SANS SECURITY AWARENESS

OUCH!

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

مخصُوص ذاتی جعلسازی

جائزہ

سائبر مُجرمان لوگوں کو بیوقوف بنانے کے نت نئے طریقے ڈھونڈتے رہتے ہیں- اب ایک نئی طرح کی جعلسازی بہت مقبول ہو رہی ہے جو کہ مخصُوص ذاتی جعلسازی یا Personalized Scams کہلاتی ہے- سائبر مُجرمان لاکھوں لوگوں کی معلومات خریدتے ہیں یا ڈھونڈتے ہیں اور پھر ان معلومات کے ذریعے اپنے حملوں کو مخصُوص بناتے ہیں- نیچے ہم آپ کو یہ بتائیں گے کہ اس طرح کی جعلسازی کس طرح سے ہوتی ہے اور آپ کو اس کی ایک عام مثال بھی دیں گے- آپ کو جتنا زیادہ اس طرح کی جعلسازی کے بارے میں معلومات ہوں گی، آپ کے لیئے اس کی شناخت کرنا اور روکنا اتنا ہی آسان ہو گا-

یہ کام کس طرح سے کرتے ہیں؟

ای میل اور فون کال کے ذریعے جعلسازی کوئی نئی بات نہیں ہے، سائبر مُجرمان لوگوں کو اس طرح سے کئی سالوں سے بیوقوف بنانے کی کوشش کر رہے ہیں- اس کی بہت عام مثالوں میں «آپ نے لاٹری جیت لی ہے» یا مشہور زمانہ نائجیریا کے شہزادے کی جعلسازی شامل ہے- تاہم ان حملوں میں سائبر مُجرمان کو اپنے ہدف کے بارے میں پتہ نہیں ہوتا ہے- وہ ایک عام سا پیغام تخلیق کرتے ہیں اور اُسے لاکھوں لوگوں کو بھیج دیتے ہیں- کیونکہ اس طرح کی جعلسازی بہت عام ہوتی ہے اور اس کی نشاندہی کرنا بھی آسان ہوتا ہے- ایک مخصُوص اور ذاتی جعلسازی مختلف ہوتی ہے، اس میں سائبر مُجرمان پہلے تحقیق کرتے ہیں اور پھر اپنے ہر ہدف کے حساب سے مخصُوص پیغام تخلیق کرتے ہیں- وہ یہ سب ایک ایسے ڈیٹا بیس کو ڈھونڈ کر یا خرید کر کرتے ہیں جس میں لوگوں کے نام، پاس ورڈز، فون نمبرز یا دوسری تفصیلات موجود ہوتی ہیں- یہ معلومات باآسانی اُن ویب سائٹس کے ذریعے مل جاتی ہیں جو کہ پہلے ہیک ہو چکی ہوتی ہیں- یہ معلومات عام طور پر سوشل میڈیا سائٹس اور عوامی طور موجود حکومتی دستاویزات میں بھی موجود ہوتی ہیں- پھر مُجرمان ان حاصل کردہ معلومات کے مطابق اپنے شکار کو ہدف بناتے ہیں-

ایک عام چال جسے سائبر مُجرمان چُنتے ہیں وہ خوف یا بھتہ خوری کے ذریعے آپ سے زبردستی پیسے بٹورنا ہے- یہ حملہ کام اس طرح سے کرتا ہے کہ سائبر مُجرمان ہیک شدہ ویب سائٹ کے ذریعے لوگوں کے لاگ اِن اور پاس ورڈز کی معلومات کو ڈھونڈتے ہیں یا اُنہیں خریدتے ہیں- وہ آپ کے اکاؤنٹ کی معلومات کو ایسے ہی کسی ڈیٹا بیس کے ذریعے حاصل کرتے ہیں اور پھر آپ کو (اور اس ڈیٹا بیس میں موجود تمام دوسرے لوگوں کو) ایک ای میل کے ذریعے آپ کی ذاتی معلومات کی تفصیل بھیجتے ہیں جس میں ہیک شدہ ویب سائٹ میں استعمال ہونے والا آپ کا اصل پاس ورڈ بھی شامل ہوتا ہے- سائبر مجرم اس ای میل میں لکھے گئے پاس ورڈ کو «ثبوت» کے طور پر پیش کرتا ہے اور کہتا ہے کہ اس نے آپ کا کمپیوٹر یا آلہ ہیک کر لیا ہے، جو کہ بالکل غلط بات ہے- پھر سائبر مجرم دعوہ کرتا ہے کہ کمپیوٹر کو ہیک کرنے کے دوران اس نے آپ کو غیر اخلاقی ویب سائٹس پر جاتے ہوئے پکڑا ہے- پھر وہ آپ کو دھمکی دیتا ہے کہ اگر آپ نے اُسے بھتے کی رقم نہیں دی تو وہ شرمندہ کرنے والی آپ کی تمام آن لائن سرگرمیوں کے ثبوت آپ کے خاندان اور دوستوں کو بھیج دیں گے-

