OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

فِشنگ کو روکیں

جائزہ

ای میل اور پیغام رسانی کی سروسز (جیسے کہ اسکائپ، ٹوئیٹر یا اسنیپ چیٹ) ہماری مواصلات کے بنیادی طریقوں میں سے ایک ہیں- ہم نہ صرف اپنے کام کے لیئے ان ٹیکنالوجیز کا ہر روز استعمال کرتے ہیں بلکہ اپنے دوستوں اور خاندان سے رابطے میں رہنے کے لیئے بھی اس کا استعمال کرتے ہیں- چونکہ دنیا بھر میں کافی سارے لوگ ان ٹیکنالوجیز پر انحصار کرتے ہیں اس لیئے یہ سائبر حملہ آوروں کے لیئے بنیادی طریقوں میں سے ایک طریقہ بن گیا ہے- ان طریقوں میں سے ایک فِشنگ کہلاتا ہے- اس بات سے قطع نظر کہ آپ گھر میں ہیں یا دفتر میں، آپ کو فِشنگ کے بارے میں علم ہونا چاہیئے اور یہ بھی معلوم ہونا چاہیئے کہ اس کی شناخت کس طرح کرنی ہے اور اس طرح کے حملوں کو کیسے روکنا ہے-

فشنگ کیا ہے؟

فِشنگ، حملے کی ایک ایسی قسم ہے جس میں ای میل یا پیغامات کی سروس کے استعمال کے ذریعے آپ کو بیوقوف بنانے کی کوشش کی جاتی ہے جیسے کہ کسی مضر لنک پر کلک کرنا، اپنے پاس ورڈ کا کسی سے اشتراک کرنا یا کسی متاثرہ ای میل اٹیچمنٹ کو کھولنا- حملہ آور ان پیغامات کو سچ ثابت کرنے کے لیئے بہت محنت کرتے ہیں اور ان کی کوشش ہوتی ہے کہ وہ آپ کو جذباتی کر دیں، آپ کو عجلت کا احساس دلائیں یا آپ کے تجسّس کو بڑھائیں- وہ اس پیغام کو ایسا بنا کے پیش کرتے ہیں جیسے کہ وہ کسی ایسی جگہ سے آیا ہے جسے آپ جانتے ہیں جیسے کہ آپ کے دوست کی طرف سے یا کسی ایسی قابل بھروسہ کمپنی کی جانب سے جسے آپ اکثر استعمال کرتے ہیں- یہ بھی ہو سکتا ہے کہ وہ کسی بینک کا لوگو ساتھ لگا کر پیغام بھیجیں یا وہ کوئی جعلی ای میل ایڈریس بھی استعمال کر سکتے ہیں تاکہ ان کا پیغام دیکھنے میں سچ لگے- حملہ آور پھر ان پیغامات کو لاکھوں لوگوں کو بھیجتے ہیں- انہیں یہ نہیں پتہ ہوتا ہے کہ کون ان کا شکار بنے گا، وہ صرف یہ جانتے ہیں کہ وہ جتنے زیادہ لوگوں کو پیغامات بھیجیں گے اتنے ہی زیادہ لوگ ان کا شکار بن سکتے ہیں-

اپنی حفاظت کرنا

تقریباً تمام صورتوں میں ای میل یا کسی پیغام کو کھولنا اور پڑھنا ٹھیک ہے- فِشنگ حملے کو کامیاب بنانے کے لیئے برے لوگ یہ چاہتے ہیں کہ وہ آپ سے دھوکہ دہی کے ذریعے کوئی غلط قدم اٹھوائیں- خوش قسمتی سے کچھ ایسے اشارے ہیں جن سے پتہ چل جاتا ہے کہ کوئی پیغام فِشنگ حملہ ہے یا نہیں- آپ مندرجہ ذیل مشترکہ نشانیاں ملاحظہ فرمائیں:

