

OUCH!

Backup

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

کیا آپ کے پاس بیک اپ ہے؟

جائزہ

اگر آپ ایک کمپیوٹر یا موبائل آلہ کافی عرصے سے استعمال کر رہے ہیں تو کبھی نہ کبھی کچھ نہ کچھ خراب ہو جائے گا۔ ہو سکتا ہے کہ آپ غلطی سے غلط فائلز کو ڈیلیٹ کر دیں، کوئی ہارڈویئر خراب ہو جائے یا کوئی آلہ گم ہو جائے۔ سب سے بدترین صورت یہ ہو سکتی ہے کہ کوئی میلویئر جیسے کہ رینسم ویئر آپ کی فائلز کا صفایا کر دے اور/یا ان فائلز پر قبضہ کر لے۔ ایسے اوقات میں بیک اپس ہی اکثر آپ کی ڈیجیٹل زندگی کی از سر نو تعمیر کا واحد ذریعہ رہ جاتا ہے۔

کیا، کب اور کیسے؟

بیک اپس آپ کی ان معلومات کی نقول ہوتی ہیں جو آپ کے کمپیوٹر یا آلہ کے علاوہ کہیں اور ذخیرہ کی گئی ہوں۔ جب آپ قیمتی معلومات کھو دیتے ہیں تو آپ اسے بیک اپ کے ذریعے بحال کر سکتے ہیں۔ پہلا قدم یہ ہے کہ آپ اس بات کا فیصلہ کریں کہ آپ کو بیک اپ کیا کرنا ہے (۱) (مخصوص معلومات جو آپ کے لیئے اہم ہیں یا (۲) تمام معلومات جس میں آپ کا مکمل آپریٹنگ سسٹم بھی شامل ہے۔ کئی بیک اپ کے حل میں پہلا طریقہ ڈیفالٹ کنفیگر ہوا ہوتا ہے جس میں صرف زیادہ استعمال ہونے والے فولڈرز کا بیک اپ لیا جاتا ہے۔ اگر آپ کو اس بات کا علم نہیں ہے کہ کیا بیک اپ کرنا چاہیئے یا آپ زیادہ محتاط رہنا چاہتے ہیں تو آپ ہر چیز کا بیک اپ لے لیں۔

دوسرا آپ کو اس بات کا فیصلہ کرنا ہے کہ آپ نے بیک اپ کس کثرت سے لینا ہے۔ پلٹ-ان بیک اپ پروگرامز جیسے کہ ایپل کی ٹائم مشین یا ونڈوز بیک اپ اینڈ ری اسٹور آپ کو خودکار طور پر بیک اپ شیڈول کرنے کا اختیار فراہم کرتے ہیں (set it and forget it)۔ عام اختیارات میں ہر گھنٹے، روزانہ، ہفتہ وار بیک اپ جیسے اختیارات شامل ہیں۔ دوسرے بیک اپ کے حل « continuous protection » کی خدمات پیش کرتے ہیں جس میں نئی یا تبدیل شدہ فائلز کو آپ جیسے ہی محفوظ کرتے ہیں، فوراً اس کا بیک اپ بن جاتا ہے۔ ہمارا مشورہ ہے کہ آپ کم از کم اہم فائلز کا بیک اپ روزانہ لیں۔

آخر میں آپ اس بات کا فیصلہ کریں کہ آپ بیک اپ کس طرح لیں گے۔ دو طریقے ہیں: مقامی طور پر ذخیرہ کریں یا کلاؤڈ پر ذخیرہ کریں۔ مقامی بیک اپ کا انحصار ان آلات پر ہوتا ہے جن پر آپ کا اختیار ہوتا ہے جیسے کہ بیرونی یو ایس بی ڈرائیوز یا وائی فائی کا اختیار رکھنے والے نیٹ ورک آلات۔ مقامی طور پر بیک اپ لینے کا فائدہ یہ ہے کہ آپ بہت جلدی بڑی مقدار میں معلومات کا بیک اپ لے سکتے ہیں۔ نقصان یہ ہے کہ اگر آپ کسی میلویئر سے متاثر ہو جاتے ہیں جیسے کہ رینسم ویئر، تو اس صورت میں آپ کے بیک اپ کے متاثر ہونے کے امکانات بڑھ جاتے ہیں۔ اس کے علاوہ اگر کوئی حادثہ ہو جاتا ہے جیسے کہ آگ لگنا یا چوری ہونا، تو اس کے نتیجے میں آپ نہ صرف اپنے کمپیوٹر سے ہاتھ دھو بیٹھتے ہیں بلکہ اپنے بیک اپ سے بھی۔ اگر آپ بیک اپ کے لیئے بیرونی آلات استعمال کرتے ہیں تو اپنے بیک اپ کی ایک نقل دور کسی محفوظ جگہ پر رکھ دیں اور اس بات کی یقین دہانی کر لیں کہ اس پر ایک چٹ لگا دیں جس پر لکھا ہوا ہو کہ وہ کس چیز کا بیک اپ ہے۔

کلاؤڈ پر موجود بیک اپ مصنوعات وہ آن لائن سروسز ہوتی ہیں جو آپ کی فائلز کا ذخیرہ انٹرنیٹ پر رکھتی ہیں۔ عام طور پر آپ اپنے کمپیوٹر پر ایک ایپلیکیشن انسٹال کرتے ہیں، یہ ایپلیکیشن پھر خودکار طور پر فائلز کا بیک اپ لیتی ہیں یا ہر تھوڑے عرصے بعد یا پھر جیسے جیسے آپ کی فائل میں ترمیم ہوتی رہتی ہے۔ کلاؤڈ مصنوعات کا فائدہ یہ ہے کہ یہ بہت آسان ہوتی ہیں، ان میں بیک اپ خودکار طور پر ہو جاتا ہے اور آپ

