SANS SECURING THE HUMAN

OUCH! اپریل ۲۰۱۷

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

پاس فریزز

پس منظر

پاس ورڈ ایسی چیز ہے جسے آپ تقریباً روز استعمال کرتے ہیں اپنی ای-میل تک رسائی یا آن-لائن اشیاء کی خریداری سے لے کر اپنے اسمارٹ فون تک رسائی کے لیئے- تاہم پاس ورڈز آپ کا کمزور ترین نکتہ ہیں؛ اگر کسی کو آپ کا پاس ورڈ پتہ چل جائے یا وہ اُس کا اندازہ لگا لے تو وہ آپ کے طور پر آپ کے اکاؤنٹس تک رسائی حاصل کر سکتا ہے، جس کے ذریعے وہ رقم مُنتقل کر سکتا ہے، آپ کی ای-میلز پڑھ سکتا ہے یا آپ کی شناخت چرا سکتا ہے- اس لیئے مضبوُط پاس ورڈز آپ کی حفاظت کے لیئے بہت ضروری ہے- تاہم پاس ورڈز عام طور پر اُلجھن پیدا کر دیتے ہیں، یاد رکھنے اور لکھنے میں مُشکل ہوتے ہیں- اس نیوزلیٹر میں آپ یہ سیکھیں گے کہ ایسے مضبوُط پاس ورڈز کیسے بنائے جاتے ہیں جنہیں یاد رکھنا اور لکھنا آسان ہو، یہ پاس فریزز کہلاتے ہیں-

مہمان ایڈیٹر

مینوپ وائن SANS کی سند یافتہ انسٹرکٹر اور ‹سکیورڈ آئی ٹی سولیوشنز› کی ‹سی ای او› / ‹پرنسپل کنسلٹنٹ› ہیں- وہ اعلی ترین سرٹیفیکیشنز اور سائبر سکیورٹی پروگرامز کو مختلف صنعتوں اور شعبوں کے لیئے بنانے اور منظّم کرنے کے ۱۴ سالہ تجربے کی بنیاد پر کافی مہارت رکھتی ہیں- Twitter: **@MenopN** LinkedIn: My-Ngoc «Menop» Nguyen

پاس فریزز

جو مسئلہ ہم سب کو درپیش ہے وہ یہ ہے کہ سائبر حملہ آوروں نے پاس ورڈز کو بروُٹ فورس (خوُدکار طور پر اندازہ لگانا) کرنے کے لیئے بہت نفیس اور مؤثر طریقے نکال لیئے ہیں- اس کا مطلب ہے کہ اگر آپ کا پاس ورڈ کمزور ہے یا اُس کا اندازہ لگانا آسان ہے تو بُرے لوگ با آسانی آپ کے پاس ورڈز تک رسائی حاصل کر سکتے ہیں- اپنے آپ کو محفوُظ رکھنے کے لیئے ایک اہم قدم مضبوُط پاس ورڈز کا استعمال ہے- یہ عام طور پر پیچیدہ پاس ورڈز تخلیق کر کے کیا جاتا ہے، تاہم اُنہیں یاد رکھنا مُشکل، مُبہم اور اُسے لکھنا مُشکل ہو سکتا ہے- اس کے بجائے ہمارا مشورہ ہے کہ آپ پاس فریزز کا استعمال کریں جو کہ کئی بے ترتیب الفاظ کا مجموعہ ہوتا ہے- آپ کے پاس فریز میں جتنے حرُوف ہوں گے وہ اُتنا ہی مضبوُط ہو گا- اس کا فائدہ یہ ہے کہ اُسے یاد رکھنا اور لکھنا کافی آسان ہوتا ہے لیکن سائبر مُجرمان کے لیئے اُسے ہیک کرنا پھر بھی مشکل ہوتا ہے- مُندرجہ ذیل دو مختلف مثالیں ملاحظہ فرمائیں-

