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

OUCH!

اس شمارے میں شامل ہے:

- کیا بیک اپ کرنا ہے اور کب؟
- بیک اپ کیسے کرنا ہے؟
- ریکوڑی
- اہم نکات

بیک اپ اور ریکوڑی

جائزہ:۔

آپ کے ساتھ کبھی نہ کبھی کچھ غلط ہوگا اور آپ اپنی ذاتی فائلز، دستاویزات یا تصاویر کھو دیں گے۔ مثال کے طور پر غلط فائلز کو حادثاتی طور پر ڈیلیٹ کرنا، ہارڈویئر کا ناکارہ ہونا، اپنا لیپ ٹاپ کھو دینا یا آپ کے کمپیوٹر کا متاثر ہونا شامل ہے۔ ایسی صورت حال میں بیک اپ اکثر آپ کی ڈیجیٹل زندگی کی تعمیر نو کا واحد ذریعہ بن جاتا ہے۔ اس نیوزلیٹر میں ہم آپ کو بتائیں گے کہ بیک اپس کیا ہوتے ہیں؟ آپ کو اپنی معلومات کا بیک اپ کیسے کرنا ہے؟ اور ایسی حکمت عملی کیسے بنانی ہے جو آپ کے لیئے صحیح ثابت ہو۔

مہمان ایڈیٹر

ہیتھر مہالک صنعت کی تسلیم شدہ فارینزک کی ماہر ہیں اور زیادہ تر توجہ اسمارٹ فون فارینزک پر دیتی ہیں۔ وہ ‹پریکٹیکل موبائل فارینزک› کی شریک مصنفہ، ‹لرننگ اینڈرائڈ فارینزکس› کی ٹیکنیکل ایڈیٹر اور SANS انسٹیٹیوٹ میں FOR 585› ایڈوانسڈ اسمارٹ فون فارینزکس› اور ‹FOR518 میک انٹاش فارنزکس› کی شریک مصنفہ ہیں۔ آپ ہیتھر کو **smarterforensics.com** پر اور ٹوئیٹر پر **@heathermahalik** کے ذریعے فالو کر سکتے ہیں۔

کیا بیک اپ کرنا ہے اور کب؟

بیک اپس آپ کی ان معلومات کی نقول ہوتی ہیں جنہیں آپ کہیں اور محفوظ کرتے ہیں۔ جب آپ اہم معلومات کھو دیتے ہیں تو آپ ان معلومات کو بیک اپس کے ذریعے ریکوڑ کر سکتے ہیں۔ یہاں مسئلہ یہ ہے کہ زیادہ تر لوگ بیک اپس نہیں لیتے جو ایک شرمندگی کی بات ہے کیونکہ یہ بہت آسان اور سستے ہو سکتے ہیں۔ بیک اپ کس چیز کا لینا ہے، اس بات کا فیصلہ کرنے کے دو طریقے ہیں:1. وہ مخصوص معلومات جو آپ کے لیئے اہم ہیں یا 2. سب کچھ جس میں آپ کاپورا آپریٹنگ سسٹم شامل ہے۔ پہلا طریقہ کار آپ کے بیک اپس کو مؤثر بناتا ہے اور ہارڈ ڈرائیو کی جگہ بچاتا ہے، تاہم دوسرا طریقہ کار زیادہ آسان اور جامع ہے۔ بیک اپ کن معلومات کا لینا ہے؟ اگر آ پ اس بارے میں تذبذب کا شکار ہیں تو ہمارا مشورہ ہے کہ آ پ مکمل بیک اپ لے لیں۔

پھر آپ کو اس بات کا فیصلہ کرنا ہے کہ آپ کو اپنی معلومات کا بیک اپ کس کثرت سے لینا ہے۔ عام اختیارات میں گھنٹہ وار، روزانہ یا ہفتہ وار بیک اپ شامل ہے۔ گھر کے استعمال کے لیئے ذاتی بیک اپ کے پروگرامز موجود ہیں جیسے کہ ایپّل کا «ٹائم مشین» یا مائیکروسافٹ کا «ونڈوز بیک اپ اینڈ ری اسٹور» جو کہ آ پ کو خودکار طور پر «انسٹال کریں اور بھول جائیں» والے طریقے سے بیک اپ ترتیب دینے کی سہولت فراہم کرتے ہیں۔ جب آپ کام کر رہے ہوتے ہیں یا اپنے کمپیوٹر سے دور ہوتے ہیں تو یہ پروگرامز خاموشی سے دن بھر آ پ کی معلومات کا بیک اپ لیتے رہتے ہیں۔ دوسرے پروگرامز آپ کو ‹مسلسل حفاظت› کی پیشکش کرتے ہیں جو کہ کسی بھی نئی یا تبدیل شدہ فائلز کے بند ہوتے ساتھ ہی فوراً اس کا بیک اپ لے لیتے ہیں۔ ہم آ پ کو کم از کم روزانہ بیک اپ لینے کا مشورہ دیتے ہیں- بالآخر جو سوال آ پ کو اپنے آپ سے کرنا ہے وہ یہ ہے کہ «اگر مجھے تمام معلومات کو بیک اپ کے ذریعے ری اسٹور کرنا ہے تو میں کتنی معلومات سے ہاتھ دھونا برداشت کر سکتا ہوں؟»

