SANS SECURITY AWARENESS

OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

سی ای او فراڈ / بی ای سی (بزنس ای میل کمپرومائز)

سی ای او فراڈ / بی ای سی کیا ہے؟

سائبر حملہ آور مسلسل ایک ای میل حملے پر کام کرتے رہتے ہیں جو کہ سی ای او فراڈ یا بزنس ای میل کمپرومائز (بی ای سی) کہلاتا ہے- یہ ای میل خاص طور پر مخصُوص شکار کو ہدف بنا کر کی جاتی ہے تاکہ اس شخص سے دھوکہ دہی کے ذریعے ایسے اقدامات اٹھوائے جائیں جو کہ اسے نہیں اٹھانے چاہیئے- زیادہ تر حالات میں بُرے لوگ پیسے کے پیچھے ہوتے ہیں- جو بات اس حملے کو انتہائی خطرناک بناتی ہے وہ یہ ہے کہ سائبر حملہ آور اپنے شکار کے بارے میں تحقیق اُس پر حملہ کرنے سے پہلے کرتے ہیں- سکیورٹی ٹیکنالوجیز کے لیئے ان حملوں کو روکنا انتہائی مشکل ہوتا ہے کیونکہ اس ای میل میں کوئی متاثرہ اٹیچمنٹ یا مُضر لِنک موجود نہیں ہوتا ہے- یہ حملہ کچھ اس طرح سے کام کرتا ہے-

سائبر حملہ آور انٹرنیٹ کا استعمال کرتے ہوئے اپنے مُمکنہ شکار اور اُس سے ملنے جُلنے والے لوگوں کے بارے میں تحقیق کرتے ہیں- مثال کے طور پر اگر وہ آپ کو نشانہ بنانا چاہتے ہیں تو وہ آپ کے بالا افسر کے بارے میں تحقیق کریں گے کہ وہ کون ہے یا شاید وہ یہ دیکھیں کہ آپ اپنے گھر سے کس اسٹیٹ ایجنٹ کے ساتھ کام کر رہے ہیں- سائبر حملہ آور ان لوگوں میں سے کوئی شخص بن کر ایک ای میل تخلیق کرتا ہے اور آپ کو بھیجتا ہے- یہ ای میل عُجلت کا احساس دلاتی ہے اور آپ کو فوری قدم اُٹھانے کا کہتی ہے جیسے کہ کسی انوائس پر عمل درآمد کرنا، پیسوں کی ادائیگی کے لیئے کسی کا نام تبدیل کرنا یا آپ کو حسّاس دستاویزات کے ساتھ جواب دینے پر قائل کرتی ہیں- یہ ای میل کام اس طرح سے کرتی ہے کہ حملہ آور آپ پر دباؤ کے ذریعے اپنی مرضی کے اقدامات اٹھواتا ہے- آپ کو مندرجہ ذیل دو مثالوں سے اندازہ ہو جائے گا کہ ایسے حملے کام کس طرح سے کرتے ہیں-

وائر ٹرانسفر: سائبر مُجرمان پیسوں کے پیچھے پڑے ہوتے ہیں- آپ جس تنظیم میں کام کرتے ہیں وہ اُس کے بارے میں تحقیق کرتے ہیں کہ وہاں اکاؤنٹس میں کون کام کرتا ہے یا فنڈز کی مُنتقلی کا کون ذمہ دار ہے- مُجرمان پھر ایک ای میل تخلیق کرتے ہیں اور اُن افراد کو اُن کے بالا افسر یا سینئر ایگزیکٹو بن کر بھیجتے ہیں- یہ ای میل انہیں بتاتی ہے کہ ایک ہنگامی صورتحال رونما ہو گئی ہے اور ایک نئے اکاؤنٹ میں پیسے فوری طور پر منتقل کرنے ہیں- وہ ای میل انہیں دباؤ کے ذریعے غلطی سرزد کرنے پر مجبور کرتی ہے لیکن در حقیقت وہ یہ پیسے سائبر مُجرمان کو بھیج رہے ہوتے ہیں-

