں مدد بھی کرے گا- جب آپ ان فائلز کو ڈھونڈ لیتے ہیں تو وہ کالر آپ کو اس بات پر آمادہ کرتا ہے کہ ان فائلز کا ملنا اس بات کو یقینی بناتا ہے کہ آپ کا کمپیوٹر متاثر ہو چکا ہے، جبکہ حقیقت میں یہ عام سسٹم فائلز ہوتی ہیں جو کہ دنیا کے ہر کمپیوٹر میں پائی جاتی ہیں- ایک بار جب وہ آپ کو اس بات کا یقین دلا دیتے ہیں کہ آپ کا کمپیوٹر متاثر ہو گیا ہے تو پھر وہ آپ پر اپنے سکیورٹی سافٹ ویئر کو خریدنے کے لیئے دباؤ ڈالتے ہیں یا اپنے کمپیوٹر کا ریموٹ ایکسیس فراہم کرنے کے لیئے کہتے ہیں تاکہ وہ اسے صحیح کر سکیں- تاہم جو سافٹ ویئر وہ آپ کو بیچ رہے ہیں وہ درحقیقت ایک مضر پروگرام ہے- اگر آپ اسے خریدتے اور انسٹال کرتے ہیں تو اس کا مطلب ہے کہ انہوں نے نہ صرف آپ کو بیوقوف بنا کر آپ کا کمپیوٹر مضر پروگرام

سوشل انجینئرنگ

سے متاثر کر دیا ہے بلکہ اس کام کے لیئے آپ نے انہیں پیسے بھی دیئے ہیں- اگر آپ انہیں اپنے کمپیوٹر کا ریموٹ ایکسیس فراہم کر دیتے ہیں تو وہ اس پر قابض ہو سکتے ہیں، اس میں سے معلومات چرا سکتے ہیں یا پھر اسے بولی لگانے کے لیئے استعمال کر سکتے ہیں-

سوشل انجینئرنگ حملوں کی شناخت اور انہیں روکنے کے لیئے عام فہم ہی آپ کا سب سے مضبوط دفاع ہے-

ایک اور مثال ای میل حملے کی ہے جو کہ ‹سی ای او فراڈ› کہلاتی ہے اور زیادہ تر دفتر میں رونما ہوتی ہے- یہ اس وقت ممکن ہوتا ہے جب ایک سائبر حملہ آور آپ کی تنظیم کے بارے میں آن لائن تحقیق کرتا ہے اور آپ کے افسر اور ساتھ کام کرنے والے لوگوں کے نام کی شناخت کرتا ہے- پھر یہ حملہ آور ان میں سے کوئی بھی فرد بن کر ایک ای میل تخلیق کرتا ہے اور آپ کو ارسال کرتا ہے- یہ ای میل آپ کو فوری اقدام اٹھانےکا کہتی ہے جیسے کہ آن لائن پیسے بھیجنا یا کسی ملازم کی حسّاس معلومات ای میل کرنا- اکثر اوقات یہ ای-میلز کسی ہنگامی صورتحال کا دکھاوا کرتی ہیں اور آپ کو تمام حفاظتی حصار کو پار کر کے فوری اقدامات اٹھانے کا کہتی ہیں- مثال کے طور پر یہ ای-میلز آپ سے یہ کہہ سکتی ہیں کہ آپ کوئی بہت ہی حسّاس معلومات کسی ذاتی @gmail.com اکاؤنٹ پر بھیج دیں- جو چیز ان مخصوص حملوں کو بہت خطرناک بناتی ہے وہ یہ ہے کہ سائبر حملہ آور اپنی تحقیق پہلے سے کر لیتے ہیں- اس کے علاوہ سکیورٹی ٹیکنالوجیز جیسے کہ اینٹی وائرس یا فائروال ان حملوں کی شناخت یا انہیں روک نہیں سکتے ہیں کیونکہ ان میں کوئی میلویئر یا مضر لنکس شامل نہیں ہوتے ہیں-

