SANS SECURITY AWARENESS

OUCH!

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

# جی ہاں، آپ نشانے پر ہیں

## جائزہ

کئی لوگوں کو یہ غلط فہمی ہوتی ہے کہ وہ سائبر حملہ آوروں کے نشانہ پر نہیں ہیں اور ان کے سسٹمز یا اکاؤنٹس کی کوئی حیثیت نہیں ہے- اس بات میں کوئی حقیقت نہیں ہے- اگر آپ اپنے گھر یا دفتر میں ٹیکنالوجی کا کسی بھی طریقے سے استعمال کرتے ہیں تو یقین کریں کہ بُرے لوگوں کے نزدیک آپ کی اہمیت ہے لیکن آپ کی قسمت اچھی ہے- آپ کے پاس ان سائبر حملہ آوروں سے تحفّظ کا سب سے بہترین ذریعہ پہلے سے موجود ہے اور وہ آپ خود ہیں-

## آپ کیوں نشانے پر ہیں؟

آج انٹرنیٹ پر طرح طرح کے سائبر حملہ آور موجود ہیں اور اُن سب کے مختلف مُحرّکات ہوتے ہیں- پھر یہ آپ کو نشانہ کیوں بنائیں گے؟ آپ کو ہیک کرنے سے اُنہیں اپنے مقصد میں کامیاب ہونے میں مدد ملے گی- سائبر حملہ آوروں کی آپ کو نشانہ بنانے کی دو بہت ہی عام مثالیں مندرجہ ذیل بیان کی گئی ہیں:

⚠ **سائبر مجرم**: ان لوگوں کا مقصد زیادہ سے زیادہ پیسے کمانا ہے- جو چیز انٹرنیٹ کو ان کے لیئے قیمتی بناتی ہے وہ یہ ہے کہ اس کے ذریعے وہ دنیا بھر میں کسی کو بھی صرف ایک بٹن دبا کر نشانہ بناسکتے ہیں- ایسے بے تحاشہ طریقے موجود ہیں جن کے ذریعے وہ آپ سے پیسے کما سکتے ہیں- مثال کے طور پر آپ کے بینک یا ریٹائرمنٹ اکاؤنٹ سے پیسے چرانا، آپ کے نام پر کریڈٹ کارڈ بنانا اور اس کا بل بھیجنا، آپ کا کمپیوٹر استعمال کر کے دوسرے لوگوں کو ہیک کرنا، آپ کے سوشل میڈیا یا گیمنگ اکاؤنٹس کو چوری کر کے دوسرے مجرمان کو بیچنا اس میں شامل ہے- بُرے لوگوں کے آپ سے پیسے کمانے کے بےتحاشہ طریقے ہیں اور یہ شاید ایک نہ ختم ہونے والی فہرست ہے- ہزاروں لاکھوں کی تعداد میں ایسے بُرے لوگ موجود ہیں جو ہر صبح اس مقصد کے لیئے اٹھتے ہیں کہ وہ ہر دن جتنے زیادہ لوگوں کو ہو سکے ہیک کر لیں، بشمول آپ کے-

☆ **مخصوص حملہ آور**: یہ اعلیٰ تربیت یافتہ حملہ آور ہوتے ہیں جو کہ اکثر حکومتوں، جرائم پیشہ عناصر یا آپ کے حریفوں کے لیئے آپ کو دفتر میں نشانہ بناتے ہیں- شاید آپ کو لگتا ہو کہ آپ کی دفتری معلومات کسی کی توجہ کا مرکز نہیں ہیں لیکن آپ اس کے بارے میں سن کر بہت حیران ہوں گے-

- مختلف تنظیموں یا حکومتوں کے نزدیک ان معلومات کی بہت زیادہ اہمیت ہوتی ہے جو آپ کے دفتر میں موجود ہیں-

- مخصوص حملہ آور آپ کو دفتر میں اس لیئے نشانہ نہیں بناتے ہیں کہ وہ آپ کو ہیک کرنا چاہتے ہیں، بلکہ اس لیئے تاکہ آپ کے ذریعے وہ آپ کے ساتھ کام کرنے والے لوگوں یا دوسرے سسٹمز کو ہیک کر سکیں۔
- یہ مخصوص حملہ آور آپ کے ساتھ کام کرنے والی دوسری تنظیموں کی وجہ سے بھی آپ کو نشانہ بنا سکتے ہیں۔

