SANS SECURITY AWARENESS

OUCH!

آپ کے لیئے سکیورٹی سے آگاہی کا ماہانہ نیوز لیٹر

آسان پاس ورڈز بنانا

جائزہ

آپ کو اکثر بتایا جاتا ہے کہ آپ کے پاس ورڈ آپ کے اکاؤنٹس کو محفوظ بنانے کا اہم ترین ذریعہ ہیں (جو کہ درست بات ہے)، لیکن شاید ہی آپ کو کبھی بھی یہ بتایا گیا ہو کہ آسان طریقے سے مضبوط پاس ورڈ کیسے بنایا جائے اور اسے کس طرح سے محفوظ رکھا جائے- ہم نے آپ کو اپنے پاس ورڈ کو آسان بنانے کے لیئے، اپنے اکاؤنٹس کو محفوظ رکھنے کے لیئے اور اپنے مستقبل کو محفوظ بنانے کے لیئے مندرجہ ذیل تین آسان اقدامات بیان کیئے ہیں-

پاس فریزز

مشکل اور پیچیدہ پاس ورڈز رکھنے کے دن اب گُزر چُکے ہیں- ایسے پاس ورڈز کو یاد رکھنا اور لکھنا کافی مشکل ہوتا ہے اور آج کل کے برق رفتار کمپیوٹرز کے ہوتے ہوئے سائبر حملہ آوروں کے لیئے ان کا پتہ لگانا مشکل نہیں ہے- مضبوط پاس ورڈ رکھنے کا طریقہ یہ ہے کہ آپ لمبے پاس ورڈز رکھیں یعنی اس میں جتنے زیادہ الفاظ ہوں گے اُتنا بہتر ہے- یہ پاس فریزز کہلاتے ہیں، یہ ایسے مضبوط پاس ورڈز ہوتے ہیں جن میں چھوٹے جُملے یا بے ترتیب الفاظ استعمال ہوتے ہیں- مندرجہ ذیل دو مثالیں ملاحظہ فرمائیں:

Time for strong coffee!
lost-snail-crawl-beach

ان دونوں مثالوں میں بیس سے زیادہ حروف ہیں جو کہ یاد رکھنے اور لکھنے میں آسان مگر ان کا اندازہ لگانا بہت مشکل ہے- آپ ایسی ویب سائٹس پر بھی جائیں گے جہاں پاس ورڈ میں سمبلز، نمبرز یا بڑے حروف کو شامل کرنا لازمی ہو گا- یاد رہے کہ یہاں پاس ورڈ کا لمبا ہونا بہت اہم ہے-

پاس ورڈ مینیجرز

آپ کو ہر اکاؤنٹ کے لیئے ایک منفرد پاس ورڈ چاہیئے ہو گا- اگر آپ ایک ہی پاس ورڈ کو ایک سے زیادہ اکاؤنٹس کے لیئے استعمال کرتے ہیں تو اس طرح آپ اپنے آپ کو بہت بڑے خطرے میں ڈال رہے ہیں- اس طرح سائبر حملہ آور کو آپ کے استعمال میں موجود صرف ایک ویب سائٹ ہیک کرنی ہو گی، اس میں سے آپ سمیت تمام لوگوں پاس ورڈز چُرانے ہوں گے اور پھر وہ آپ کے اس ایک پاس ورڈ کے ذریعے آپ کے باقی تمام اکاؤنٹس میں آپ بن کر لاگ اِن ہو جائے گا- ایسا اکثر ہوتا رہتا ہے، شاید آپ کی سوچ سے بھی زیادہ- آپ کو یقین نہیں آیا؟ آپ اس ویب سائٹ کا دورہ کریں www.haveibeenpwned.com اور دیکھیں کہ آپ کے استعمال میں موجود کون کون سی ویب سائٹس ہیک ہو چکی ہیں اور ان کے پاس ورڈز، بشمول آپ کے، چوری ہو چکے ہیں- اس صورت میں آپ کو کیا کرنا چاہیئے؟ آپ کو پاس ورڈ مینیجر استعمال کرنا چاہیئے-

یہ ایسے خاص کمپیوٹر پروگرامز ہوتے ہیں جو آپ کے تمام پاس ورڈز کو محفوظ طریقے سے انکرپٹڈ والٹ میں ذخیرہ کرتے ہیں- آپ کو صرف ایک پاس ورڈ یاد رکھنا ہو گا جو کہ آپ کے پاس ورڈ مینیجر کا ہو گا- آپ کو جب بھی ضرورت ہو، پاس ورڈ مینیجر خودکار طور پر آپ کے تمام پاس ورڈز کو نکال لے گا اور آپ کو ویب سائٹس میں لاگ اِن کر دے گا- ان میں اور بھی خصوصیات ہوتی ہیں جیسے کہ آپ کے خفیہ سوالوں کے

