تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

# OUCH!

## اس شمارے میں شامل ہے:

- جائزہ
- کلاؤڈ پروائیڈر کا انتخاب کرنا
- اپنی معلومات کی حفاظت کرنا

# کلاؤڈ کا محفوظ طریقے سے استعمال

## جائزہ

«کلاؤڈ» کا مطلب مُختلف لوگوں کے لیئے مُختلف ہو سکتا ہے لیکن عمُوماً اِس کا مطلب انٹرنیٹ پر اپنے کمپیوٹنگ سِسٹمز یا/اور معلومات کو سروس پرووائیڈر کے ذریعے ذخیرہ کرنا ہے- کلاؤڈ کا ایک فائدہ یہ ہے کہ آپ دنیا میں کہیں سے بھی مختلف آلات کے ذریعے اپنی معلومات تک رسائی حاصل کر سکتے ہیں اور اسے سِنکرونائز کر سکتے ہیں- اِس کے علاوہ آپ اپنی معلومات کا اشتراک جس کے ساتھ چاہیں کر سکتے ہیں- ہم اِن سروسز کو «کلاؤڈ» کہتے ہیں کیونکہ آپ کو اکثر پتہ نہیں ہوتا ہے کہ آپ کی معلومات درحقیقت کہاں ذخیرہ ہوئی ہوئی ہیں- کلاؤڈ کمپیوٹنگ کی مثال میں گوُگل ڈاکس پر دستاویزات کو بنانا، ڈراپ باکس کے ذریعے فائلز کا اشتراک کرنا، ایمازون کلاؤڈ پر اپنا سرور قائم کرنا، سیلزفورس پر صارف کی معلومات ذخیرہ کرنا یا ایپّل کے ذریعے کلاؤڈ پر اپنی موسیقی یا تصویر آرکائیو کرنا شامل ہے- یہ آن لائن سروسز آپ کو کہیں زیادہ کارآمد بنا سکتی ہیں، لیکن اِن کے ساتھ مُنفرد خطرات بھی لاحق ہوتے ہیں- اِس نیوز لیٹر میں ہم آپ کو یہ باتیں گے کہ آپ محفوظ طریقے سے کلاؤڈ کا استعمال کیسے کر سکتے ہیں-

### مہمان ایڈیٹر

ڈیو شیکلفورڈ (**@daveshackleford**) ایک پیشہ ور کنسلٹنٹ ہیں جو کہ وُوڈو سکیورٹی کے مالک اور سینز کے مُتعدد تربیتی کورسز کے مُصنّف ہیں- اِن کورسز میں سینز سکیورٹی ۵۷۹: وِرچُوالائیزیشن اینڈ پرائیویٹ کلاؤڈ سکیورٹی اور سکیورٹی ۵۲۴: کلاؤڈ سکیورٹی فنڈامینٹلز شامل ہیں-

## کلاؤڈ پروائیڈر کا انتخاب کرنا

کلاؤڈ نہ ہی اچّھا ہے اور نہ ہی بُرا، یہ صرف ایک ٹوُل ہے جسے آپ گھر اور دفتر، دونوں جگہوں پر کام کرنے کے لیئے استعمال کر سکتے ہیں- تاہم جب آپ یہ سروسز استعمال کر رہے ہوتے ہیں تو آپ اپنی ذاتی معلومات دوسروں تک پہنچا رہے ہوتے ہیں اور اُمید کرتے ہیں کہ وہ اِن معلومات کو آپ کے لیئے کو ہر وقت دستیاب اور محفوظ رکھیں گے- آپ کو کلاؤڈ پرووائیڈر کا انتخاب کرتے وقت دانشمندی سے کام لینا چاہیئے- اپنے دفتر کے کمپیوٹرز یا کام سے متعلق کسی بھی معلومات کے لیئے اپنے سپروائزر سے رجوع کریں تاکہ آپ یہ جان سکیں کہ آپ کی تنظیم کلاؤڈ سروسز استعمال کرنے کی اجازت دیتی ہے یا نہیں- اگر کلاؤڈ استعمال کرنے کی اجازت ہے تو آپ اس بات کی تصدیق کرلیں کہ آپ کون سی کلاؤڈ سروسز استعمال کر سکتے ہیں اور اُن کے استعمال سے متعلق کیا پالیسیز ہیں- اگر آپ کلاؤڈ سروس کو ذاتی طور پر استعمال کرنا چاہ رہے ہیں تو مُندرجہ ذیل اقدامات استعمال کرنے پر غور کریں:

