کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- انکرپشن کیا ہے؟
- آپ کیا اِنکرپٹ کر سکتے ہیں؟
- صحیح طریقہ کار

انکرپشن

انکرپشن کیا ہے؟

آپ نے شاید "انکرپشن"کی اصطلاح سنی ہو اور یہ بھی کہ اُس کے ذریعے آپ اپنی معلومات کی کس طرح حفاظت کرسکتے ہیں تاہم انکرپشن مُبہم بھی ہو سکتی ہیں اس لیئے آپ کو اس کی حدود کو سمجھنا چاہیئے- اس شُمارے میں ہم آپ کو آسان الفاظ میں انکرپشن کے بارے میں بتائیں گے کہ یہ کیا ہے اور کس طرح سے آپ کی حفاظت کر سکتی ہے اور اسے صحیح طریقے سے کیسے لاگُو کرنا چاہیئے-

مہمان ایڈیٹر

فرانسیسکا باسکو (@francibosco) ایک محقق اور پراجیکٹ آفیسر ہیں جو کہ سائبر جرائم اور سائبر سکیورٹی اور ٹیکنالوجی کے غلط استعمال سے متعلق منصوبوں کی دیکھ بھال کرتی ہیں- وہ اقوام متحدہ برائے علاقائی جرائم اور انصاف کی تحقیق کے انسٹیٹیوٹ میں کام کرتی ہیں اور "ٹیک اینڈ لاء سینٹر" کی شریک بانی ہیں-

آپ کےآلہ میں کافی بڑی تعداد میں حسّاس معلومات ہوتی ہیں، جیسے کہ ذاتی تصاویر اور ای-میلز- اگر آپ کا کوئی ایک آلہ گُم یا چوری ہو جائے تو اُس میں موجود تمام حسّاس معلومات تک وہ شخص رسائی حاصل کر سکتا ہے جس کے پاس وہ آلہ موجود ہے- مزید یہ کہ آپ آن لائن کُچھ حسّاس ٹرانزیکشنز بھی کر سکتے ہیں جیسے کہ بینکنگ یا خریداری- اگر کوئی آپ کی اِن سَرگرمیوں پر نظر رکھتا ہے تو وہ آپ کی معلومات کو چُرا بھی سکتا ہے جیسے کہ آپ کے مالی اکاؤنٹ یا کریڈٹ کارڈ کے نمبرز- انکرپشن آپ کو اِن حالات میں تحفظ فراہم کرتا ہے اِس بات کو یقینی بناتے ہوئے کہ غیرمجاز لوگ آپ کی معلومات تک رسائی یا اُس میں ردّو بدل نہیں کر سکتے ہیں-

انکرپشن ہزاروں سالوں سے موجود ہے- آج کی انکرپشن پہلے سے کہیں زیادہ پیچیدہ ہے لیکن اس کا مقصد وہی ہے یعنی خُفیہ پیغام کی ایک جگہ سے دوسری جگہ اِس طرح ترسیل کہ صرف اِس پیغام کو پڑھنے کے مجاز لوگ ہی اس تک رسائی حاصل کر سکتے ہیں- جب معلومات اِنکرپٹڈ نہیں ہوتی ہیں تو وہ «پلین ٹیکسٹ» کہلاتی ہیں- اِس کا مطلب ہے کہ کوئی بھی اُسے با آسانی پڑھ سکتا ہے یا اُس تک رسائی حاصل کر سکتا ہے- انکرپشن اُن معلومات کو نہ پڑھے جانے والے فارمیٹ میں تبدیل کر دیتی ہے جو کہ «سائفر ٹیکسٹ» کہلاتا ہے- آج کی انکرپشن پیچیدہ ریاضی آپریشنز اور مُنفرد چابی (کی) کے ذریعے آپ کی معلومات کو سائفر ٹیکسٹ میں تبدیل کردیتی ہے- یہ وہ چابی ہوتی ہے جس کے ذریعے آپ اپنی معلومات کو بند یا کھول سکتے ہیں- کئی صُورتوں میں یہ چابی آپ کا پاس ورڈ یا پاس کوڈ ہوتی ہے-

