کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

انکرپشن:
- انکرپشن کیا ہے ؟
- ساکٹ انکرپشن
- متحرک انکرپشن

انکرپشن

انکرپشن کیا ہے؟

آپ شاید لوگوں کو"انکرپشن " کی اصطلاح استعمال کرتے ہوئے سنیں اور یہ بھی کہ آپ کو اُسکے ذریعے اپنے آپ کو اور اپنی معلومات کو کیسے محفوظ رکھنا ہے۔ انکرپشن کا تصور مبہم ہو سکتا ہے۔ اسکے علاوہ یہ کہ انکرپشن آپ کو ہر چیز سے محفوظ نہیں رکھ سکتی ہے، اس کی کچھ حدود ہیں۔ اس نیوز لیٹر میں ہمنے بہت آسان طریقے سے کچھ اصطلاحات بیا ن کی ہیں جیسے کہ انکرپشن کیا ہے، آپ کو اسے کیوں استعمال کر نا چاہیے اور اُسے صحیح طریقے سے کیسے نافذ کرنا چاہیے ۔

مہمان ایڈیٹر

کرسٹوفر کراؤلی (@CCrowMontance; +ChrisCrowley) واشنگٹن ڈی سی میں مقیم ایک کنسلٹنٹ ہیں۔ وہ SANS انسٹیٹیوٹ میں موبائل ڈیوائیس سیکیورٹی اور ایتھیکل ہیکنگ (SEC575)کے لیڈ انسٹرکٹر ہیں اور انسیڈینٹ رسپانس ٹیم مینیجمنٹ (MGT535) کے مصنف ہیں۔

آپ کی ڈیوائیس میں بہت ساری اہم معلومات ہوتی ہیں جیسے کہ مالی دستاویزات، تصاویر، ای۔ میل یا طبی معلومات۔ اگرآپ کی کوئی ڈیوائیس گم یا چوری ہو جاتی ہے تو جس کسی کے بھی ہاتھ لگتی ہے وہ آپ کی تمام اہم معلومات تک رسائی حاصل کر سکتا ہے۔ اسکے علاوہ ہو سکتا ہے کہ آپ آن لائن بہت اہم لین دین کریں جیسے کہ آن لائن بینکنگ یا خریداری۔ اگر سائبر حملہ آور آپ کی آن لائن سرگرمی پر نظر رکھتے ہیں تو وہ آپ کی تمام معلومات چُرا سکتے ہیں جیسے کہ آپ کا مالی اکاؤنٹ یا کریڈٹ کارڈ نمبر۔ انکرپشن آپ کو ایسی صورتِ حال میں حفاظت فراہم کرتی ہے اس بات کو یقینی بناتے ہوئے کہ کوئی بھی غیر مجاز شخص آپ کی معلومات تک رسائی یا اُس میں تبدیلی نہیں کر سکے۔

جب معلومات انکرپٹ نہیں ہوتی ہیں تو وہ «پلین ٹیکسٹ» کہلاتی ہیں۔ اس کا مطلب ہے کہ کوئی بھی اُسے پڑھ سکتا ہے یا اُس تک رسائی حاصل کر سکتا ہے۔ انکرپشن ان معلومات کو نہ پڑھے جانے والی شکل میں تبدیل کر دیتی ہے جسے «سایفرٹیکسٹ» کہتے ہیں۔ انکرپشن پیچیدہ ریاضیاتی قوائد اور ایک منفرد ‹کی› (چابی) کا استعمال کرتے ہوئے آپ کی معلومات سایفرٹیکسٹ میں تبدیل کر دیتی ہے۔ ‹کی› (چابی) آپ کی معلومات کو بند کرتی ہے یا کھولتی ہے بالکل اُسی طرح جس طرح ایک چابی دروازے کو بند یا کھول سکتی ہے- ‹کی› کی ایک عام مثال پاس ورڈ ہے- جن لوگوں کے پاس وہ پاس ورڈ ہوتا ہے صرف وہی لوگ آپ کی معلومات کو ڈیکرپٹ اور اس تک رسائی حاصل کرسکتے ہیں۔ اپنی انکرپٹڈ معلومات کو محفوظ رکھنے کے لیے آپ کو اپنی ‹کی› کو محفوظ کرنے کی ضرورت ہے- عموماً انکرپشن دو طرح سے کام کرتی ہے یعنی آپ ساکت معلومات (جیسے کہ آپ کے لیپ ٹاپ کی معلومات) اور متحرک معلومات (جیسے کہ آن لائن معلومات بھیجنا) کو انکرپٹ کر سکتے ہیں۔

