کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- سی ای او فراڈ کیا ہے؟
- اپنی حفاظت کرنا

سی ای او فراڈ

سی ای او فراڈ کیا ہے؟

سائبر مُجرمان بہت چالاک ہوتے ہیں اور وہ مسلسل نئے طریقے ڈھونڈتے رہتے ہیں- اُن کا ایک مؤثر طریقہ آپ جیسے لوگوں کو ہدف بنانا ہے- سائبر مُجرمان یہ بات اچھّی طرح سے جان چُکے ہیں کہ کسی بھی تنظیم میں ‹لوگ، حفاظت کا سب سے کمزور ترین ذریعہ ہوتے ہیں لیکن وہ یہ بات بُھول چُکے ہیں کہ OUCH کے قارئین جیسے صاحب علم لوگ کسی بھی تنظیم کا بہترین دفاع ہو سکتے ہیں-

مہمان ایڈیٹر

اینجلا پیاس، تھامسن ریوٹرز میں انفارمیشن سکیورٹی کی تربیت اور آگاہی کی ڈائریکٹر ہیں- اینجلا اس حیثیت سے سفیر پروگرام، ‹ای-لرننگ، اور ملازمین کی فشنگ سے متعلق تعلیم کی ذمہ دار ہیں-

سائبر مُجرمان نے ایک نیا حملہ تخلیق کیا ہے جو کہ ‹سی ای او فراڈ، کہلاتا ہے، اسے ‹بزنس ای-میل کمپرومائز، (BEC) بھی کہتے ہیں- ان حملوں میں ایک سائبر مُجرم آپ کی تنظیم کے سی ای او یا سینیئر افسر ہونے کا ڈرامہ رچاتا ہے- یہ ملزمان آپ کی طرح کے عملے کو ایک ای-میل بھیجتے ہیں اور آپ کو کچھ ایسا کرنے پر اُکساتے ہیں جو آپ کو نہیں کرنا چاہیئے- اِس طرح کے حملے بہت زیادہ مؤثر ہوتے ہیں کیونکہ سائبر مُجرمان نے اِس سلسلے میں اپنی تحقیق کی ہوئی ہوتی ہے- وہ آپ کی تنظیم کی ویب سائٹ کی چھان بین کرتے ہیں تاکہ وہاں سے معلومات حاصل کر سکیں- ان معلومات میں اس تنظیم کا محلّ وقوع، اس کے اعلیٰ افسران کون ہیں اور دوسری تنظیمیں جن کے ساتھ وہ کام کرتے ہیں، شامل ہیں- سائبر مُجرمان پِھر آپ کے ساتھ کام کرنے والے لوگوں کے بارے میں لِنکڈاِن، فیس بُک یا ٹوئیٹر جیسی سائٹس کے ذریعے معلومات حاصل کرتے ہیں- ایک بار اُنہیں تنظیم کا ڈھانچہ پتہ چل جاتا ہے تو وہ مخصُوص ملازمین کو ہدف بناتے ہیں اور اُن کے بارے میں تحقیق شروع کرتے ہیں- وہ اپنے ہدف کا انتخاب مخصُوص مقاصد کے مطابق کرتے ہیں- اگر سائبر مُجرمان کا مقصد پیسے حاصل کرنا ہے تو ہو سکتا ہے کہ وہ اکاؤنٹس کی ادئیگی کے ڈیپارٹمنٹ کو ہدف بنا ئیں- اگر اُنہیں ٹیکس سے متعلق معلومات حاصل کرنی ہے تو وہ ہیومن ریسورس کے ڈیپارٹمنٹ کو ہدف بنا سکتے ہیں- اگر وہ ڈیٹابیس سرورز تک رسائی حاصل کرنا چاہتے ہیں تو اِس کے لیۓ وہ آئی ٹی ڈیپارٹمنٹ میں کسی کو نشانہ بنا سکتے ہیں-

