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

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- آپ کے ہیک ہونے کی نشاندہی
- آپ کا ردّعمل

میں ہیک ہو چکا ہوں، اب؟

جائزہ

ہمیں معلوم ہے کہ آپ کو اپنے کمپیوٹر اور موبائل آلات کا خیال ہے اور آپ اس سلسلے میں کچھ اقدامات بھی اٹھاتے ہیں۔ تاہم آپ ٹیکنالوجی کو جتنا بھی حفاظت سے استعمال کریں، آج یا کل آ پ ہیک یا مُتأثر ہو سکتے ہیں- اس شمارے میں آپ یہ سیکھیں گے کہ آپ کس طرح اس بات کا تعیّن کر سکتے ہیں کہ آپ کا کمپیوٹر یا موبائل آلہ ہیک ہو گیا ہے اور اگر ایسا ہے تو آپ اس صورت حال میں کیا اقدامات اُٹھائیں گے۔ بالآخر آپ جتنا جلدی اس بات کی نشاندہی کریں گے کہ کچھ غلط ہے اور جتنا جلدی اُس مسئلے کا حل نکالیں گے اُتنا ہی زیادہ کسی سائبر مجرم کے لیۓ آپ کو نُقصان پہنچانے کے امکانات کم ہو جائیں گے۔

مہمان ایڈیٹر

سیمینتھا ڈےویسن (@sam_e_davison) اُوبر میں ‹سکیورٹی سے آگاہی اور اُس کی تعلیم› کی پروگرام مینیجر ہیں جہاں وہ دنیا بھر میں ۳۵۰ سے زائد شہروں میں پھیلے مُلازمین کو تعلیم فراہم کرتی ہیں-

آپ کے ہیک ہونے کی نشاندہی

اس بات کا اندازہ لگانا مشکل ہو سکتا ہے کہ آپ ہیک ہو گئے ہیں کیونکہ کوئی ایسا ایک طریقہ موجود نہیں ہے جس کے ذریعے آپ اس بات کی تصدیق کر سکیں۔ اس کے بجائے اکثر ہیکرز خود ہی کئی سُراغ چھوڑ جاتے ہیں جو کہ «انڈیکیٹرز» (علامات) کہلاتے ہیں۔ آپ کے سسٹم میں اگر مُندرجہ ذیل علامات میں سے کسی سے بھی مُماثلت پائی جاتی ہے تو اس بات کے امکانات زیادہ ہیں کہ وہ ہیک ہو گیا ہے۔

- آپ کے اینٹی وائرس پروگرام نے ایک الرٹ جاری کیا ہے کہ آپ کا سسٹم مُتأثر ہو گیا ہے خُصوصاً جب وہ یہ بھی کہے کہ وہ اُن مُتأثرہ فائلز کو حذف یا کُوارنٹائن نہیں کر سکا ہے۔
- آپ کے براؤزر کا ہوم پیج غیر متوقع طور پر تبدیل ہو گیا ہے یا آپ کا براؤزر آپ کو ایسی ویب سائٹس پر لے کر جا رہا ہے جن پر آپ جانا نہیں چاہتے ہیں۔
- آپ کے کمپیوٹر یا آلا ت پر ایسے نئے اکاؤنٹس بن گئے ہیں جنہیں آپ نے نہیں بنایا ہے یا ایسے نئے پروگرامز چل رہے ہیں جنھیں آپ نے انسٹال نہیں کیا ہے۔
- آپ کا کمپیوٹر یا ایپلیکیشنز متواتر بند ہو رہی ہیں، آپ کے پاس نا معلوم ایپلیکیشنز کے آئیکنز یا عجیب ونڈوز بار بار آپ کے سامنے نمودار ہو رہی ہیں-
- ایک پروگرام آپ سے آپ کے سسٹم میں تبدیلی کرنے کے لیئے اس وقت اجازت مانگتا ہے جب آپ کسی ایپلیکیشن کو انسٹال یا اپڈیٹ نہیں کر رہے ہوتے ہیں۔
- آ پ کا پاس ورڈ آپ کے سسٹم یا کسی آن لائن اکاؤنٹ میں نہیں چل رہا ہے، حالانکہ آ پ کو پتہ ہے کہ وہ صحیح ہے۔
- آپ کے دوست آپ سے پوچھ رہے ہیں کہ آپ کیوں اُنھیں اسپیم ای-میلز بھیج رہے ہیں جبکہ آپ کو پتہ ہے کہ آپ نے کوئی ای-میل نہیں بھیجی ہے-

میں ہیک ہو چکا ہوں، اب؟

- آپ کا موبائل آلہ پریمیئم ایس-ایم-ایس نمبرز پر بغیر اجازت ایس-ایم-ایس بھیج رہا ہے جس کی وجہ سے آپ کے پیسے کٹ رہے ہیں۔
- آپ کے آلہ پر غیر متوقع طور پر اچانک سے ڈیٹا اور بیٹری کا استعمال بڑھ گیا ہے۔

آج یا کل آپ کا کمپیوٹر یا آلہ مُتأثر ہو سکتا ہے، اس لیئے آپ جتنا جلدی کسی واقعے کی تشخیص کر لیں گے اور اُس کے بارے میں اقدامات اُٹھائیں گے، اُتنا ہی بہتر ہوگا۔

آپ کا ردّعمل

اگر آپ کو لگتا ہے کہ آپ کا کمپیوٹر یا آلہ ہیک ہو چکا ہے تو آپ جتنا جلدی اُس کا ردّعمل دیں گے اُتنا ہی اچھا ہوگا۔ اگر وہ کمپیوٹر یا آلہ آپ کی تنظیم کی طرف سے دیا گیا ہے یا وہ صرف کام کے لیئے استعمال ہوتا ہے تو اُسے آپ خود صحیح کرنے کی کوشش نہ کریں۔ ایسا کرنے سے آپ نہ صرف اُسے صحیح کرنے کے بجائے مزید نُقصان پہنچا سکتے ہیں بلکہ آپ تفتیش کے لیئے کارآمد شواہد کو بھی نُقصان پہنچا سکتے ہیں۔ اس کے بجائے آپ اس واقعے کی خبر ہیلپ ڈیسک، سکیورٹی ٹیم یا سُپروائزر کے ذریعے اپنی تنظیم کو فوراً دیں۔ اگر آپ کسی وجہ سے اپنی تنظیم سے رابطہ نہیں کر پا رہے ہیں یا آپ کو تاخیر کی وجہ سے پریشانی ہو رہی ہے تو آپ اپنے کمپیوٹر یا آلہ کو نیٹ ورک سے مُنقطع کر دیں اور پھر اُسے سلیپ، سسپینڈ یا ایروپلین موڈ میں ڈال دیں۔ اگر آپ اس بارے میں مُتأکد نہیں بھی ہیں کہ آپ ہیک ہو گئے ہیں، پھر بھی اس واقعے کی متعلقہ لوگوں کو فالفور خبر کریں۔ اگر کمپیوٹر یا آلہ آپ کے ذاتی استعمال کے لیئے ہے تو آپ مُندرجہ ذیل اقدامات اٹھا سکتے ہیں۔

- **پاس ورڈ تبدیل کردیں**: اس میں نہ صرف کمپیوٹر یا آلات، بلکہ آپ کے تمام آن لائن اکاؤنٹس کے پاس ورڈ تبدیل کرنا شامل ہیں۔ آپ اس بات کی یقین دہانی کرلیں کہ آپ ہیک شُدہ کمپیوٹر کے ذریعے پاس ورڈ تبدیل نہیں کر رہے ہیں۔ اس کے بجائے آپ کسی دوسرے کمپیوٹر یا آلہ کو استعمال کریں جس کے بارے میں آپ کو معلوم ہے کہ وہ پاس ورڈ کی تبدیلی کے لیئے محفوظ ہے۔
- **اینٹی وائرس**: اگر آپ کا اینٹی وائرس سافٹ ویئر آپ کو کسی مُتأثرہ فائل کے بارے میں مطلع کرتا ہے تو آپ اس کی بتائی ہوئی تجویز پر عمل کرسکتے ہیں۔ اس میں عمومُاً فائل کو کُوارنٹائن کرنا، صاف کرنا یا حذف کرنا شامل ہے۔ زیادہ تر اینٹی وائرس میں ایسے لنکس موجود ہوتے ہیں جن کے ذریعے آپ کسی مخصُوص انفیکشن کے بارے میں مزید معلومات حاصل کر سکتے ہیں۔ جب آپ کو کسی فائل کے بارے میں خدشہ ہو تو آپ اسے کُوارنٹائن کر دیں۔ اگر یہ مُمکن نہ ہو تو آ پ اُسے حذف کر دیں ۔
- **تعمیرنو**: اگر آپ کسی انفیکشن کو صحیح کرنے سے قاصر ہیں یا آپ مُتأکد ہونا چاہتے ہیں کہ آپ کا سسٹم صحیح ہو گیا ہے تو اس کا بہتر اور محفوظ طریقہ اس سسٹم کی تعمیرنو کرنا ہے۔ کمپیوٹر کے لیئے اپنے سسٹم کے مینوفیکچرر کی ہدایت پر عمل کریں۔ زیادہ تر صُورتوں میں اس کا مطلب پہلے سے موجود یوٹیلیٹیز کو استعمال کرتے ہوئے آپریٹنگ سسٹم کو پھر سے انسٹال کرنا ہے۔ اگر یہ یوٹیلیٹیز موجود نہیں ہوں، کرپٹ یا مُتأثرہ ہوں تو پھر آپ اپنے مینوفیکچرر سے رہنمائی کے لیئے رابطہ کریں یا اُن کی ویب سائٹ کا دورہ کریں۔ ہیک اپس کے ذریعے آپریٹنگ سسٹم کو پھر سے انسٹال نہیں کریں کیونکہ ہو سکتا ہے کہ اس میں بھی وہی کمزوریاں موجود ہوں جن کے ذریعے ہیکر نے پہلے اُس تک رسائی حاصل کی تھی۔ ہیک اپس کو صرف معلومات ریکوَر کرنے کے لیئے استعمال کرنا چاہئیے۔ موبائل آلات کے لیئے آپ اپنے آلہ کے مینوفیکچرر یا سروس پروائیڈر کی جانب سے دی گئی ہدایات پر عمل کریں، یہ اُن کی ویب سائٹ پر موجود ہوتی ہیں۔ کئی صورتوں میں یہ کام صرف آپ کے موبائل آلہ کو فیکٹری ڈیفالٹ پر ری-اسٹور کرنے سے ہو

میں ہیک ہو چکا ہوں، اب؟

جاتا ہے- اگر آپ تعمیرنو کے عمل سے غیر مُطمئن ہیں تو آپ کسی پروفیشنل سروس سے مددحاصل کرنے کے بارے میں سوچیں یا اگر آپ کا کمپیوٹر یا آلہ پرانا ہے تو اس صورت میں زیادہ آسان اور سستا طریقہ نیا کمپیوٹر یا آلہ خریدنا ہو سکتا ہے- آخر میں یہ کہ جب آپ اپنے کمپیوٹر یا آلہ کی تعمیر نو کر لیں یا نیا خرید لیں تو اس بات کی یقین دہانی کر لیں کہ وہ مُکمّل طور پر اپڈیٹڈ اور جدید ترین ہے اور جب بھی مُمکن ہو خود کار اپڈیٹنگ کو فعّال کر دیں-

- **بیک اپس**: اپنی حفاظت کے لیئے سب سے اہم ترین قدم جو آپ قبل از وقت اُٹھا سکتے ہیں وہ باقاعدگی سے بیک-اپ لینا ہے- آپ جتنے تواتر سے بیک-اپ لیں گے اُتنا ہی بہتر ہوگا- کُچھ ایسے حل موجود ہیں جو کہ کسی بھی نئی فائل کے آنے یا کسی فائل میں تبدیلی واقع ہونے پر ہر گھنٹے خوُدکار طور پر بیک-اپ لیتے ہیں- اس بات سے قطع نظر کہ آپ بیک-اپ کا کون سا حل استعمال کر رہے ہیں، آپ وقتاً فوقتاً اُن فائلز کو ری-اسٹور کر کے دیکھتے رہیں- بیک ہونے کے بعد اکثر بیک-اپ کے ذریعے معلومات ری کوؤر کرنا ہی واحد طریقہ رہ جاتا ہے-
- **قانون نافذ کرنا**: اگر آپ کو کسی بھی طرح سے کوئی بھی خطرہ محسوُس ہو رہا ہے تو آپ اس واقعے کی اطلاع مقامی قانوُن نافذ کرنے والے ادارے کو کریں-

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:

بیک اپس:	https://securingthehuman.sans.org/ouch/2015#august2015
پاس فریزز:	https://securingthehuman.sans.org/ouch/2015#april2015
میلویئر کیا ہے:	https://securingthehuman.sans.org/ouch/2016#march2016
اپنے نئے ٹیبلیٹ کو محفوظ بنانا:	https://securingthehuman.sans.org/ouch/2016#january2016

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

ترجمہ: شعیب ہاشمی