SANS SECURITY AWARENESS

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

کیا میں ہیک ہو چکا ہوں؟

جائزہ

آپ جتنے بھی محفوظ کیوں نہ ہو جائیں، یہ بالکل ایسا ہی ہے جیسے آپ گاڑی چلا رہے ہیں اور کبھی نہ کبھی آپ کو کوئی حادثہ پیش آ جائے گا۔ مندرجہ ذیل کچھ ایسے اشارے بیان کئے گئے ہیں جو اس بات کی نشاندہی کریں گے کہ آیا آپ ہیک ہوئے ہیں یا نہیں اور اگر ہوئے ہیں تو آپ کو کیا اقدامات اٹھانے چاہیئے۔ جتنی جلدی آپ اس بات کی نشاندہی کر لیں گے کہ کچھ برا ہوا ہے، اتنا ہی جلدی آپ کے لیئے اس کا حل نکالنا آسان ہو گا۔

ہیک ہو جانے کی علامات

آپ کا اینٹی-وائرس پروگرام الرٹ بھیج رہا ہے کہ آپ کا سسٹم متاثر ہو چکا ہے۔ آپ اس بات کی یقین دہانی کر لیں کہ آپ کا اینٹی وائرس سافٹ ویئر ہی یہ الرٹ بھیج رہا ہے، نہ کہ کسی ویب سائٹ کا کوئی پاپ اپ ونڈو، جو کہ آپ کو بیوقوف بنا کر کسی نمبر پر کال کرنے یا کوئی چیز انسٹال کرنے کا کہتا ہے۔ آپ کو یقین نہیں آ رہا ہے؟ اس کا بہترین حل یہ ہے کہ آپ اپنا اینٹی وائرس پروگرام کھول لیں۔

آپ کے سامنے ایک پاپ اپ ونڈو آتی ہے جو یہ کہتی ہے کہ آپ کا کمپیوٹر انکرپٹ ہو چکا ہے اور اگر آپ کو اپنی فائلز واپس چاہیئے تو آپ کو اس کا تاوان ادا کرنا پڑے گا۔

آپ کا براؤزر آپ کو ان ویب سائٹس پر لے جا رہا ہے جس پر آپ جانا نہیں چاہتے ہیں۔

آپ کا کمپیوٹر یا ایپلیکیشنز مسلسل کریش ہو رہی ہیں، آپ کے پاس نامعلوم ایپلیکیشنز کے آئیکنز نظر آ رہے ہیں یا کچھ عجیب طرح کی ونڈوز نمودار ہو رہی ہیں۔

آپ کا پاس ورڈ مزید کام نہیں کر رہا ہے حالانکہ آپ کو پتہ ہے کہ وہ درست ہے۔

آپ کے دوست آپ سے پوچھتے ہیں کہ آپ انہیں بہت ساری اسپیم ای میلز کیوں بھیج رہے ہیں حالانکہ آپ کو پتہ ہے کہ آپ نے نہیں بھیجی ہیں۔

آپ کے کریڈٹ کارڈ سے کچھ پیسے چارج ہو گئے ہیں یا آپ کے بینک اکاؤنٹ سے کچھ پیسے نکلے ہیں جو کہ آپ نے نہیں نکالے ہیں۔

کیا کرنا چاہیئے؟

اگر آپ کو گمان ہو کہ آپ ہیک ہو چکے ہیں تو آپ جتنی جلدی اقدامات اٹھانا شروع کریں گے اتنا اچھا ہو گا۔ اگر ہیکنگ آپ کے دفتر سے متعلق ہے تو آپ مسئلے کو خود حل کرنے کی کوشش نہیں کریں بلکہ اس کی اطلاع فوری طور پر متعلقہ شعبے کو دیں۔ اگر آپ کا ذاتی سسٹم یا اکاؤنٹ ہیک ہو گیا ہے تو آپ مندرجہ ذیل اقدامات اٹھا سکتے ہیں:

اپنا پاس ورڈ تبدیل کر دیں: آپ نہ صرف اپنے کمپیوٹرز اور موبائل آلات بلکہ اپنے آن لائن اکاؤنٹس کے پاس ورڈ بھی تبدیل کر دیں۔ آپ ہیک شدہ کمپیوٹر استعمال کرتے ہوئے اپنے پاس ورڈز تبدیل نہیں کریں بلکہ اس مقصد کے لیئے ایسے مختلف سسٹم کا انتخاب کریں جو محفوظ ہو۔ اگر آپ کے پاس کافی سارے اکاؤنٹس ہیں تو آپ سب سے اہم اکاؤنٹس سے ابتدا کریں۔ اگر آپ اپنے تمام پاس ورڈز کو یاد نہیں رکھ سکتے ہیں تو آپ پاس ورڈ مینیجر کا استعمال کریں۔