ایک بار جب وہ اِس بات کا تعیّن کرلیں کہ اُنہیں کیا چاہیۓ اور کسے ہدف بنانا ہے تو پِھر وہ اپنا حملہ تخلیق کرنا شروع کرتے ہیں- وہ زیادہ تر اسپیئرفشنگ استعمال کرتے ہیں- فشنگ اُس وقت ہوتی ہے جب ایک حملہ آور ایک ای-میل کو لاکھوں لوگوں کو ارسال کرتا ہے جس کا مقصد لوگوں کو جھانسا دے کر کُچھ کرنے پر اُکسانا ہوتا ہے، مثال کے طور پر کسی مُتاثرہ اٹیچمنٹ کو کھولنا یا کسی مُضر ویب سائٹ کا دورہ کرنا- اسپیئر فشنگ بھی فشنگ کی طرح ہوتی ہے- تاہم لاکھوں لوگوں کو ایک عام ای-میل بھیجنے کے بجائے سائبر مُجرمان ایک مخصُوص ای-میل ایک بہت ہی چھوٹے، منتخب گروہ کو بھیجتے ہیں- یہ اسپیئر فشنگ ای-میلز بالکل اصل لگتی ہیں اِس لیۓ اُن کی تشخیص کرنا بہت مُشکل ہوتا ہے- اکثر ایسا لگتا ہے کہ یہ ای-میلز کسی ایسے شخص کی جانب سے آئی ہیں جسے آپ جانتے ہیں یا جس کے ساتھ آپ کام کرتے ہیں جیسے کہ آپ کے ساتھ کام

سی ای او فراڈ

کرنے والے ملازمین یا شاید آپ کے بالا افسر- یہ ای-میلز بالکل اصل لگتی ہیں کیونکہ اُن میں ایسی اصطلاحات استعمال ہوئی ہوتی ہیں جو کہ آپ کے ساتھی مُلازمین استعمال کرتے ہیں، وہ آپ کی تنظیم کا لوگو یا شاید کسی افسر کا آفیشل دستخط بھی استعمال کر سکتے ہیں- یہ ای-میلز اکثر بہت زیادہ عُجلت کا احساس دلاتی ہیں اور آپ کو کسی کو بتائے بغیر کوئی فوری اقدام اٹھانے پر مجبور کرتی ہیں- سائبر مُجرمان کا حدف آپ سے کوئی غلطی سرزد کروانا ہے- آپ مندرجہ ذیل تین عام صورتوں کو ملاحظہ فرمائیں:

سی ای او فراڈ ایک بہت ہی طاقتور حملہ ہے جو کہ آپ کے بہت سارے حفاظتی اقدامات کو پار کر سکتا ہے۔ بالآخر ہمارے لیئے آپ ہی سب سے بہترین دفاع ہیں-

- **وائر ٹرانسفر**: ایک سائبر مُجرم پیسوں کی طاق میں ہوتا ہے- اس کا مطلب ہے کہ یہ لوگ اس بات کی تحقیق کرتے ہیں اور پتہ لگاتے ہیں کہ اکاؤنٹس کی ادائیگی کے ڈپارٹمنٹ میں کون کام کرتا ہے، یا آپ کی تنظیم کے مالی امُور کی دیکھ بھال کون سی ٹیم کرتی ہے- یہ مُجرمان پھر ایک ای-میل تخلیق کرتے ہیں اور ان کے بالا افسر کے طور پر اُنھیں بھیجتے ہیں- وہ ای-میل اُنھیں ایک ایمرجنسی کے بارے میں آگاہ کرتی ہے اور کسی مخصُوص اکاؤنٹ میں فوری پیسے منتقل کرنے کی ہدایت کرتی ہے۔

- **ٹیکس فنڈ**: سائبر مُجرمان آپ کے ساتھی ملازمین کی معلومات چُرانا چاہتے ہیں تاکہ وہ اُن کے طور پر ٹیکس فراڈ کر سکیں- وہ آپ کی تنظیم کے بارے میں تحقیق کرتے ہیں اور اس بات کا تعیّن کرتے ہیں کہ ملازمین کی معلومات کون سنبھال رہا ہے، مثال کہ طور پر ہیومن ریسورس میں کوئی ملازم- اس کے بعد سائبر مُجرمان جعلی ای-میلز بھیجتے ہیں جو کہ دیکھنے میں ایسی لگتی ہیں کہ کسی اعلیٰ افسر کی جانب سے آئی ہیں جس میں وہ فوری طور پر بعض دستاویزات کا مطالبہ کرتی ہیں-