۱. **سپورٹ**: آپ کے لیئے کوئی مدد لینا یا کسی سوال کا جواب لینا کتنا آسان ہے؟ کیا کوئی ای-میل ایڈریس ہے جس پر آپ رابطہ کر سکتے ہیں، کوئی پبلک فورمز جن پر آپ اپنے سوالات بھیج سکتے ہیں یا اُن کی ویب سائٹ پر زیادہ پوچھے گئے سوالات کے جوابات موجود ہیں؟

۲. **سادگی**: سروس کو استعمال کرنا کتنا آسان ہے؟ سروس جتنی پیچیدہ ہوگی، آپ کے لیئے غلطیاں کرنے اور حادثاتی طور پر معلومات ظاہر کرنے یا معلومات کھونے کے امکانات اتنے ہی بڑھ جائیں گے- آپ ایسے کلاؤڈ پرووائیڈر کا انتخاب کریں جسے سمجھنا، کنفیگر کرنا اور استعمال کرنا آسان ہو-

# کلاؤڈ کا محفوظ طریقے سے استعمال

۳. **سکیورٹی**: اگر آپ سے کوئی معلومات لی جا رہی ہیں تو وہ کیا ہیں؟ آپ کی معلومات آپ کے کمپیوٹر سے کلاؤڈ پر کیسے جائیں گی اور کلاؤڈ پر ذخیرہ کیسے ہوں گی؟ کیا وہ اِنکرپٹڈ ہیں؟ اور اگر ہیں تو اُنھیں ڈیکرپٹ کون کر سکتا ہے؟

۴. **سروس استعمال کرنے کی شرائط**: آپ تھوڑا وقت نکال کر سروس استعمال کرنے کی شرائط کا جائزہ لے لیں (وہ اکثر حیران کُن طور پر آسان ہوتی ہیں)- آپ اس بات کی تصدیق کر لیں کہ آپ کی معلومات تک کس کس کو رسائی حاصل ہے اور آپ کے قانونی حقوق کیا ہیں؟ اس کے ساتھ ساتھ اس بات کا بھی جائزہ لیں کہ سکیورٹی کی کون سی ذمّہ داری پرووائیڈر پر ہے اور کون سی آپ پر-

کلاؤڈ آپ کی معلومات تک رسائی کو بہتر بناتا ہے اور آپ کی کارکردگی مزید بڑھاتا ہے لیکن آپ اپنی معلومات تک رسائی اور اُس کے اشتراک کے بارے میں مُحتاط رہیں-

## اپنی معلومات کی حفاظت کرنا

ایک بار جب آپ کلاؤڈ پرووائیڈر کا انتخاب کر لیں تو اگلا قدم اس بات کی یقین دہانی کرنا ہے کہ آپ کلاؤڈ سروسز کا استعمال احسن طریقے سے کر رہے ہیں- آپ اپنی معلومات تک کس طرح رسائی حاصل کرتے ہیں اور اُس کا اشتراک کس طرح کرتے ہیں، اس بات کا جتنا گہرا اثر آپ کی فائلز کی سکیورٹی پر پڑ سکتا ہے اُتنا کسی اور چیز کا نہیں پڑسکتا- کچھ اہم اقدامات جنھیں آپ شامل کر سکتے ہیں وہ یہ ہیں:

۱. **اوتھنٹیکیشن**: آپ اپنے کلاؤڈ کے اکاؤنٹ پر بہت مضبوط اور منفرد پاس فریز کا استعمال کریں- اگر آپ کا کلاؤڈ پرووائیڈر ٹُو-اسٹیپ ویریفیکیشن کی سہولت فراہم کرتا ہے تو ہمارا پُرزور مشورہ ہے کہ آپ اُسے فعّال کر دیں- یہ اپنے اکاؤنٹ کی حفاظت کے لیئے سب سے اہم ترین اقدامات میں سے ایک ہے-