مالیاتی: اپنے کریڈٹ کارڈ یا مالیاتی اکاؤنٹس میں کسی قسم کے مسئلے کی صورت میں آپ اپنے بینک یا کریڈٹ کارڈ کی کمپنی سے فوری طور پر رابطہ کریں- آپ ان کے کسی قابل بھروسہ فون نمبر پر کال کریں، جیسے کہ آپ کے بینک کارڈ کی پچھلی جانب دیئے گئے نمبر پر، آپ کی مالی تفصیلات کی دستاویز پر موجود نمبر پر یا کسی قابل بھروسہ کمپیوٹر کے ذریعے ان کی ویب سائٹ پر دیئے گئے نمبر پر- اس کے علاوہ آپ اپنی کریڈٹ فائلز کو منجمد (Credit Freeze) کرنے پر غور کریں-

اینٹی وائرس: اگر آپ کا اینٹی وائرس سافٹ ویئر آپ کو کسی فائل کے متاثر ہونے کی اطلاع دیتا ہے تو آپ اس کی دی ہوئی تجویز پر عمل کریں- زیادہ تر اینٹی وائرس سافٹ ویئر میں لنکس دیئے گئے ہوتے ہیں جن کے ذریعے آپ اس انفیکشن کے بارے میں مزید معلومات حاصل کر سکتے ہیں-

دوبارہ انسٹال کرنا: اگر آپ کسی متاثرہ کمپیوٹر کی مرمّت کرنے سے قاصر ہیں یا اس بات کی مزید یقین دہانی کرنا چاہتے ہیں کہ آپ کا سسٹم محفوظ ہے تو آپ آپریٹنگ سسٹم کو دوبارہ انسٹال کریں- اس بات کا خیال رہے کہ آپ اسے بیک اپس کے ذریعے ری انسٹال نہیں کر رہے ہیں کیونکہ بیک اپس کو صرف اپنی ذاتی فائلز کو بحال کرنے کے لیئے استعمال کرنا چاہیئے- اگر آپ ری انسٹال کرنے میں غیر آرامدہ محسوس کر رہے ہیں تو آپ کسی پیشہ ورانہ سروس کی مدد حاصل کریں یا اگر آپ کا کمپیوٹر یا آلہ پرانہ ہے تو اس صورت میں نیا آلہ خریدنا زیادہ آسان ہو گا- بالآخر جب آپ اپنے سسٹم کو واپس بنا لیں یا نیا خرید لیں تو اس بات کی یقین دہانی کر لیں کہ وہ اپڈیٹ ہو اور جب بھی ممکن ہو اس میں خودکار اپڈیٹ کو فعال کر دیں-

بیک اپس: وقت سے پہلے اپنی حفاظت کے لیئے ایک اہم قدم باقاعدگی سے بیک اپس لینا ہے- کئی ایسے حل موجود ہیں جو آپ کی فائلز کو خود کار طور پر روزانہ یا کبھی کبھی ہر گھنٹے پر بیک اپ کرتے ہیں- اس بات سے قطع نظر کہ آپ کون سا حل استعمال کر رہے ہیں، آپ وقتاً فوقتاً اپنی فائلز کو بحال کر کے دیکھتے رہا کریں کیونکہ اکثر بیک ہونے کے بعد بیک اپس وہ واحد ذریعہ رہ جاتے ہیں جس کے ذریعے آپ اپنی معلومات کو بحال کر سکتے ہیں-

قانون کا نفاذ: اگر آپ کو کسی بھی طرح سے خطرہ محسوس ہوتا ہے تو آپ اس واقعے کی اطلاع قانون نافذ کرنے والے اداروں کو دیں- اگر آپ شناخت کی چوری کا شکار ہو چکے ہیں اور امریکہ میں رہتے ہیں تو آپ https://www.identitytheft.gov 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

ڈاکٹر جوہانس الرچ (@johullrich) ٹیکنالوجی انسٹیٹیوٹ میں ریسرچ کے ڈین اور SANS انٹرنیٹ اسٹورم سینٹر کے ڈائریکٹر اور SANS فیلو ہیں- انہوں نے DShield Collabrative Sensor Network تخلیق کیا ہے اور وہ انٹرنیٹ اسٹورم سینٹر میں روزانہ نیٹ ورک سکیورٹی کی خبروں کی پاڈکاسٹ کی میزبانی کرتے ہیں-

وسائل:

بیک اپس: https://www.sans.org/u/JGP
پاس فریز: https://www.sans.org/u/JGU
پاس ورڈ مینیجرز: https://www.sans.org/u/JGZ
میلویئر کیا ہے؟: https://www.sans.org/u/JH4
کریڈٹ منجمد کرنا (Credit Freeze): https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/