OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

فون کال کے ذریعے دھوکہ دہی اور حملے کرنا

جائزہ

جب آپ سائبر مجرمان کے بارے میں سوچتے ہیں تو آپ کے ذہن میں شاید ایک ایسے شیطانی دماغ کا خیال آتا ہے جو کمپیوٹر کے پیچھے بیٹھ کر انٹرنیٹ پر بہت نفیس قسم کے حملے کرتا ہے- حالانکہ آج کل کے سائبر مجرمان اپنے شکار کو ہدف بنانے کے لیئے ای میل یا انسٹینٹ میسیجنگ جیسی ٹیکنالوجیز استعمال کرتے ہیں لیکن اس کے علاوہ وہ اس مقصد کے لیئے فون کا بھی استعمال کرتے ہیں- فون استعمال کرنے کے دو فائدے ہیں- پہلا یہ کہ ای میل کے برعکس اس وقت بہت ہی کم سکیورٹی ٹیکنالوجیز موجود ہیں جو کہ فون کالز کی نگرانی کے ذریعے کسی حملے کی شناخت کر سکتی ہیں اور اسے روک سکتی ہیں- دوسرا یہ کہ مجرمان کے لیئے فون کے ذریعے اپنے جذبات کا اظہار کرنا اور اپنے ہدف کو شکار کرنا کافی آسان ہوتا ہے- آئیں ہم ان حملوں کو شناخت کرنے اور انہیں روکنے کے بارے میں سیکھتے ہیں-

فون کال کے ذریعے حملے کیسے ہوتے ہیں؟

سب سے پہلے آپ کو یہ بات سمجھنی ہو گی کہ یہ حملہ آور آخر کس چیز کے پیچھے ہیں- اکثر وہ آپ کے پیسوں، معلومات یا آپ کے کمپیوٹر تک رسائی (یا تینوں) کے پیچھے پڑے ہوتے ہیں- وہ دھوکہ دہی کے ذریعے آپ سے اپنی مرضی کے اقدامات اٹھواتے ہیں- مجرمان دنیا بھر میں لوگوں کو کال کر کے ایسی صورت حال بیان کرتے ہیں اور شدید عجلت کا احساس دلاتے ہیں کہ اگر کال موصول کرنے والے نے ان کے کہے ہوئے اقدامات نہ اٹھائے تو وہ نقصان اٹھائے گا- ان کا مقصد آپ کو اتنا ڈرا دینا ہے کہ آپ پریشان ہو کر سوچے سمجھے بغیر کوئی غلطی کر بیٹھیں- کچھ بہت عام مثالیں مندرجہ ذیل بیان کی گئی ہیں:

کال کرنے والا آپ کو کہتا ہے کہ وہ حکومت کے ٹیکس وصول کرنے والے ادارے سے ہے اور آپ کو یہ کہتا ہے کہ آپ نے اپنا ٹیکس جمع نہیں کروایا ہے- وہ آپ کو مزید یہ کہہ کر ڈراتے ہیں کہ اگر آپ نے ٹیکس فوراً جمع نہیں کروایا تو آپ کو جیل جانا پڑے گا- اس کے بعد وہ آپ پر دباؤ ڈالتے ہیں کہ آپ فون پر کریڈٹ کارڈ کے ذریعے اپنے ٹیکس جمع کروائیں- یہ دھوکہ دہی کا ایک طریقہ ہے- کئی ٹیکس وصول کرنے والے ڈیپارٹمنٹس بشمول ‹آئی آر ایس›، لوگوں کو کبھی بھی ای میل یا کال نہیں کرتے ہیں بلکہ تمام باضابطہ اطلاعات ڈاک کے ذریعے بھیجی جاتی ہیں-

کال کرنے والا آپ سے مائیکروسافٹ ٹیک سپورٹ کا نمائندہ بن کر بات کرتا ہے اور آپ کو بتاتا ہے کہ آپ کا کمپیوٹر کسی وائرس سے متاثر ہو گیا ہے- ایک بار جب وہ آپ کو اس بات پر قائل کر دے کہ آپ کا کمپیوٹر متاثر ہو چکا ہے تو پھر وہ آپ پر دباؤ ڈالتا ہے کہ آپ اس کا سافٹ ویئر خریدیں یا اسے اپنے کمپیوٹر تک رسائی فراہم کریں- مائیکروسافٹ آپ کو کبھی بھی گھر پر کال نہیں کرے گا-