جواب ذخیرہ کرنا، ایک ہی پاس ورڈ کو دوبارہ استعمال کرتے وقت آپ کو متنبّہ کرنا، ایک پاس ورڈ جنریٹر جس کا کام اس بات کو یقینی بنانا ہو کہ آپ مضبوط پاس ورڈ استعمال کر رہے ہیں اور کئی مزید خصوصیات شامل ہیں- زیادہ تر پاس ورڈ مینیجرز محفوظ طریقے سے تقریباً کسی بھی کمپیوٹر یا آلہ کے ساتھ سنکرونائز ہو سکتے ہیں اس لیئے اس بات سے قطع نظر کہ آپ کون سا سِسٹم استعمال کر رہے ہیں، پاس ورڈ مینیجر آپ کے تمام پاس ورڈز کو محفوظ بناتا ہے-

آخری بات یہ کہ آپ اپنے پاس ورڈ مینیجر کے پاس ورڈ کو کہیں لکھ کر گھر کے کسی محفوظ مقام پر ذخیرہ کر لیں- کچھ پاس ورڈ مینیجرز آپ کو پاس ورڈ مینیجر ریکوَری کِٹ کو پرنٹ کرنے کی بھی سہولت فراہم کرتے ہیں- اس طرح اگر آپ اپنے پاس ورڈ مینیجر کا پاس ورڈ بھول بھی جاتے ہیں تو آپ کے پاس اس کا بیک اپ موجود ہوتا ہے- یا اگر آپ بیمار ہو جاتے ہیں یا کسی ہنگامی حالت میں آ جاتے ہیں تو آپ کی شریک حیات یا خاندان کے قابل بھروسہ لوگ آپ کے لیئے ان معلومات کو بازیاب کر سکتے ہیں-

ٹواسٹیپ ویریفیکیشن

ٹُواسٹیپ ویریفیکیشن (جو کہ اکثر ٹو فیکٹر اوتھنٹیکیشن یا ملٹی فیکٹر اوتھنٹیکیشن بھی کہلاتی ہے) سکیورٹی کی مزید ایک تہہ بچھا دیتی ہے- آپ کو اپنے اکاؤنٹ میں لاگ اِن کرنے کے لیئے دو چیزوں کی ضرورت ہوتی ہے، ایک آپ کا پاس ورڈ اور دوسرا ایک عددی کوڈ جو کہ آپ کے اسمارٹ فون کے ذریعے نکلتا ہے یا آپ کے فون پر بھیجا جاتا ہے- یہ تمام تر عمل اس بات کو یقینی بناتا ہے کہ اگر کسی سائبر حملہ آور کے ہاتھ آپ کا پاس ورڈ لگ بھی جائے تو وہ پھر بھی آپ کے اکاؤنٹ میں داخل نہیں ہو سکے- ٹُواسٹیپ ویریفیکیشن کو لگانا بہت آسان ہوتا ہے اور آپ کو اسے نئے کمپیوٹر یا آلہ میں لاگ اِن کرتے وقت صرف ایک بار استعمال کرنا ہوتا ہے- جب بھی ممکن ہو آپ اسے فعال کر دیں، خصوصاً اپنے سب سے اہم اکاؤنٹس کے لیئے جیسے کہ آپ کے بینک کا اکاؤنٹ یا ریٹائرمنٹ سے متعلق اکاؤنٹس یا آپ کا ای میل اکاؤنٹ- اگر آپ پاس ورڈ مینیجر کا استعمال کر رہے ہیں تو ہمارا مشورہ ہے کہ آپ اسے ایک مضبوط پاس فریز اور ٹُواسٹیپ ویریفیکیشن کے ذریعے محفوظ بنائیں-

آپ کو شاید سُننے میں عجیب لگے لیکن یہ تین آسان اقدامات اپنا کر آپ اپنی ملازمت، ساکھ اور مالی مستقبل کو کافی حد تک محفوظ بنا سکتے ہیں-

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

جسٹن ہینڈرسن (@SecurityMapper) H & A سکیورٹی سولُوشنز کے شریک بانی ہیں، وہ SANS انسٹیٹیوٹ میں تصدیق شدہ انسٹرکٹر اور SANS سائبر ڈیفینس اور SIEM سے متعلق کورسز کے مصنف بھی ہیں- وہ سائبر ڈیفینس میں کافی دلچسپی رکھتے ہیں اور اپنے پاس مشاورت فراہم کرنے کا پندرہ سالہ تجربہ بھی رکھتے ہیں-

وسائل:

Have I Been Pwned: https://haveibeenpwned.com/

ٹو فیکٹر اوتھنٹیکیشن سائٹ: https://twofactorauth.org/

NIST SP800-63B ڈیجیٹل آئڈینٹی گائیڈلائنز: https://pages.nist.gov/800-63-3/sp800-63b.html

پوسٹر: آپ ہدف ہیں: https://www.sans.org/u/OGi