ساکت معلومات کو انکرپٹ کرنا

ساکت معلومات کو انکرپٹ کرنے کا بنیادی مقصد آپ کی معلومات کی حفاظت کرنا ہے اس صورت میں جب آپ کا کمپیوٹر یا موبائل ڈیوائیس چوری یا گم ہو جائے- 15سال پہلے یہ مسئلہ نہیں تھا کیونکہ زیادہ تر کمپیوٹرز بڑے اور بھاری بھرکم ڈیسک ٹاپ آلات ہوتے تھے جنہیں کہیں بھی لے

انکرپشن

انکرپشن آپ کی معلومات کو محفوظ کرنے کا ایک مضبوط طریقہ ہے لیکن یہ اتنا ہی مضبوط ہے جتنا کہ آپ کی ‹کی› (چابی)۔

جانا بہت مشکل کام ہوتا تھا۔ آج زیادہ تر لیپ ٹاپس کا وزن صرف چند پاؤنڈز ہے جب کہ موبائل آلات کا وزن صرف چند اونس ہے- یہ آلات بہت زیادہ طاقتور ہوتے ہیں اور بڑی تعداد میں معلومات رکھتے ہیں لیکن یہ بہت آسانی سے گم بھی ہوسکتے ہیں- اس کے علاوہ دوسرے موبائل میڈیا جیسے کہ USB, Flash Drive یا CD Rom اہم معلومات رکھ سکتے ہیں- ان آلات پر معلومات کو انکرپٹ کرنے کا ایک عام طریقہ Full Diskانکرپشن (ایف۔ ڈی۔ای) کہلاتا ہے- اس کا مطلب ہے کہ سسٹم میں موجود ہر چیز خود بہ خود انکرپٹ ہوجاتی ہے اور آپ کو یہ فیصلہ نہیں کرنا پڑتا ہے کہ کیا انکرپٹ کرنا ہے اور کیا نہیں۔ آج کل زیادہ تر آپریٹنگ سسٹم پہلے سے موجود Full Diskانکرپشن کے ساتھ آرہے ہیں- آپ کو صرف اُسے فعال کرنا پڑتا ہے، مثال کے طور پر میک OS X میں ‹فائل والٹ›(FileVault) موجود ہوتا ہے جبکہ ونڈوز کے کچھ ورژنز میں ‹بٹ لاکر›(Bitlocker) ہوتا ہے۔ اگر آپ کا کمپیوٹر Full Diskانکرپشن کی حمایت کرتا ہے تو ہمارا پُرزور مشورہ ہے کہ آپ اسے فعال کر دیں- اس کے علاوہ زیادہ تر موبائل فونز Full Diskانکرپشن کی حمایت کرتے ہیں اپنے انٹرنل اسٹوریج آلات کے لیے مثلاً iOSجو کہ آئیفون اور آئی پیڈ کا آپریٹنگ سسٹم ہے, ایک بار پاس کوڈ مقررہونے کے بعد خودبہ خود Full Diskانکرپشن لاگو کر دیتا ہے- اس بارے میں جاننے کے لیے کہ آیا آپ کا کمپیوٹر یا دفتر کا موبائل ڈیوائیس Full Diskانکرپشن کی حمایت کر تا ہے, آپ اپنے ہیلپ ڈیسک یا سپروائزر سے رابطہ کریں- ذاتی کمپیوٹرز کے لیے آپ اپنے کمپیوٹر کے بنانے والے کمپنی سے رابطہ کریں یا آن لائن دستاویز کا جائزہ لیں۔