اس میں ایک اہم بات یہ ہے کہ تقریباً ان تمام صورتوں میں سائبر مُجرمان آپ کے سسٹم کو کبھی بھی ہیک نہیں کرتے ہیں- اُنہیں تو یہ بھی نہیں پتہ ہوتا ہے کہ آپ کون ہیں اور آپ نے کن ویب سائٹس کا دورہ کیا ہے- جعلساز صرف آپ کی چند ذاتی معلومات کی بنا پر آپ کو ڈرانے کی

کوشش کرتے ہیں اور آپ کو یقین دلانے کی کوشش کرتے ہیں کہ آپ کا کمپیوٹر یا آلہ ہیک ہو گیا ہے اور پھر دھوکہ دہی کے ذریعے آپ سے پیسے نکلواتے ہیں- یاد رکھیں کہ بُرے لوگ اسی طرح کی تکنیک استعمال کر کے فون کے ذریعے بھی جعلسازی کر سکتے ہیں-

مجھے کیا کرنا چاہیئے؟

آپ اس طرح کی ای میلز یا فون کالز کو پہچانیں کہ وہ جعلی ہیں- اگر کوئی آپ سے آپ کی ذاتی معلومات کا اشتراک کرتا ہے تو یہ بات قدرتی ہے کہ آپ خوف محسوس کریں گے تاہم یہ بات یاد رکھیں کہ وہ شخص جھوٹ بول رہا ہے- یہ حملہ ایک بہت بڑے پیمانے پر ہونے والے خودکار حملے کی مہم کا حصّہ ہے، نہ کہ آپ کی طرف کوئی مخصُوص حملہ- سائبر مُجرمان کے لیئے لوگوں کی ذاتی معلومات کو ڈھونڈنا یا خریدنا بہت آسان ہوتا جا رہا ہے اس لیئے آپ مستقبل میں مخصُوص ذاتی جعلسازی کے مزید حملوں کی توقع رکھیں- ان میں سے چند علامات جن کی آپ شناخت کر سکتے ہیں وہ یہ ہیں:

- **آپ کو جب بھی کوئی شدید عُجلت والی ای میل ملے، پیغام ملے یا کوئی کال آئے تو آپ مشکوک ہو جائیں- اگر کوئی آپ کے ساتھ خوف یا عُجلت جیسے احساسات کا استعمال کرتا ہے تو اس کا مطلب ہے کہ وہ آپ سے جلد بازی میں کوئی غلطی سرزد کروانا چاہتا ہے-**
- **جب کوئی آپ سے بِٹ کوائن، گفٹ کارڈز یا کسی ایسے طریقے سے ادائیگی کا تقاضا کرے جس کا پتہ نہیں لگایا جا سکتا ہو-**
- **جب آپ کو کوئی مشکوک ای میل آئے تو آپ اس کے بارے میں گُوگل پر دوسرے لوگوں کی رائے جانیں کہ آیا انہوں نے بھی اُس سے ملتے جُلتے حملوں کے بارے میں اطلاع دی ہے-**

بلآخر عام فہم ہی آپ کا سب سے بہترین دفاع ہے تاہم ہمارا مشورہ یہ بھی ہے کہ آپ ہمیشہ اپنے ہر آن لائن اکاؤنٹ کے لیئے مُنفرد اور لمبے پاس ورڈ کا استعمال کریں- کیا آپ اپنے تمام پاس ورڈز یاد نہیں رکھ سکتے ہیں؟ اس کا حل یہ ہے کہ آپ پاس ورڈ مینیجر استعمال کریں- اس کے علاوہ جب بھی مُمکن ہو ‹ٹُو اسٹیپ ویریفیکیشن› کو فعّال کردیں-

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

لینی زیلٹسر ایک تجربہ کار سائبر سکیورٹی کے ماہر ہیں- وہ مینروہ لیبس میں اینٹی میلویئر سے متعلق مصنوعات بناتے ہیں اور SANS انسٹیٹیوٹ میں سکیورٹی سے متعلق پڑھاتے ہیں- وہ مینیجڈ سکیورٹی سروسز اور کنسلٹنگ کا بھی تجربہ رکھتے ہیں- آپ ان کا بلاگ zeltser.com/blog پر پڑھ سکتے ہیں اور اُنہیں ٹوئیٹر پر @lennyzeltser کے ذریعے ڈھونڈ سکتے ہیں-

وسائل:

سوشل انجینئرنگ: https://www.sans.org/u/MUU
فِشنگ کو روکیں: https://www.sans.org/u/MUZ
اپنے آپ کو آن لائن ڈھونڈیں: https://www.sans.org/u/MV4
پاس ورڈ مینیجر: https://www.sans.org/u/MV9

OUCH! کی ا شاعتSANS Security Awareness Programکے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 4.0 License کے تحت تقسیم کرنے کی اجازت ہوتی ہے-
آپ اس نیوز لیٹر کو تقسیم سکتے ہیں اگر آپ اس کا حوالہ دیں ، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لئے استعمال کریں - ترجمے اور مزید معلومات کے لئے www.sans.org/security-awareness/ouch-newsletterپر رابطہ کریں. ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley- | ترجمہ: شعیب ہاشمی