آپ کو خودکار وائس میل پر پیغام موصول ہوتا ہے کہ آپ کا بینک اکاؤنٹ منسوخ کر دیا گیا ہے اور یہ کہ آپ کو اسے واپس فعال کروانے کے لیئے ایک نمبر پر کال کرنی پڑے گی- جب آپ اس نمبر پر کال کرتے ہیں تو آپ سے خودکار سسٹم کے ذریعے آپ کی شناخت معلوم کی جاتی ہے اور آپ سے کئی ذاتی سوالات پوچھے جاتے ہیں- حقیقت میں یہ آپ کا بینک نہیں ہوتا ہے، یہ صرف ایک ریکارڈنگ ہوتی ہے جس کا مقصد آپ کی معلومات چرا کر آپ کی شناخت کو دھوکہ دہی کے لیئے استعمال کرنا ہے-

اپنی حفاظت کرنا

فون کالز کے حملوں کے خلاف سب سے بہترین دفاع آپ خود ہیں- آپ مندرجہ ذیل باتوں کا خیال رکھیں:

جب کبھی آپ کو کوئی کال کر کے شدید عجلت کا احساس دلا رہا ہو، یا کسی کام کے کرنے کے لیئے شدید دباؤ ڈال رہا ہو تو آپ بہت محتاط ہو جائیں- کال شروع میں چاہے صحیح لگ رہی ہو لیکن آہستہ آہستہ وہ عجیب لگنے لگتی ہے- اس موقع پر آپ کو رک کر کال کرنے والے کو «نہیں» کہہ دینا چاہیئے-

اگر آپ کو لگتا ہے کہ فون کال کوئی حملہ ہے تو آپ فون بند کر دیں- اگر آپ یہ جاننا چاہتے ہیں کہ فون کال صحیح ہے تو آپ کال کرنے والے کی تنظیم (جیسے کہ آپ کا بینک) کی ویب سائٹ پر جائیں اور ان کے کسٹمر سپورٹ کے نمبر کے ذریعے خود کال کر کے بات کریں- اس طرح آپ کو یہ پتہ چل جائے گا کہ آپ حقیقی تنظیم سے بات کر رہے ہیں یا نہیں-

آپ کالر آئی ڈی پر کبھی بھی بھروسہ نہیں کریں- برے لوگ اکثر کال کرنے والے نمبر کو چھپا کر ایسے نمبر سے تبدیل کر دیتے ہیں کہ ایسا لگے کہ وہ کسی اصل تنظیم کی جانب سے آئی ہے یا پھر اس میں وہی ایریا کوڈ استعمال ہوا ہوتا ہے جو کہ آپ کے فون نمبر کا ہوتا ہے-

آپ کبھی بھی کسی بھی کالر کو اپنے کمپیوٹر کا عارضی طور پر کنٹرول سنبھالنے نہیں دیں یا کسی کے دھوکے میں آ کر سافٹ ویئر ڈاؤن لوڈ نہیں کریں- برے لوگ ان طریقوں کو استعمال کر کے آپ کے کمپیوٹر کو متاثر کر سکتے ہیں-

اگر فون کال کسی ایسے شخص کی جانب سے آ رہی ہے جسے آپ ذاتی طور پر نہیں جانتے ہیں تو اس کال کو آپ سیدھا وائس میل کی جانب منتقل کر دیں- اس طرح آپ نامعلوم کالز کا اپنے وقت کے مطابق جائزہ لے سکتے ہیں- بہت سارے فونز میں «ڈو ناٹ ڈسٹرب» کی خصوصیت موجود ہوتی ہے، بہتر ہے کہ آپ اسے ڈیفالٹ کے طور پر فعال کر دیں-

فون کے ذریعے دھوکہ دہی اور حملے بڑھتے جا رہے ہیں- ان حملوں کی تشخیص کرنے اور ان سے تحفّظ کا سب سے بہترین ذریعہ آپ خود 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-

مہمان مُدیر

جین فاکس 'آل کوورڈ' میں سینئر سکیورٹی کنسلٹنٹ کے طور پر سکیورٹی سے متعلق آگاہی، سوشل انجینئرنگ اور رسک ایسسمینٹ کی خدمات سرانجام دیتی ہیں- آپ ٹوئیٹر پر جین تک @j_fox کے ذریعے رسائی حاصل کر سکتے ہیں-

وسائل:

شناخت، پرائیویسی اور آن لائن سکیورٹی سے متعلق صارفین کی معلومات:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

فون کے ذریعے دھوکہ دہی کو رپورٹ کریں (امریکہ میں):
https://www.ftccomplaintassistant.gov/#crnt

سوشل انجینئرنگ:
https://www.sans.org/u/Fi5