- **وکیل کا رُوپ دھارنا**: تمام سی ای او حملوں میں ای-میل استعمال نہیں ہوتی، دوسرے طریقے بھی استعمال ہو سکتے ہیں جسے کہ ٹیلیفون- اس صورت میں مُجرمان آپ کو شروع میں ایک اعلیٰ افسر بن کر ای-میل کرتے ہیں جس میں وہ یہ بتاتے ہیں کہ آپ کو ایک بہت ضروری کام کے سلسلے میں ایک وکیل کی کال آئے گی- پھر وہ مُجرم آپ کو وکیل بن کر کال کرتا ہے اور آپ سے جلدی میں نازک معاملات پر بات کرتے ہوئے شدید عُجلت کا احساس دلاتا ہے- اس عُجلت کے نتیجے میں آپ کوئی فوری قدم اُٹھا بیٹھتے ہیں-

اپنی حفاظت کرنا

تو آپ اپنی اور اپنی تنظیم کی حفاظت کے لیئے کیا کر سکتے ہیں؟ آپ کے عام فہم کا استعمال ہی آپ کا سب سے بہترین دفاع ہے- اگر آپ کو اپنے اعلیٰ افسر یا ساتھ کام کرنے والے شخص کی جانب سے کوئی ای-میل آتی ہے جو کہ آپ کو لگ رہا ہو کہ کچھ صحیح نہیں ہے تو ہو سکتا ہے کہ یہ ایک حملہ ہو- اس کی نشاندہی میں عُجلت کا احساس، ایک دستخط جو کہ صحیح نہیں لگ رہا ہو، ایک ایسا لہجہ جس کی آپ توقع نہ کر رہے

سی ای او فراڈ

ہوں یا ای-میل میں استعمال ہونے والا نام اُس نام سے مختلف ہو جس سے وہ شخص آپ کو پُکارتا ہے، شامل ہے- ایک اور نشاندہی یہ ہو سکتی ہے کہ حملہ آور ایک ایسا ای-میل ایڈریس یا فون نمبر استعمال کر رہا ہے جسے آپ نے پہلے کبھی نہیں دیکھا ہے یا شاید وہ ایک ایسا ای-میل ایڈریس استعمال کر رہا ہے جو کہ آپ کے ساتھی ملازم یا اعلیٰ افسر کے ای-میل ایڈریس سے ملتا جُلتا ہے- آپ کو جب بھی شک ہوآپ اُس شخص کو کسی بھی بااعتماد نمبر پر کال کریں یا اُس سے خُود مل لیں (ای-میل کے ذریعے جواب نہیں دیں) اور اُن سے خُود اُس ای-میل کی تصدیق کریں- آپ کبھی بھی سکیورٹی پالیسیز یا پروسیجرز کو نظر انداز نہ کریں- آپ کی تنظیم میں شاید ایسی پالیسیز پہلے سے موجود ہوں جن کے ذریعے رقم کی منتقلی یا حسّاس معلومات جاری کرنے سے متعلق باقاعدہ طریقہ کار کی وضاحت کی گئی ہو- کوئی بھی ایسی درخواست جو اُن پالیسیز کو نظر انداز کرنے کی کوشش کرے، چاہے وہ کسی کی بھی جانب سے ہو، اُسے مشکوک سمجھنا چاہیئے اور کوئی بھی قدم اُٹھانے سے پہلے اُس کی تصدیق کر لینی چاہیئے- اگر آپ کے پاس کوئی بھی ایسی درخواست آئے اور آپ کو سمجھ نہیں آرہا ہو کہ کیا کرنا چاہیئے تو آپ کو اپنے سُپروائزر، ہیلپ ڈیسک یا انفارمیشن سکیورٹی کی ٹیم سے فوراً رابطہ کرنا چاہیئے-

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:

سوشل انجینئرنگ:	https://securingthehuman.sans.org/ouch/2014#november2014
فشنگ:	https://securingthehuman.sans.org//ouch/2015#december2015
میلویئر کیا ہے:	https://securingthehuman.sans.org/ouch/2016#march2016
ٹوُ اسٹیپ ویریفیکیشن:	https://securingthehuman.sans.org/ouch/2015#september2015
آج کی سکیورٹی تجویز:	https://www.sans.org/tip-of-the-day

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

ترجمہ: شعیب ہاشمی