آپ کیا اِنکرپٹ کر سکتے ہیں؟

عموماً دو طرح کی معلومات اِنکرپٹ کی جاتی ہیں، ایک وہ معلومات جو ساکن ہوں (جیسے کہ آپ کے موبائل میں ذخیرہ کی ہوئی معلومات) اور دوسری وہ جو کہ مُتحرّک ہوں (جیسے کہ ای-میل وصول کرنا یا کسی دوست کو پیغام بھیجنا)-

اگر آپ کا کمپیوٹر یا آلہ چوری ہوجاتا ہے تو اس صُورت میں مُتحرّک معلومات کو اِنکرپٹ کرنا بہت ضروری ہوجاتا ہے- آج کل کے آلات بہت طاقتور ہیں اور اُن میں بہت زیادہ معلومات موجود ہوتی ہیں- لیکن اُن کے با آسانی کھو جانے کا خدشہ بھی ہوتا ہے- مزید یہ کہ کُچھ اقسام کے موبائل

انکرپشــن

میڈیا، حسّاس معلومات بھی رکھ سکتے ہیں جیسے کہ یو-ایس-بی فلیش ڈرائیوز یا بیرونی ہارڈ ڈرائیوز- فُل ڈسک اِنکرپشن (ایف-ڈی-ای) ایک بہت وسیع پیمانے پر استعمال ہونے والی انکرپشن ہے جو کہ آپ کے سسٹم کی مُکمل ڈرائیو کو اِنکرپٹ کر دیتی ہے- اس کا مطلب ہے کہ اس سسٹم پر موجود ہر چیز خودکار طور پر آپ کے لیۓ اِنکرپٹ ہوجائیگی اور آپ کو اِس بات کا فیصلہ نہیں کرنا پڑے گا کہ آپ کو کیا اِنکرپٹ کرنا ہے اور کیا نہیں- آج زیادہ تر کمپیوٹرز ایف-ڈی-ای کے ساتھ آتے ہیں۔ لیکن آپ کو اُسے خود فعّال کرنا پڑتا ہے- میک کمپیوٹرز میں یہ «فائل والٹ» کہلاتا ہے جبکہ ونڈوز کمپیوٹرز میں ورژن کے حساب سے آپ ‹بِٹ لاکر› یا ‹ڈیوائس انکرپشن› استعمال کر سکتے ہیں- زیادہ تر موبائل آلات ایف-ڈی-ای سپورٹ فراہم کرتے ہیں- آئی پیڈز اور آئی فونز میں ایک دفعہ پاس کوڈ لگنے کے بعد آئی-او-ایس خوُدکار طور پر ایف-ڈی-ای فعّال کر دیتا ہے- اینڈروائڈ 6.0 (مارش میلو) اور اُس کے بعد والے ورژنز میں گوُگل نے خوُدکار طور پر ایف-ڈی-ای کو پہلے سے ہی فعّال کرنے کو لازمی قرار دے دیا ہے، اگر وہ ہارڈویئر کے کم اَز کم معیارپر پورا اُترتا ہے تو-

انکرپشن اپنی معلومات کی حفاظت کا بہت ہی طاقتور طریقہ ہے لیکن یہ اُتنا ہی مضبوط ہے جتنی مضبوط آپ کی چابی-

معلوُمات ایک جگہ سے دوسری جگہ منتقل ہوتے وقت بھی غیر محفوظ ہوتی ہیں۔ اگر معلومات اِنکرپٹڈ نہیں ہیں تو انہیں کوئی بھی دیکھ سکتا ہے، اُن میں تبدیلی کرسکتا ہے اوراُنہیں آن-لائن چُرا بھی سکتا ہے- اس لیۓ آپ کو اس بات کو یقینی بنانا ہے کہ آپ کی حسّاس آن-لائن ٹرانزیکشنز اور مواصلات اِنکرپٹڈ ہیں- ایک عام آن لائن انکرپشن کی قسم HTTPS ہے- اس کا مطلب ہے کہ آپ کے براؤزر اور ویب سائٹ کے درمیان تمام مواصلات اِنکرپٹڈ ہے- اِس کی توثیق کرنے کے لیۓ آپ یو-آر-ایل میں https:// کو دیکھیں، اپنے براؤزر میں تالے کے آئیکن کو تلاش کریں یا پِھر اپنے یو-آر-ایل کے خانے کے سبز رنگ کے ہونے کا انتظار کریں- ایک اور مثال ای-میل بھیجنے اور وصول کرنے کی ہے- زیادہ تر ای-میل کلائنٹس میں اِنکرپشن کی صلاحیات موجود ہوتی ہیں جنہیں شاید آپکو فعّال کرنا پڑے- تیسری مثال دو لوگوں کے درمیان چیٹ کے دوران مُتحرّک معلومات کی ہے جیسے کہ iMessage, Wickr, Signal, WhatsApp یا Telegram- اِس طرح کی ایپلیکیشنز میں ‹اینڈ ٹوُ اینڈ› اِنکرپشن کا استعمال ہوتا ہے جو کسی بھی تیسری فریق کو ایک سسٹم یا آلہ سے معلومات کے کسی دوسرے سسٹم یا آلہ میں منتقلی کے دوران مُتحرّک معلومات تک رسائی کو روکتا ہے- اِس کا مطلب ہے کہ صرف آپ اور وہ دوسرا شخص جس سے آپ بات کر رہے ہیں، اُن بھیجے ہوئے پیغامات کو پڑھ سکتے ہیں-