- جب کوئی آپ کو شدید عجلت کا احساس دلائے، آپ سے «فوری طور پر کوئی قدم» اٹھانے کا کہے تاکہ آپ کے ساتھ کچھ برا نہیں ہو جیسے کہ آپ کے کسی اکاؤنٹ کا بند ہونا یا آپ کو جیل بھجوانا- حملہ آور کی کوشش ہوتی ہے کہ وہ آپ سے جلد بازی میں کوئی غلطی سرزد کروا دے-
- کوئی آپ پر اپنی تنظیم سے متعلق پالیسیز اور کام کرنے کے طریقہ کار کو بالائے طاق رکھنے کے لیئے آپ پر دباؤ ڈالے-
- کوئی آپ کو شدید تجسّس کا احساس دلائے یا کوئی ایسی بات بتائے جو سچ نہیں لگ رہی ہو (جیسے کہ آپ نے لاٹری جیت لی ہے جو کہ سچ نہیں ہے)-
- عام طریقے سے مخاطب کرنا جیسے «معزز صارف»- زیادہ تر تنظیموں یا آپ کے دوستوں کو، جو آپ سے رابطہ کرتے ہیں، آپ کا نام پتہ ہوتا ہے-

- جب کوئی آپ سے بہت حسّاس معلومات مانگ رہا ہو جیسے کہ آپ کا کریڈٹ کارڈ نمبر یا پاس ورڈ یا کوئی اور ایسی معلومات جو کہ بھیجنے والے کو پہلے سے معلوم ہونی چاہیئے، تو اس صورتحال میں آپ اس بات کو یقینی بنائیں کہ معلومات مانگنے والا وہی شخص ہے جس کا وہ دعوہ کر رہا ہے۔
- کوئی پیغام آپ سے یہ کہہ رہا ہو کہ وہ کسی سرکاری تنظیم کی جانب سے بھیجا گیا ہے لیکن اس میں گرائمر کی غلطیاں ہوں یا ذاتی ای میل ایڈریس کا استعمال کیا گیا ہو جیسے کہ @gmail.com۔
- اگر کوئی پیغام کسی سرکاری ای میل (جیسے کہ آپ کے اعلی افسر) کی جانب سے بھیجا گیا ہے لیکن oT-ylpeR (جواب) میں کسی کا ذاتی ای میل ایڈریس لکھا ہوا ہے۔
- آپ کو اپنے کسی جاننے والے کی جانب سے کوئی پیغام موصول ہوتا ہے لیکن اس میں جو لب و لہجہ یا الفاظ استعمال کے گئے ہوتے ہیں ان سے یہ نہیں لگتا کہ وہ اس کی جانب سے بھیجا گیا ہے۔ اگر آپ کو شک ہو تو بھیجنے والے کو کال کر کے اس بات کی تصدیق کر لیں کہ وہ اس نے ہی بھیجا ہے کیونکہ سائبر حملہ آور کے لیئے کوئی ایسا پیغام تخلیق کرنا بہت آسان ہے جس سے یہ تأثر جائے کہ وہ آپ کے کسی دوست یا آپ کے دفتر میں ساتھ کام کرنے والے کسی شخص کی جانب سے آیا ہے۔

ان تجاویز پر عمل کر کے آپ اپنے آن لائن تجربے کو کافی حد تک محفوظ بنا سکتے ہیں۔ سوشل میڈیا سائٹس کے محفوظ استعمال یا کسی غیر مجاز سرگرمی کی اطلاع دینے کے لیئے آپ اس سوشل میڈیا سائٹ کے سکیورٹی سے متعلق صفحے کا دورہ کریں۔

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

ٹونیا ڈاڈلی ۲۰۱۱ سے سکیورٹی سے آگاہی سے متعلق پروگرامز بنا رہی ہیں اور انہیں کامیابی سے چلا رہی ہیں جن میں انعام یافتہ فِشنگ کی تربیت کا پروگرام بھی شامل ہے۔ آپ ان تک www.linkedin.com/in/toniadudley کے ذریعے رابطہ کر سکتے ہیں۔

وسائل:

سوشل انجینرنگ:	https://www.sans.org/u/Cb1
دورسوں کو اُن کی حفاظت میں مدد فراہم کرنا:	https://www.sans.org/u/Cb6
ای-میل سے متعلق کیا کرنا چاہیئے اور کیا نہیں:	https://www.sans.org/u/Cbg
سی ای او فراڈ:	https://www.sans.org/u/Cbl
OUCH! ترجمے اور آرکائیوز:	https://www.sans.org/u/Cbq

لائسنس