بیک اپ کیسے کرنا ہے؟

اپنی معلومات کو بیک اپ کرنے کے دو طریقے ہیں: فزیکل میڈیا کے ذریعے یا کلاؤڈ پر منحصر اسٹوریج کے ذریعے۔ فزیکل میڈیا کسی بھی قسم کا ہارڈویئر ہو سکتا ہے جیسے کہ DVDs, USB ڈرائیوز یا ایکسٹرنل ہارڈ ڈرائیوز۔ آپ جس میڈیا کا بھی انتخاب کریں، اس بات کی یقین

بیک اپ اور ریکوری

خودکار، قابل اعتماد بیک اپس اکثر آ پ کی معلومات کی حفاظت کے لیئے دفاع کی آخری سطح ہوتے ہیں۔

دہانی کرلیں کہ آپ اپنی فائلز کا بیک اپ اسی ڈرائیو پر نہ لیں جس میں اصل فائلز موجود ہوں۔ فزیکل میڈیا کے ساتھ مسئلہ یہ ہے کہ اگر اس مقام پر کوئی آفت آتی ہے (جیسے کہ آ گ لگنا یا چوری ہونا) تو اس صورتحال میں آپ نہ صرف اپنے کمپیوٹر بلکہ بیک اپس کو بھی کھو دیتے ہیں۔ آپ کے پاس اپنے بیک اپ کو کسی دوسرے محفوظ مقام پر محفوظ کرنے کا منصوبہ ہونا چاہیئے۔ اگر آپ اسے کسی دوسری جگہ پر محفوظ کرتے ہیں تو اس کی نشاندہی کے لیئے اس پر ایک عنوان کے ذریعے لکھ دیں کہ آپ نے کیا بیک اپ کیا ہے اور کب کیا ہے۔ مزید حفاظت کے لیئے آ پ اپنے بیک اپس کو انکرپٹ کردیں۔

کلاؤڈ پر منحصر حل ذرا مختلف ہوتے ہیں، یہ ایک سروس ہوتی ہے جس کے ذریعے آپ کی فائلز انٹرنیٹ پر کہیں محفوظ ہوتی ہیں۔ یہ پیسوں والی سروس بھی ہو سکتی ہے لیکن اس کا انحصار اس بات پر ہے کہ آ پ کو کتنی معلومات کا بیک اپ لینا ہے۔ یہ کام اس طرح کرتی ہے کہ آپ کو اپنے کمپیوٹر میں ایک پروگرام انسٹال کرنا پڑتا ہے جو کہ خودکار طور پر آ پ کی فائلز کا بیک اپ لیتا رہتا ہے- اس حل کا فائدہ یہ ہے کہ چونکہ آپ کے بیک اپس کلاؤڈ پر ہوتے ہیں اس لیئے اگر آپ کے گھر پر کوئی آفت آتی ہے تو یہ بیک اپس پھر بھی محفوظ رہتے ہیں۔ اس کے علاوہ آپ اپنے بیک اپس یا انفرادی فائلز تک کہیں سے بھی رسائی حاصل کر سکتے ہیں حتّی کہ سفر میں بھی۔ کلاؤڈ پر منحصر بیک اپس (اور ریکوری) کا نقصان یہ ہے کہ یہ سست رفتار ہو سکتے ہیں خصوصاً اس وقت جب آپ کے پاس معلومات کا حجم بہت زیادہ ہو- اگر آپ کسی حل کے بارے میں تذبذب کا شکار ہیں کہ آپ کے لیئے بہترین حل کون سا ہے (فزیکل میڈیا یا کلاؤڈ)، تو آپ اس بات کو ذہن نشین کر لیں کہ آپ ان دونوں اختیارات کو ساتھ استعمال کر سکتے ہیں۔