## میرے پاس اینٹی-وائرس ہے اس لیئے میں محفوظ ہوں

ٹھیک ہے میں اگر کسی کے نشانے پر ہوں تو کوئی مسئلہ نہیں ہے۔ مجھے اپنے کمپیوٹر پر صرف ایک اینٹی-وائرس اور ایک فائروال انسٹال کرنا ہے اور میں محفوظ ہو جاؤں گا، کیا ایسا ہی ہے؟ بدقسمتی سے ایسا نہیں ہے۔ کئی لوگوں کو لگتا ہے کہ اگر وہ سکیورٹی سافٹ ویئر انسٹال کر دیں گے تو وہ محفوظ ہو جائیں گے۔ بدقسمتی سے یہ مکمّل درست بات نہیں ہے۔ سائبر حملہ آور دن بدن بہتر ہوتے جا رہے ہیں اور ان کے حملوں کے کئی طریقے سکیورٹی ٹیکنالوجیز کو با آسانی پار کر سکتے ہیں۔ مثال کے طور پر اکثر وہ ایک خاص میلویئر بناتے ہیں جس کی تشخیص آپ کا اینٹی-وائرس نہیں کر سکتا ہے۔ وہ آپ کے ای میل فلٹرز کو اپنی مرضی کے مطابق بنائے گئے فشنگ حملے کے ذریعے پار کرتے ہیں یا آپ کو فون کال کے ذریعے بیوقوف بنا کر یا دھوکہ دہی کے ذریعے آپ کا کریڈٹ کارڈ، پیسے یا پاس ورڈ نکلوا لیتے ہیں۔ ٹیکنالوجی آپ کی حفاظت میں بہت اہم کردار ادا کرتی ہے لیکن آخر میں آپ خود ہی اپنا بہترین دفاع ہیں۔

خوش قسمتی سے محفوظ بننا اتنا مشکل نہیں ہے، بلآخر عام فہم اور کچھ بنیادی رویّے ہی آپ کا بہترین دفاع ہیں۔ اگر آپ کو کوئی ای میل، پیغام یا فون کال موصول ہوتی ہے جو شدید عجلت کا احساس دلا رہی ہو، عجیب لگ رہی ہو یا مشکوک لگ رہی ہو تو ہو سکتا ہے کہ یہ ایک حملہ ہو۔ اپنے کمپیوٹرز اور دوسرے آلات کی حفاظت کو یقینی بنانے کے لیئے آپ ان میں خودکار اپڈیٹ کو فعّال کر دیں۔ آخری بات یہ کہ آپ اپنے ہر اکاؤنٹ کے لیئے ایک مضبوط اور منفرد پاس ورڈ کا استعمال کریں۔ سائبر آگاہی ہی آپ کا بہترین دفاع ہے۔ اگر آپ کو اس بات کا اندازہ نہیں ہے کہ کہاں سے شروع کرنا چاہیئے تو ہمارا مشورہ ہے کہ آپ ماہانہ OUCH! نیوز لیٹر کو sans.org/ouch کے ذریعے سبسکرائب کر کے پہلا قدم اٹھائیں۔

## 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

میٹ برومائیلی (@mbromileyDFIR) انسیڈنٹ ریسپانڈر اور ڈیجیٹل فارنزیک کے ماہر ہیں اور اپنے پاس دنیا بھر کی مختلف تنظیموں اور واقعات پر کام کرنے کا آٹھ سالوں سے زیادہ کا تجربہ رکھتے ہیں۔ میٹ ڈیجیٹل فارنزیک اور انسیڈنٹ رسپانس کے مُعلّم ہیں اور SANS میں یہ دونوں کورسز FOR58 اور FOR572 پڑھاتے ہیں۔

SANS SECURITY AWARENESS

## وسائل:

میلویئر کو روکیں: https://www.sans.org/u/L1J
سوشل انجینئرنگ: https://www.sans.org/u/L1O
فون کال کے ذریعے دھوکہ دہی: https://www.sans.org/u/L1T
پاس فریزز: https://www.sans.org/u/L1Y
پوسٹر - آپ نشانے پر ہیں: https://www.sans.org/u/L23