اپنی فائلز تک کہیں سے بھی رسائی حاصل کر سکتے ہیں۔ آپ کی معلومات چونکہ کلاؤڈ پر موجود ہوتی ہیں اس لیے گھریلو حادثات جیسے کہ آگ لگنے یا چوری ہونے کی صورت میں آپ کے بیک اپ پر اثر نہیں پڑے گا۔ آخری بات یہ کہ کلاؤڈ پر موجود بیک اپ کے ذریعے آپ میلوینر، جیسے کہ رینسم ویئر، سے متاثر ہونے کے بعد معلومات با آسانی بحال ہو سکتی ہیں۔ کلاؤڈ پر نقصان یہ ہے کہ بیک اپ اور اس کی بحالی کا دار و مدار اس بات پر ہے کہ آپ کتنی معلومات کا بیک اپ لے رہے ہیں اور آپ کے نیٹ ورک کی رفتار کتنی ہے۔ کیا آپ کے لیے یہ فیصلہ کرنا مشکل ہو رہا ہے کہ آپ کو مقامی بیک اپ استعمال کرنا چاہیے یا کلاؤڈ بیک اپ استعمال کرنا چاہیے؟ آپ زیادہ محتاط رہتے ہوئے دونوں اختیارات ایک ساتھ استعمال کریں۔

موبائل آلات کی زیادہ تر معلومات پہلے سے ہی کلاؤڈ پر ذخیرہ ہوتی ہیں۔ تاہم آپ کی موبائل ایپلیکیشن کی کنفیگریشن، حالیہ تصاویر اور سسٹم پریفرنسز شاید ذخیرہ نہ ہوتی ہوں۔ اپنے موبائل آلہ کا بیک اپ لینے سے آپ نہ صرف ان معلومات کا بیک اپ لے لیتے ہیں بلکہ آپ کے لیے کسی نئے آلہ پر منتقل ہوتے وقت تمام معلومات کو اس میں منتقل کرنا بھی آسان ہو جاتا ہے۔

اہم نکات:

- معلومات کا بیک اپ آدھا کام ہے اس لیے آپ کو اس بات کا یقین ہونا چاہیے کہ آپ ان معلومات کو بحال کر سکتے ہیں۔ آپ ہر تھوڑے دنوں بعد اپنے بیک اپس کو بحال کر کے اور اس میں موجود فائلز کو کھول کر اس کا جائزہ لیتے رہیں کہ آیا وہ صحیح سے کام کر رہے ہیں کہ نہیں۔
- اگر آپ اپنے سسٹم کے بیک اپ کے ذریعے از سر نو تعمیر کرتے ہیں تو استعمال سے پہلے آپ اس بات کو یقینی بنائیں کہ آپ نے اس میں تازہ ترین پیچرز اور اپڈیٹس انسٹال کر دی ہیں۔
- اگر آپ کلاؤڈ بیک اپ کی طرف جاتے ہیں تو اس بات کو یقینی بنائیں کہ آپ کی منتخب کردہ مصنوعات استعمال کرنے میں آسان ہوں اور آپ نے اس کے سکیورٹی کے اختیارات کا جائزہ لے لیا ہے۔ مثال کے طور پر آپ کے آن لائن اکاؤنٹ کی حفاظت کے لیے کیا اس میں (ٹو-اسٹیپ ویریفیکیشن) کا اختیار موجود ہے؟

بیک اپس آپ کی ڈیجیٹل زندگی کی حفاظت کا آسان اور سستا طریقہ ہے۔

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 لیے <http://www.rewterz.com> کا دورہ کریں یا ہمارے فیس بک پیج <https://www.facebook.com/Rewterz> کو 'لائک' کریں یا ٹویٹر [@Rewterz](https://twitter.com/Rewterz) پر فالو کریں۔



مہمان مدیر

میٹ برومیلی ایک پیشہ ور سائبر سکیورٹی انسٹیٹنٹ ریسپانڈر ہیں اور انہوں نے چھوٹی بڑی مختلف تنظیموں کے ساتھ کام کیا ہوا ہے۔ وہ SANS میں انسٹرکٹر بھی ہیں جہاں وہ ایڈوانسڈ ہوسٹ اینڈ نیٹ ورک انسٹیٹنٹ رسپانڈر اور تھریٹ ہنٹنگ (FOR ۵۰۸ اور FOR ۵۷۲) کی کلاس کو پڑھاتے ہیں۔ آپ ان تک ٹویٹر پر [@mbromileyDFIR](https://twitter.com/mbromileyDFIR) کے ذریعے رسائی حاصل کر سکتے ہیں۔

وسائل:

<https://www.sans.org/u/TqR>

آسان پاس ورڈز بنانا:

<https://www.sans.org/u/TqW>

میلوینر کو روکیں:

<https://www.sans.org/u/Tr1>

اپنے گھر کے اٹرنیٹ کو محفوظ بنانا:

OUCH! کی اشاعت SANS Security Awareness Program کے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 4.0 License تحت تقسیم کرنے کی اجازت ہوتی ہے۔ آپ اس نیوز لیٹر کو تقسیم کر سکتے ہیں اگر آپ اس کا حوالہ دیں، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لیے استعمال کریں۔ ترجمے اور مزید معلومات کے لیے www.sans.org/security-awareness/ouch-newsletter پر رابطہ کریں۔ ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | ترجمہ: شعبہ ہاشمی