آخر میں یہ کہ آپ اس ضمن میں اپنے موبائل آلا ت کو نہ بھولیں۔ موبائل آلات کا فائدہ یہ ہے کہ وہ پہلے سے ہی آپ کی معلومات کلاؤڈ پر محفوظ کر رہے ہوتے ہیں جسے کہ آپ کی ای-میل، کلینڈر ایونٹس یا کانٹیکٹس۔ تاہم آپ کے پاس ایسی معلومات ہوسکتی ہیں جو کہ کلاؤڈ پر محفوظ نہ ہوں جیسے کہ موبائل اپلیکیشنز کی کنفگریشنز، حالیہ تصاویر اور سسٹم پریفرینسز۔ اپنے موبائل آلہ کو بیک اپ کرنے سے نہ صرف آپ اپنی معلومات کو محفوظ کرتے ہیں بلکہ اس طرح سے کسی آلے کی تعمیر نوع بھی آسان ہو جاتی ہے- مثال کہ طور پر جب آپ نیا فون خریدتے ہیں تو اس پر پرانے فون کی معلومات منتقل کرنا آسان ہو جاتا ہے۔ آئی فون/آئی پیڈ خودکار طور پر ایپّل کے آئی کلاؤڈ پر بیک اپ کر سکتے ہیں۔ اینڈرائڈ یا دوسرے موبائل آلات میں بیک اپ کا انحصار سروس پرووائیڈر یا اس آلے کی بنانے والی کمپنی پر ہوتا ہے۔ بعض صورتوں میں ہوسکتا ہے کہ آپ کو ایسی موبائل اپلیکیشن خریدنی پڑ جائیں جو خاص طور پر بیک اپس کے لیئے بنائی گئی ہوں۔

ریکوری:۔

اپنی معلومات کا بیک اپ لینا صرف آدھا کام ہے، آپ اس بات کو بھی یقینی بنائیں کہ آپ ان معلومات کو ریکوَر کر سکتے ہیں۔ آپ ہر مہینے فائل ریکوَر کر کے اور اس کے مواد کی تصدیق کے ذریعے بیک اپ کو ریکوَر کر کے دیکھتے رہیں۔ اس کے علاوہ آپ اس بات کو بھی یقینی

بیک اپ اور ریکوری

بنائیں کہ کسی بھی اہم اپ گریڈ (جیسے کہ کسی نئے سسٹم یا موبائل آلہ پر منتقل ہوتے وقت) یا کسی اہم مرمت (جیسے کہ ہارڈویئر تبدیل کرنا) سے قبل آپ بیک اپ لے لیں اور اس بات کی بھی تصدیق کر لیں کہ وہ بیک اپ بحال ہو سکتا ہے۔

اہم نکات

- جتنا ممکن ہو اپنے بیک اپس کو خودکار بنائیں اور باقاعدگی سے اسے جانچتے رہیں۔
- جب آپ پورے سسٹم کی تعمیر نو کر رہے ہوں تو آپ اس بات کو یقینی بنائیں کہ اس سسٹم کے استعمال سے پہلے آپ اس پر تمام پیچز اور اپڈیٹس لاگو کر دیں۔
- پرانے اور متروکہ بیک اپس آ پ کے لیئے ایک بوجھ بن سکتے ہیں اس لیئے آپ کو انہیں تباہ کر دینا چاہیئے تا کہ غیر مجاذ لوگ اس تک رسائی حاصل نہ کر سکیں۔
- اگر آپ کلاؤڈ والا حل استعمال کر رہے ہیں تو اس سروس کو فراہم کرنے والی کمپنی کی پالیسیز اور ساکھ کے بارے میں تحقیق کر لیں کہ وہ آپ کی ضروریات کے عین مطابق ہیں- مثال کے طور پر کیا وہ آپ کی معلومات کو محفوظ کرنے سے پہلے انکرپٹ کرتے ہیں؟ آپ کے بیک اپس تک کسی اور کو رسائی حاصل ہے؟ کیا وہ مضبوط اوتھنٹیکیشن جیسے کہ ‹ٹو-اسٹیپ ویریفیکیشن› کی حمایت کرتے ہیں؟

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:

پاس فریزز:	http://www.securingthehuman.org/ouch/2015#april2015
ٹوُ اسٹیپ ویریفیکیشن:	http://www.securingthehuman.org/ouch/2013#august2013
کلاؤڈ سکیورٹی:	http://www.securingthehuman.org/ouch/2014#september2014
انکرپشن:	http://www.securingthehuman.org/ouch/2014#august2014
آج کی تجویز:	http://www.sans.org/tip_of_the_day.php

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