SANS SECURITY AWARENESS

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

ورچوئل پرائیویٹ نیٹ ورکس (VPN)

جائزہ

ہو سکتا ہے کہ آپ جب گھر سے دور ہوں تو آپ کو عوامی وائی فائی استعمال کرنے کی ضرورت پڑے جیسے کہ جب آپ کسی مقامی ریستوران میں جاتے ہیں، کسی کافی کی دکان پر جاتے ہیں یا سفر کے دوران جب آپ کسی ہوٹل یا ہوائی اڈّے پر جاتے ہیں- لیکن یہ عوامی نیٹ ورکس کتنے محفوظ ہیں اور ان کے ذریعے کون آپ کی آن لائن سرگرمی پر نظر رکھ رہا ہے یا اسے ریکارڈ کر رہا ہے؟ اس طرح شاید آپ اپنے گھر میں استعمال ہونے والے انٹرنیٹ کی ISP (انٹرنیٹ سروس پرووائیڈر) پر بھی بھروسہ نہیں کریں اور اس بات کی یقین دہانی کر لیں کہ وہ آپ کی آن لائن سرگرمی کی نگرانی نہیں کر سکتی ہے- آپ اپنی آن لائن سرگرمیوں اور پرائیویسی کا تحفّظ VPN (ورچوئل پرائیویٹ نیٹ ورکس) کے ذریعے کریں- VPN ایک ایسی ٹیکنالوجی ہے جو آپ کی آن لائن سرگرمی کے لیئے پرائیویٹ اور انکرپٹڈ ٹنل بنا دیتی ہے جس کی بدولت کسی کے لیئے بھی آپ کی آن لائن سرگرمی کی نگرانی کرنا یا دیکھنا کافی مشکل ہو جاتا ہے- اس کے علاوہ VPN آپ کے محل وقوع کو بھی چھپا دیتا ہے جس کی وجہ سے ان ویب سائٹس کے لیئے آپ کی جگہ کا تعیّن کرنا مشکل ہو جاتا ہے جن کا آپ دورہ کرتے ہیں-

یہ ٹیکنالوجی کام کس طرح کرتی ہے؟

VPN کام اس طرح سے کرتا ہے کہ آپ کے کمپیوٹر اور آپ کے منتخب کردہ VPN پرووائیڈر کے درمیان ایک پرائیویٹ، انکرپٹڈ ٹَنل بنتا ہے- آپ کی تمام آن لائن سرگرمیوں کی آمد و رفت پہلے اس ٹَنل کے ذریعے اور پھر آپ کے VPN پرووائیڈر کے نیٹ ورک سے ہوتے ہوئے آپ کی منزل مقصود تک پہنچتی ہے- مثال کے طور پر اگر آپ ٹیمپا، فلاریڈا میں مقیم ہیں اور آپ میونخ، جرمنی کے کسی VPN سرور سے منسلک ہوتے ہیں تو آپ جس ویب سائٹ کا بھی دورہ کریں گے وہ یہ سمجھے گی کہ آپ میونخ، جرمنی سے اس کا دورہ کر رہے ہیں- VPN کا استعمال آسان ہے- سب سے پہلا قدم یہ ہے کہ آپ کسی قابل بھروسہ VPN پرووائیڈر کو ڈھونڈیں اور پھر وہاں اکاؤنٹ بنائیں (اکثر ایسی خدمات آپ کو خریدنی پڑتی ہیں)- ایک بار آپ کا اکاؤنٹ بن جائے تو پھر آپ VPN سافٹ ویئر کو ڈاؤن لوڈ، انسٹال اور کنفیگر کر لیں- اس کے بعد آپ انٹرنیٹ سے ویسے ہی منسلک ہو جائیں جیسے آپ ہمیشہ ہوتے ہیں- VPN سافٹ ویئر خاموشی سے آپ کے لیئے انکرپٹڈ ٹَنل بنا دے گا اور آپ کی پرائیویسی کی حفاظت کرنا شروع کر دے گا اور آپ کو اس کا احساس بھی نہیں ہو گا-

VPN پرووائیڈر کا انتخاب کرنا

آپ کی آن لائن سرگرمیاں اتنی ہی محفوظ اور ذاتی ہیں جتنا کہ آپ کا VPN پرووائیڈر- اس لیئے آپ ایسے VPN پرووائیڈر کا انتخاب کریں جس پر آپ بھروسہ کرتے ہوں- آپ VPN سروس پرووائیڈر کا انتخاب کرتے ہوئے مندرجہ ذیل باتوں کا خیال رکھیں:

لاگنگ : آپ کسی ایسی سروس کا انتخاب کریں جو کسی بھی قسم کی لاگز کو اپنے پاس نہیں رکھتی ہوں اور ان کی تمام توجہ کا مرکز صرف پرائیویسی ہو- اگر آپ کا VPN سروس پرووائیڈر کوئی لاگز اپنے پاس نہیں رکھ رہا ہے تو اس صورت میں کسی کے لیئے بھی بہت مشکل ہو گا کہ وہ آپ کی پچھلی سرگرمیوں کے بارے میں جان سکیں-

کمپنی کہاں واقع ہے ؟ مختلف VPN پرووائیڈرز مختلف ممالک میں مقیم ہوتے ہیں- آپ اس بات کی یقین دہانی کر لیں کہ آپ صرف اُس VPN پرووائیڈر کا انتخاب کریں جو ایک ایسے ملک میں واقع ہو جہاں پرائیویسی کے قوانین کافی سخت ہوں- کیونکہ اگر آپ کسی ایسے VPN پرووائیڈر کا انتخاب کرتے ہیں جو کسی ایسے ملک میں واقع ہے جہاں پرائیویسی کے قوانین کمزور ہوں تو اس بات کا امکان ہے کہ وہ آپ سے حاصل کردہ معلومات کسی اور کو دے دیں-

سرورز: آپ ایسی VPN سروس کا انتخاب کریں جن کے سرورز اُن مُمالک یا شہروں میں ہوں جہاں آپ کو ضرورت ہے- کچھ VPN پرووائیڈرز کے پاس دنیا بھر میں مُختلف مقامات پر ہزاروں سرورز موجود ہوتے ہیں- کیا آپ کو یہ دکھانے کی ضرورت ہے کہ آپ کا انٹرنیٹ کنیکشن کسی خاص مُلک سے آ رہا ہے اور کیا آپ کا VPN پرووائیڈر یہ سروس فراہم کر سکتا ہے؟

مطابقت: آپ ایسی سروس کا انتخاب کریں جسے آپ مختلف کمپیوٹرز اور موبائل آلات پر استعمال کر سکیں- مثال کے طور پر اگر آپ ونڈوز کا لیپ ٹاپ، کوئی ٹیبلٹ یا آئی فون استعمال کر رہے ہیں تو آپ چاہیں گے کہ VPN سروس ان تمام آلات پر کام کرے-

مُفت سروس سے اجتناب کریں: آپ کسی بھی «مفت» VPN سروس سے ہوشیار رہیں کیونکہ اگر وہ یہ سروس مُفت فراہم کر رہی ہیں تو وہ پیسے کیسے بنا رہی ہیں اور اُن کا کاروبار کیسے چل رہا ہے؟ مُفت سروسز فراہم کرنے والی تنظیمیں آپ کی معلومات حاصل کر کے اسے بیچ سکتی ہیں-

VPN آپ کی آن لائن پرائیویسی کی حفاظت کا بہت زبردست طریقہ ہے- تاہم یہ آپ کے کمپیوٹر، آلات یا آن لائن اکاؤنٹس کی حفاظت کے لیئے کچھ نہیں کرتا ہے- اس لیئے اگر آپ VPN استعمال کر بھی رہے ہیں تو اس بات کو یقینی بنائیں کہ آپ نے بنیادی سکیورٹی کے اقدامات اٹھا لیئے ہیں جن میں اس بات کو یقینی بنانا کہ آپ کے آلات اپڈیٹ ہیں، آپ کا اسکرین لاک کافی مضبوط ہے اور آپ ہر اکاؤنٹ کے لیئے منفرد پاس ورڈ استعمال کر رہے ہیں، شامل 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 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-

مہمان مُدیر

فِل جانسی (@peakreflections) پام بیچ کاؤنٹی میں آئی ٹی کے پیشہ ور ہیں اور اپنے پاس سکیورٹی، فارنزیکس اور آڈٹ کا تجربہ رکھتے ہیں- وہ SANS سے ڈیجیٹل فارنزیک اور سکیورٹی ایسینشلز میں سند یافتہ ہیں اور OUCH کے کمیونٹی ریویئو بورڈ کے رکن بھی ہیں- ان میں سکیورٹی کو دوسروں کے لیئے آسان بنانے کا شدید جذبہ ہے-

وسائل:

آسان پاس ورڈز بنانا: https://www.sans.org/u/Sd8
اپنے موبائل آلات کو محفوظ بنانا: https://www.sans.org/u/Sdd
میلویئر کو روکیں: https://www.sans.org/u/Sdi