ٹیکس فراڈ: سائبر مُجرمان لوگوں کی ذاتی معلومات کے پیچھے پڑے ہوتے ہیں تاکہ اُسے ٹیکس فراڈ میں استعمال کر سکیں- یہ کام سر انجام دینے کا سب سے تیز ترین طریقہ کسی تنظیم کے ملازمین کی معلومات چُرانا ہے- سائبر مُجرمان تحقیق کے ذریعے ہیومن ریسورس ڈیپارٹمنٹ میں کام کرنے والوں کی نشاندہی کرتے ہیں اور پھر اُنہیں سینئر ایگزیکٹو یا قانونی ٹیم کا نُمائندہ بن کر جعلی ای میل کرتے ہیں- اس ای میل کے ذریعے وہ شدید عُجلت والی کہانی گڑھتے ہیں کہ اُنہیں تمام ملازمین کی ٹیکس سے متعلق معلومات فوری طور پر چاہیئے- ہیومن ریسورس ڈیپارٹمنٹ والے ملازمین سمجھتے ہیں کہ وہ یہ حسّاس دستاویزات کسی سینئر ایگزیکٹو کو بھیج رہے ہیں لیکن در حقیقت وہ سائبر مُجرمان کو بھیج رہے ہوتے ہیں-

اپنی حفاظت کرنا

تو آپ اپنی حفاظت کے لیئے کیا کر سکتے ہیں؟ عام فہم آپ کا سب سے بہترین دفاع ہے- آپ مندرجہ ذیل اشاروں کی مدد سے اس طرح کی ای میل کی نشاندہی کر سکتے ہیں:

یہ ای میل بہت چھوٹی اور شدید عُجلت والی ہوتی ہے (شاید صرف دو جملے) اور اس کے دستخط میں یہ لکھا آ رہا ہوتا ہے کہ ای میل موبائل آلہ کے ذریعے بھیجی گئی ہے-

آپ کو شدید عُجلت کا احساس دلایا جا رہا ہوتا ہے تاکہ آپ پر ایسا دباؤ ڈالا جائے کہ آپ اپنی تنظیم کی پالیسیز کو نظرانداز کر دیں- آپ ہمیشہ اپنے دفتر سے متعلق پالیسیز اور طریقہ کار پر سختی سے عمل پیرا ہوں چاہے آپ کے پاس ای میل آپ کے بالا افسر یا سی ای او کی جانب سے کیوں نہ آئی ہو-

جو ای میل آپ کو آئی ہے وہ آپ کے کام سے متعلق ہے لیکن کسی کے ذاتی ای میل ایڈریس سے آئی ہے جیسے کہ @gmail.com یا @hotmail.com سے-

آپ کو ای میل کسی ایسے سینئر لیڈر، ساتھ کام کرنے والے ساتھی یا کسی وینڈر کی جانب سے آئی ہے جسے آپ جانتے ہیں لیکن اس میں جو لہجہ استعمال کیا گیا ہے، اُس سے ایسا نہیں لگتا کہ وہ اُنہوں نے بھیجی ہے-

آپ کو ای میل میں پیسوں کی ادائیگی سے متعلق ہدایات دی گئی ہیں لیکن وہ اُن ہدایت سے مختلف ہیں جو آپ کو پہلے بھیجی جا چکی ہیں جیسے کہ کسی بینک اکاؤنٹ میں فوری طور پر پیسے جمع کروانا-

اگر آپ کو لگتا ہے کہ آپ کو دفتر میں نشانہ بنایا گیا ہے تو آپ حملہ آور سے ہر طرح کی مواصلات منقطع کر دیں اور اپنے سُپروائزر کو اس سے متعلق آگاہ کر دیں- اگر آپ کو گھر پر نشانہ بنایا گیا ہے یا آپ کسی کا شکار بن چُکے ہیں اور آپ نے پیسے مُنتقل کر دیئے ہیں تو آپ اپنے بینک کو پہلے اور پھر قانون نافذ کرنے والے ادارے کو اُس کی فوری طور پر اطلاع دیں-

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

ڈان کاوینڈر ایف بی آئی کے سابق خاص ایجنٹ ہیں اور اپنے پاس ڈیجیٹل فارینزک اور سائبر کرائم کا ۲۲ سال سے زیادہ کا تجربہ رکھتے ہیں- انہوں نے واشنگٹن ڈی سی میں حال ہی میں سائبر کرائم کی تنظیموں کے لیئے بی ای سی کوآرڈینیٹر کے طور پر کام کیا ہے- وہ ڈیجیٹل فارنزیکس اور سائبر انویسٹیگیشن کی تربیت دیتے ہیں اور اُن سے متعلق تحقیق کرتے ہیں- آپ اُن تک ٹوئیٹر پر @don_cavender اور لِنکڈاِن پر https://www.linkedin.com/in/donald-cavender کے ذریعے رسائی حاصل کر سکتے ہیں-

وسائل:

سوشل انجینئرنگ: https://www.sans.org/u/HE3
فِشنگ کو روکیں: https://www.sans.org/u/HE8
میلویئر کو روکیں: https://www.sans.org/u/HEd
اپنے لاگ اِن کو لاک کریں: https://www.sans.org/u/HEi