صحیح طریقہ کار

اِس بات کو یقینی بنانے کے لیۓ کہ انکرپشن استعمال کرتے وقت آپ محفوظ ہیں، بہتر ہو گا کہ آپ اسے صحیح طرح سے استعمال کریں-

- آپ کی انکرپشن اُتنی ہی مضبوط ہے جتنی کہ اُس کی چابی- اگر کوئی آپ کی چابی کا اندازہ لگا لیتا ہے یا اُس تک رسائی حاصل کر لیتا ہے تو وہ آپ کی معلومات تک بھی رسائی حاصل کر ستا ہے- اِس لیۓ آپ اپنی چابی کی حفاظت کریں- اگر آپ چابی کے لیۓ پاس کوڈ یا پاس ورڈ استعمال کر رہے ہیں تو اِس بات کو یقینی بنائیں کہ وہ ایک مضبوط اور مُنفرد پاس ورڈ ہے- آپ کا پاس ورڈ جتنا لمبا ہو گا اُتنا ہی

انکرپشــن

کسی بھی حملہ آور کے لیۓ اُس کا اندازہ لگانا یا بروُٹ فورس کرنا مشکل ہو گا- آپ اپنا پاس ورڈ نہ بھوُلیں کیونکہ چابی کے بغیر آپ اپنی معلومات کو ڈیکرپٹ نہیں کر سکیں گے- اگر آپ اپنے تمام پاس ورڈز یاد نہیں رکھ سکتے ہیں تو ہمارا مشورہ ہے کہ آپ پاس ورڈ مینیجر استعمال کریں-

- آپ کی انکرپشن اُتنی ہی مضبوط ہے جتنی آپ کے آلات کی سکیورٹی- اگر آپ کا آلہ میلویئر سے متاثر ہو چکا ہے تو سائبر مُجرمان اُس کی انکرپشن کو توڑ سکتے ہیں- اِس لیۓ ضروری ہے کہ آپ اپنے آلہ کی حفاظت کے لیۓ مزید اقدامات بھی اٹھائیں جن میں اینٹی وائرس، مضبوط پاس ورڈ اور آلہ کو اپڈیٹ رکھنا شامل ہے-
- کئی موبائل اور کمپیوٹر ایپلیکیشنز آپ کو اپنی معلومات اورمواصلات کی حفاظت کے لیۓ مضبوط انکرپشن کی سہولت فراہم کرتی ہیں- آپ جس ایپلیکیشن کو استعمال کرنے جا رہے ہیں اگر اُس میں انکرپشن کی سہُولت موجود نہیں ہے تو آپ اُس کی متبادل ایپلیکیشن استعمال کرنے پر غور کریں (جس میں انکرپشن کی سہولت موجود ہو)-

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 securingthehuman.sans.org/ouch/archives (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:

انکرپشن کی وضاحت: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

پاس فریزز: https://securingthehuman.sans.org/ouch/2015#april2015

پاس ورڈ مینیجرز: https://securingthehuman.sans.org/ouch/2015#october2015

میلویئر کیا ہے: https://securingthehuman.sans.org/ouch/2016#march2016

اپنے نۓ ٹیبلٹ کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#january2016

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

ترجمہ: شعیب ہاشمی