متحرک معلومات کو انکرپٹ کرنا

جب معلومات ایک جگہ سے دوسری جگہ منتقل ہورہی ہوتی ہے تو اُس وقت بھی غیر محفوظ ہوتی ہیں- اگر وہ انکرپٹ نہیں ہوتی ہیں تو کوئی بھی اُس کی نگرانی کر سکتا ہے اور اُسے آن لائن حاصل کر سکتا ہے- اس لیے آپ کو اس بات کو یقینی بنانے کی ضرورت ہے کہ کوئی بھی اہم آن لائن مواصلات جیسے کے آن لائن بینکنگ ، ای میل بھیجنایہاں تک کہ سوشل میڈیا ویب سائٹ تک رسائی انکرپٹڈ ہو ۔ سب سے عام آن لائن انکرپشن کا طریقہ HTTPSہے ۔ ا س کا مطلب ہے کہ آپ کے براؤزر اور ویب سائٹ کے درمیان تمام ٹریفک انکرپٹڈ ہے ۔ آپ URLمیں https://: کو تلاش کریں ، براؤزر میں ایک لاک کو دیکھیں یا URLبار کو سبز ہوتا ہوا دیکھیں، یہ تمام علامات اس بات کی نشاندہی کرتی ہیں کہ مواصلات انکرپٹڈ ہے ہوسکتا ہے کہ کہیں آپ کو یہ تینوں چیزیں ایک ساتھ نظر آجائیں، اس کا انحصار آپ کے براؤزر اور ویب سائٹ پر ہے ، اس کے علاوہ یہ کہ آپ جب بھی عوامی وائے فائے سے منسلک ہو ں تو اس بات کا یقین کر لیں کہ جب بھی ممکن ہو انکرپشن کا استعمال کریں - آخر میں یہ کہ ای۔ میل بھیجتے اور وصول کرتے وقت آپ اس بات کا یقین کرلیں کہ آپ کا ای۔ میل کلائنٹ اس طرح ترتیب دیا گیا ہے کہ آپ کی ای۔ میل کو انکرپٹڈ چینل پر بھیج سکتا ہے زیادہ تر ای۔ میل کلائنٹس انکرپشن فراہم کرتے ہیں اس کے علاوہ آپ کی ISPابھی آپ کے ای۔ میل کلائنٹ پر انکرپشن کو فعال کرنے میں مدد فراہم کرسکتی ہے ۔

انکرپشن

صحیح طریقے سے انکرپشن کا نفاذ کرنا

اس بات سے قطع نظر کہ آپ کس طرح کی انکرپشن استعمال کر رہے ہیں یا کیسے استعمال کر رہے ہیں، تقریباً ہر طرح کی انکرپشن میں کچھ مشترکہ اقدامات ہوتے ہیں اُسے صحیح سے استعمال کرنے کے لیے۔

- آپ کی انکرپشن اُتنی ہی مضبوط ہے جتنی آپ کی ‹کی› (چابی) اگر کوئی آپ کی چابی کا اندازہ لگا لیتا ہے یا اُسے چُرا لیتا ہے تو وہ آپ کی معلومات تک رسائی حاصل کرسکتا ہے- آپ کو اپنی چابی کی حفاظت کرنی ہے ۔
- اگر آپ اپنی چابی کے لیے پاس کوڈ یا پاس ورڈ کا استعمال کر رہے ہیں تو اس بات کا یقین کرلیں کہ وہ لمبا اور محفوظ پاس ورڈ ہو اور اُسے گم یا بھول مت جائیں۔ اگر آپ اسے بھول جاتے ہیں تو آپ اپنی ہی معلومات سے ہاتھ دھو بیٹھیں گے۔ آپ کی انکرپشن اُتنی ہی مضبوط ہے جتنی آپ کے کمپیوٹر کی سیکیورٹی ، اگر آپ کے کمپیوٹر تک کسی نے رسائی حاصل کر لی ہے یا وہ متاثر ہو چکا ہے تو سائبر حملہ آور آپ کی انکرپشن کو توڑ سکتے ہیں اس لیے آپ اس بات کا یقین کر لیں کہی آپ کا کمپیوٹر یا موبائل ڈیوائیس محفوظ ہے ۔
- اگر آپ کو انکرپشن کے مختلف طریقے میّسر ہوتے ہیں تو آپ سب سے مضبوط ترین طریقہ اپنائیں ۔

مزید جانیئے:

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں، OUCH! archives تک رسائی حاصل کریں اور SANS سیکیورٹی سے مزید آگاہی کے لئے اس ویب سایٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سیکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سیکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لیے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'Like' کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

میک OS X فائل والٹ: http://support.apple.com/kb/ht4790

iOS انکرپشن: http://support.apple.com/kb/ht4175

اینڈرائیڈانکرپشن: http://www.androidauthority.com/how-to-encrypt-android-device-326700/

ونڈوزانکرپشن: http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

اپنے کمپیوٹر کو محفوظ کرنا: http://www.securingthehuman.org/ouch/2012#december2012

پاس ورڈ مینیجرز: http://www.securingthehuman.org/ouch/2013#october2013

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

ترجمہ: شعیب ہاشمی

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus