کمپیوٹر استعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- فِشنگ
- اپنی حفاظت کرنا

فِشنگ

جائزہ

ای-میل مواصلات کے بنیادی طریقوں میں سے ایک ہے۔ ہم نہ صرف اسے دفتر بلکہ اپنے دوستوں اور خاندان سے رابطے میں رہنے کے لیئے بھی استعمال کرتے ہیں۔ اِس کے علاوہ یہ کہ زیادہ تر تنظیمیں ای-میل کے ذریعے آن لائن سروس فراہم کرتی ہیں جیسے کہ آپ کے آن لائن خریداری کی تصدیق یا بینک اسٹیٹمنٹس کی دستیابی- چوُنکہ دنیا بھر کے بہت سارے لوگ ای-میل پر انحصار کرتے ہیں اِس لیئے اُس پر حملہ سائبر مجرمان کے لیئے بُنیادی طریقوں میں سے ایک بن گیا ہے۔ اس نیوُزلیٹر میں ہم فِشنگ کے بارے میں بتائیں گے جو کہ عام ای-میل حملوں کے طریقوں میں سے ایک ہے۔ اس کے علاوہ ای-میل کو محفوظ طریقے سے استعمال کرنے سے متعلق حفاظتی تدابیر کے بارے میں بھی بتائیں گے۔

مہمان ایڈیٹر

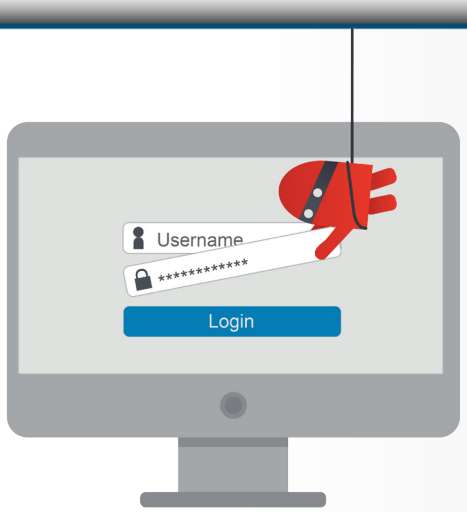
ڈاکٹر لانس ہیڈن برکلی ریسرچ گروُپ کے مینیجنگ ڈائریکٹر ہیں۔ وہ سکیورٹی اور اس سے متعلق رویّوں پر مہارت رکھتے ہیں- وہ ‹میک گرا ہِل› کی کتاب :People-Centric Security Transforming Your Enterprises Security Culture کے مصنف ہیں۔ آپ اُن تک رسائی www.linkedin.com/in/drhayden کے ذریعے حاصل کر سکتے ہیں۔

فِشنگ

فِشنگ سے مُراد وہ حملہ ہے جس میں ای-میل یا میسیجنگ سروس کا استعمال کیاجائے جیسے کہ سوشل میڈیا سائٹس پر جو کہ آپ کو دھوکہ دہی یا بیوقوف بنا کر کچھ اقدامات اٹھانے پر مجبور کرتی ہیں، جیسے کہ کسی لنک پر کلک کرنا یا کوئی اٹیچمنٹ کھولنا۔ ان حملوں کا شکار ہونے سے آپ کے کمپیوٹر کے متاثر ہونے اور/یا بہت ہی اہم معلومات کے چوری ہونے کا خدشہ بڑھ جاتا ہے۔ حملہ آور فِشنگ ای-میلز کو حقیقی روپ دینے کے لیئے بڑی محنت کرتے ہیں۔ مثلاً وہ اپنی ای-میل کو ایسے پیش کر رہے ہوتے ہیں کہ ایسا لگتا ہے کہ وہ کسی جاننے والے کی طرف سے آئی ہو جیسے کہ کسی دوست یا ایسی قابل اعتبار کمپنی سے جسے آپ بہت زیادہ استعمال کرتے ہوں۔ وہ اِن پیغامات کو صحیح دکھانے کے لیئے آپ کے بینک کے لوگوز اور ای-میل ایڈریس تک جعلی لگا دیتے ہیں- اس کے بعد حملہ آور ان فِشنگ ای-میلز کو لاکھوں لوگوں کو بھیج دیتے ہیں- اُنہیں یہ معلوم نہیں ہوتا ہے کہ اُن کا شکار کون بنے گا۔ اُنہیں صرف یہ معلوم ہوتا ہے کہ وہ جتنی زیادہ ای-میلز کریں گے، کامیابی کے امکانات اُتنے ہی زیادہ ہوں گے۔ فِشنگ مچھلی کے جال کے استعمال سے مشابہت رکھتی ہے، آپ کو یہ نہیں معلوم ہوتا ہے کہ آپ کیا شکار کریں گے لیکن جتنا بڑا جال ہواگا اُتنی ہی زیادہ مچھلیاں آپ پکڑ سکتے ہیں- حملہ آور اپنے مقاصد حاصل کرنے کے لیئے کئی طریقے استعمال کرتے ہیں۔

- **معلومات حاصل کرنا**: حملہ آور کا مقصد آپ کی ذاتی معلومات کا حصول ہے، جس میں پاس ورڈز، کریڈٹ کارڈ نمبرز یا بینکنگ تفصیلات شامل ہیں۔ ایسا کرنے کے لیئے وہ آپ کو ای-میل کے ذریعے ایک لنک بھیجتے ہیں جو بظاہر بالکل صحیح لگتا ہے۔ پھر یہ ویب سائٹ آپ کو اپنے اکاؤنٹ کی تفصیلات اور ذاتی تفصیلات فراہم کرنے کا کہتی ہے۔ چونکہ یہ ویب سائٹ جعلی ہوتی ہے اس لیئے آپ کی فراہم کردہ کوئی بھی معلومات سیدھا حملہ آور تک پہنچتی ہے۔

فِشنگ



آپ کا بہترین دفاع اپنے عام فہم کا استعمال ہے- اگر کوئی ای-میل یا پیغام آپ کو عجیب، مشکوک یا ناقابلِ اعتبار لگ رہا ہو تو ہو سکتا ہے کہ یہ فشنگ حملہ ہو۔

- **مُضر لنکس**: حملہ آور کا مقصد آپ کے آلہ کا کنٹرول حاصل کرنا ہے۔ ایسا کرنے کے لیئے وہ آپ کو ای-میل کے ذریعے ایک لنک بھیجتے ہیں- اگر آپ اُس لنک پر کلک کرتے ہیں وہ آپ کو ایک ایسی ویب سائٹ پر لے جاتا ہے جو آپ کے آلہ پر حملہ شروع کر دیتی ہے اور اگر وہ حملہ کامیاب ہوتا ہے تو آپ کا سسٹم متاثر ہو جاتا ہے۔
- **مُضر اٹیچمنٹس**: اس میں بھی حملہ آور کا مقصد وہی ہوتا ہے یعنی آپ کے آلہ کو متاثر کرنا اور اُس کا اختیار حاصل کرنا لیکن اس طریقے میں حملہ آور لنک بھیجنے کے بجائے متاثرہ فائل جیسے کہ ‹ورڈ ڈاکومنٹ› ای-میل کرتا ہے- اس اٹیچمنٹ کو کھولنے سے حملہ شروع ہو جاتا ہے اور ممکنہ طور پر حملہ آور کو آپ کے سسٹم کا اختیار مل جاتا ہے۔
- **اسکیمز**: کچھ فشنگ ای-میلز عام دغابازی ہوتی ہیں فرق صرف اتنا ہوتا ہے کہ یہ ڈجیٹل طریقے سے ہوتی ہیں۔ وہ آپ کو یہ کہہ کر بیوقوف بناتے ہیں کہ آپ نے لاٹری جیت لی ہے یا وہ خیراتی ادارہ بن کر آپ سے خیرات طلب کرتے ہیں یا وہ آپ کو لاکھوں ڈالرز کسی دوسری جگہ منتقل کرنے میں آپ سے مدد چاہتے ہیں- اگر آپ ان میں سے کسی کا بھی جواب دیتے ہیں تو وہ آپ سے اپنی خدمات کے پیسے طلب کرتے ہیں یا بینک اکاؤنٹ تک رسائی مانگتے ہیں جس کے نتیجے میں آپ اپنے پیسوں سے ہاتھ دھو بیٹھتے ہیں۔

اپنی حفاظت کرنا

تقریباً تمام صورتوں میں ای-میل یا کسی پیغام کو صرف کھولنا اور پڑھنا ٹھیک ہے۔ فشنگ حملے کو کامیاب بنانے کے لیئے بُرے لوگوں کو آپ کو دھوکہ دہی کے ذریعے کچھ اقدامات اٹھانے پر مجبور کرنا ہوتا ہے۔ خوش قسمتی سے آپ کُچھ طریقوں سے کسی بھی پیغام کی نشاندہی کر سکتے ہیں کہ آیا یہ کوئی فشنگ حملہ تو نہیں۔ فشنگ ای-میل کی نشاندہی کے سب سے عام طریقے مندرجہ ذیل بیان کیئے گئے ہیں۔

- اُس ای-میل میں ایک عُجلت نظر آتی ہے کیونکہ اُس میں یہ مطالبہ کیا گیا ہوتا ہے کہ آپ کوئی «فوری قدم» اٹھائیں اس سے قبل کہ کوئی بُری چیز ہو جائے جیسے کہ آپ کے اکاؤنٹ کا بند ہونا۔ حملہ آور کا مقصد آپ کا بغیرسوچے سمجھے جلدی میں کوئی غلطی کرنا ہے۔
- آپ کو کوئی ای-میل آتی ہے جس میں کوئی ایسی اٹیچمنٹ ہوتی ہے جس کی آپ توقع نہیں کر رہے ہوتے ہیں یا وہ ای-میل آپ کو اٹیچمنٹ کھولنے پر آمادہ کرتی ہے۔ مثا ل کہ طور پر ایک ای-میل آپ کو موصول ہوتی ہے جس میں کہا جاتا ہے کہ اُس کی اٹیچمنٹ میں اُن لوگوں کی تفصیلات موجود ہے جنہیں کام سے فارغ کیا جانے والا ہے یا کام کرنے والوں کی تنخواہ کی معلومات ہیں یا آئی-آر-ایس (انٹرنل ریونیو سروس) کی جانب سے ایک خط ہے جس میں یہ کہا گیا ہے کہ آپ کے خلاف مقدمہ چلایا جا رہا ہے۔
- آپ کا نام استعمال کرنے کے بجائے وہ ای-میل آپ کو «معزز صارف» کہہ کر مخاطب کرتی ہے۔
- وہ ای-میل آپ سے بہت اہم معلومات جیسے کہ کریڈٹ کارڈ نمبر یا پاس ورڈ کی گزارش کر سکتی ہے۔

فِشنگ

- وہ ای-میل دعویٰ کرتی ہے کہ کسی بڑی تنظیم کی طرف سے آئی ہے لیکن اُس میں خراب گرائمر اور ہجّے کا استعمال ہوتا ہے یا اس میں کسی ذاتی ای-میل ایڈریس کا استعمال ہوتا ہے جیسے کہ @yahoo.com، @hotmail.com یا @gmail.com-
- وہ لنک عجیب یا غیرسرکاری لگتا ہے۔ ایک تجویز یہ ہو سکتی ہے کہ آپ اپنے ماؤس کو اُس لنک کے اُوپر لے جائیں جب تک کہ ایک پاپ-اپ آپ کو یہ نہ دکھا دے کہ یہ لنک آپ کو اصل میں کہاں لے جا رہا ہے- اگر آپ کی ای-میل میں دیا گیا لنک اُس پاپ-اپ سے مماثلت نہیں رکھتا ہے تو آپ اُس پر کلک نہ کریں۔ موبائل آلات میں اپنی انگلی اُس لنک پر لے جا کر دبائے رکھنے سے آپ کو وہی پاپ-اپ نظر آئے گا۔ اس سے بھی زیادہ محفوظ طریقہ یہ ہے کہ آپ اُس پورے یو-آر-ایل کو ای-میل سے کاپی کر کے اپنے براؤزر میں پیسٹ کریں یا خود صحیح لنک لکھیں۔
- آپ کو اپنے کسی جاننے والے سے ای-میل موصوُل ہوئی ہے لیکن اُس کا اندازِبیان ایسا نہیں لگتا کہ یہ اُس شخص نے بھیجی ہے۔ اگر آپ کو پھر بھی شک ہے تو ای-میل بھیجنے والے کو فوُن کر کے تصدیق کرلیں۔ ایک سائبر مُجرم کے لیئے ایسی ای-میل تخلیق کرنا بہت آسان ہے جو کہ لگے کہ وہ آپ کے کسی دوست یا ساتھ کام کرنے والے کی طرف سے آئی ہے۔

اگر آپ کو لگتا ہے کہ کوئی ای-میل یا پیغام فشنگ حملہ ہے تو آپ اُسے حذف کردیں- بالآخر عام فہم ہی آپ کے لیئے 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 http://www.securingthehuman.org (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 انجینیئرنگ:	https://www.securingthehuman.org/ouch/2014#november2014
محفوظ رھنے کے پانچ اقدمات:	https://www.securingthehuman.org/ouch/2014#october2014
میں ہیک ہوچکا ہوں، اب کیا کرنا ہے؟:	https://www.securingthehuman.org/ouch/2014#may2014
آن گارڈ آن لائن:	https://www.onguardonline.gov/phishing
SANS کی آج کی سکیورٹی تجویز:	https://www.sans.org/tip_of_the_day.php

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

ترجمہ: شعیب ہاشمی