۲. **فائلز/فولڈرز کا اشتراک**: کلاؤڈ نے اشتراک کو کافی آسان بنا دیا ہے، کچھ صورتوں میں تو بہت ہی زیادہ آسان بنا دیا ہے- سب سے بدتر صورتِحال یہ ہو سکتی ہے کہ آپ یہ سمجھ رہے ہوں کہ آپ کسی مخصوص شخص سے فائلز کا اشتراک کر رہے ہیں لیکن حادثاتی طور پر اُن فائلز یا پورے فولڈر کو، عام عوام کے لیئے پورے انٹرنیٹ پر دستیاب کر دیتے ہیں- اپنی حفاظت کا سب سے بہترین طریقہ یہ ہے کہ آپ اپنی کسی بھی فائل کا بطور ڈیفالٹ کسی کے ساتھ اشتراک نہیں کریں- پھر آپ صرف اُن خاص لوگوں (یا لوگوں کے گروہ) کو مخصوص فائلز یا فولڈرز تک رسائی دیں جنھیں اُس کی ضرورت ہے- جب کسی شخص کو آپ کی فائلز تک رسائی کی مزید ضرورت نہیں رہتی، تو آپ اُن فائلز کو وہاں سے ہٹا دیں- آپ کے کلاؤڈ پرووائیڈر کو ایک ایسا آسان طریقہ فراہم کرنا چاہیئےجس کے ذریعے آپ کو باآسانی پتہ چل جائے کہ آپ کی فائلز اور فولڈرز تک کس کس کو رسائی حاصل ہے-

۳. **لِنکس کے ذریعے فائلز/فولڈرز کا اشتراک**: کلاؤڈ سروسز میں ایک عام خصوصیت ویب لِنک تخلیق کرنے کی صلاحیت ہے جو کہ آپ کی فائلز یا فولڈرز کی طرف اشارہ کرتا ہے- یہ خصوصیت آپ کو ان فائلز کو صرف ویب لِنک کے ذریعے کسی کے ساتھ بھی اشتراک کرنے کی سہولت فراہم کرتی ہے- تاہم اس طریقے میں بہت کم سکیورٹی ہوتی ہے کیونکہ جس کسی کو بھی اس لِنک کا پتہ ہوگا، اُس تک آپ کی ذاتی فائلز یا فولڈرز کی رسائی آجائے گی- اگر آپ کسی ایک شخص کو لِنک بھیجتے ہیں تو وہ شخص اُسے مزید لوگوں کو بھیج سکتا ہے یا وہ لِنک، سرچ انجنز میں بھی نظر

# کلاؤڈ کا محفوظ طریقے سے استعمال

آ سکتا ہے- اگر آپ معلومات کا اشتراک لِنک کے ذریعے کرتے ہیں تو اس بات کو یقینی بنائیں کہ جب آپ کو اُس لِنک کی مزید ضرورت نہیں رہتی ہے تو آپ اکسپائری تاریخ کے ذریعے اُسے غیر فعّال کر دیں یا اگر مُمکن ہو تو اُس لِنک کی پاس ورڈ کے ذریعے حفاظت کریں-

۴. **سیٹینگز**: آپ اپنے کلاؤڈ پرووائیڈر کی جانب سے فراہم کی گئی سکیورٹی سیٹینگز کوسمجھیں- مثال کے طور پر، اگر آپ کسی کے ساتھ فولڈر کا اشتراک کرتے ہیں تو کیا وہ آپ کی معلومات کو آپ کے علم میں لائے بغیر کسی اور کے ساتھ اشتراک کر سکتا ہے؟ آپ اِن طریقوں پر بھی غور کریں جِن کے ذریعے آپ کو پتہ چل جائے کہ آپ کے اشتراک کئے ہوئے مواد کو کِس کِس نے دیکھا ہے- کیا آپ اِشتراک کو ‹read+write› جس کے ذریعے لوگ فائلز میں تبدیلی بھی کر سکتے ہیں، کے بجائے ‹read only› سے محدود کر سکتے ہیں؟

۵. **اینٹی وائرس**: آپ اس بات کو یقینی بنائیں کہ آپ کے کمپیوٹر اور کسی بھی ایسے کمپیوٹر جس میں آپ کی معلومات کا اشتراک ہوا ہو، اُس میں اینٹی وائرس سافٹ ویئر کا جدید ترین ورژن انسٹال ہو- اگر کوئی فائل جس کا آپ اشتراک کر رہے ہیں، متأثر ہو جاتی ہے تو دوسرے تمام کمپیوٹرز جو اس فائل تک رسائی حاصل کر رہے ہیں، وہ بھی متأثر ہو سکتے 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 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:

| | |
|---|---|
| ٹُو-اسٹیپ ویریفیکیشن: | https://securingthehuman.sans.org/ouch/2015#september2015 |
| 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 |
| سکیورٹی ٥٢٤: کلاؤڈ سکیورٹی فنڈامینٹلز: | https://sans.org/sec524 |



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

**ترجمہ:** شعیب ہاشمی