آپ ایک بات ذہن میں رکھیں کہ اس طرح کے سوشل انجینئرنگ حملے صرف فون کالز یا ای میل تک ہی محدود نہیں ہیں بلکہ یہ کسی بھی طریقے سے رونما ہو سکتے ہیں جس میں آپ کے فون کے ٹیکسٹ میسیجز، سوشل میڈیا یا کسی شخص کا بذات خود ہونا بھی شامل ہیں- یہاں اہم بات یہ ہے کہ آپ کو یہ پتہ ہونا چاہیئے کہ آپ کو کس چیز سے بچنا ہے کیونکہ آپ ہی اپنا بہترین دفاع ہیں-

سوشل انجینرنگ حملوں کی شناخت کرنا/ انہیں روکنا

خوش قسمتی سے ان حملوں کو روکنا آپ کی سوچ سے بھی زیادہ آسان ہے کیونکہ عام فہم ہی آپ کا بہترین دفاع ہے- اگر آپ کو کوئی چیز مشکوک لگ رہی ہو یا کچھ صحیح نہیں لگ رہا ہو تو یہ ایک حملہ ہو سکتا ہے- سوشل انجینئرنگ حملے کی سب سے عام علامات میں شامل ہے:

- اگر کوئی شخص شدید عجلت کا احساس دلا رہا ہے تو اس کا مطلب ہے کہ وہ آپ کو کوئی غلطی کرنے پر اکسا رہا ہے-
- اگر کوئی آپ سے ایسی معلومات مانگ رہا ہے جو ان کے پاس ہونی نہیں چاہیئے یا انہیں پہلے سے پتہ ہونی چاہیئے جیسے کہ آپ کے اکاؤنٹ نمبرز-
- کوئی آپ سے آپ کا پاس ورڈ مانگ رہا ہے- کوئی بھی صحیح تنظیم آپ سے کبھی بھی پاس ورڈ نہیں مانگے گی-
- کوئی آپ پر سکیورٹی کے اس عمل یا طریقہ کار کو نظر انداز کرنے کے لیئے زور ڈال رہا ہے جس پر آپ کو دفتر میں لازمی عمل کرنا چاہیئے-

سوشل انجینئرنگ

- کوئی ایسی چیز جو صحیح نہیں لگ رہی ہو- مثال کے طور پر آپ کو کوئی مطلع کرتا ہے کہ آپ نے کوئی لاٹری یا آئی-پیڈ جیت لیا ہے، جب کہ آپ نے کسی لاٹری میں شرکت ہی نہیں کی ہے-
- آپ کو کسی دوست یا ساتھ کام کرنے والے کسی شخص کی جانب سے کوئی عجیب سی ای میل موصول ہوتی ہے جس میں ایسے الفاظ استعمال ہوئے ہوتے ہیں جو ان کے نہیں لگتے- ہو سکتا ہے کہ سائبر حملہ آور نے ان کا اکاؤنٹ ہیک کر لیا ہو اور وہ اس کے ذریعے آپ کو دھوکہ دینے کی کوشش کر رہے ہوں- اپنی حفاظت کے لیئے ضروری ہے کہ آپ اس طرح کی کسی بھی ای میل کی اپنے دوست سے، رابطے کے مختلف طریقوں میں سے کسی کو بھی استعمال کرتے ہوئے تصدیق کر لیں، جیسے کہ ان سے مل کر یا فون کے ذریعے-

اگر آپ کو لگتا ہے کہ کوئی آپ کو دھوکہ دے رہا ہے یا بیوقوف بنا رہا ہے تو آپ اس شخص سے خود مزید بات چیت نہیں کریں- اگر حملہ دفتر سے متعلق ہے تو آپ اس بات کو یقینی بنائیں کہ آپ اس کی اطلاع ہیلپ ڈیسک یا انفارمیشن سکیورٹی ٹیم کو فوراً کریں- یاد رکھیں کہ آپ کا عام فہم ہی آپ کا بہترین دفاع 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 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
سی ای او فراڈ:	https://securingthehuman.sans.org/ouch/2016#july2016
رینسم ویئر:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH نیوز لیٹر آرکائیوز:	https://securingthehuman.sans.org/ouch/archives

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

ترجمہ: شعیب ہاشمی