Sustain-Easily-Imprison

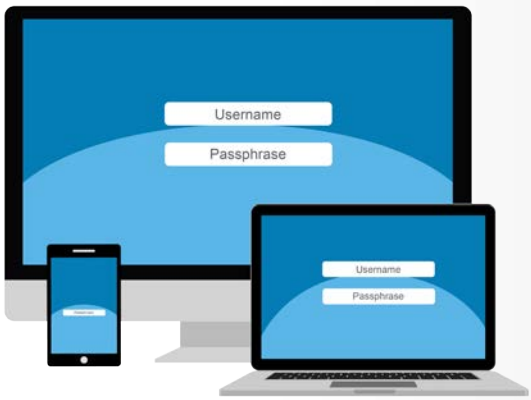
Time for tea at 1:23

جو چیز ان پاس فریزز کو اتنا مضبوُط بناتی ہے وہ ان کا صرف لمبا ہونا ہی نہیں بلکہ ان کا بڑے حرُوف (کیپیٹل لیٹرز) کا استعمال کرنا ہے (یاد رہے کہ خالی جگہ اور رموز اوقاف، سمبلز ہیں)- اس کے علاوہ ان پاس فریزز کو یاد رکھنا اور ٹائپ کرنا بھی آسان ہے- آپ اپنے پاس فریزیز کو مزید مضبوُط اس طرح سے بنا سکتے ہیں کہ آپ حرُوف کو اعداد یا سمبلز سے تبدیل کر دیں، جیسے ‹a› کو ‹@› کے سمبل سے اور حرف ‹o› کو عدد ‹0› (صفر) سے- اگر ایک ویب سائٹ یا پروگرام پاس ورڈ میں اعداد (نمبرز) کو محدوُد کرتا ہے تو اس صوُرتحال میں جتنے زیادہ حروُف کی اجازت ہو، استعمال کریں-

پاس فریزز

اپنے پاس فریز کو محفوظ طریقے سے استعمال کریں

آپ کو پاس فریز استعمال کرتے وقت مُحتاط رہنا چاہیئے- اگر بُرے لوگ آپ کے پاس فریز کو با آسانی نقل کر سکتے ہیں یا چُرا سکتے ہیں تو پھر اس کا فائدہ نہیں ہے-



پاس فریزیز، مضبوُط پاس ورڈز بنانے اور انہیں یاد رکھنے کا ایک آسان طریقہ ہے-

۱. آپ اپنے ہر اکاؤنٹ یا آلہ کے لیئے الگ پاس فریز استعمال کریں- مثال کے طور پر آپ کبھی بھی اپنے دفتر کے اکاؤنٹ یا بینک اکاؤنٹ کے لیئے استعمال ہونے والے پاس فریز کو کبھی بھی اپنے ذاتی اکاؤنٹس جیسے کہ فیس بُک، یو ٹیوب یا ٹوئیٹر، کے لیئے استعمال نہیں کریں- اس طرح اگر آپ کا کوئی ایک اکاؤنٹ ہیک ہو بھی جاتا ہے تو آپ کے باقی اکاؤنٹس محفوُظ رہتے ہیں- اگر آپ کو کافی زیادہ پاس فریزیز یاد رکھنے پڑتے ہیں (جو کہ ایک عام بات ہے) تو اس صوُرت میں آپ پاس ورڈ مینیجر استعمال کریں- یہ ایک خاص پروگرام ہے جو آپ کے تمام پاس فریزیز کو محفوُظ طریقے سے ذخیرہ کرتا ہے- اس طرح آپ کو صرف اپنے کمپیوٹر یا آلہ اور پاس ورڈ مینیجر پروگرام کا پاس فریز یاد رکھنا پڑتا ہے-

۲. آپ کبھی بھی اپنے پاس فریز یا اسے تخلیق کرنے کے طریقے کا کسی کے ساتھ اشتراک نہیں کریں بشمول آپ کے ساتھ کام کرنے والے لوگوں یا آپ کے سپروائزر کے- یاد رکھیں کہ پاس فریز ایک راز ہے اس لیئے اگر کسی کو اس کا علم ہو جاتا ہے تو پھر وہ مزید محفوُظ نہیں رہتا- اگر آپ غلطی سے کسی پاس فریز کا اشتراک کسی کے ساتھ کرتے ہیں یا آپ کو لگتا ہے کہ آپ کا پاس فریز چوری ہو گیا ہے یا کسی کو اس کے بارے میں علم ہو گیا ہے تو آپ اسے فوراً تبدیل کر دیں- صرف ایک صوُرت میں یعنی ہنگامی حالت میں آپ اپنے خاص ذاتی پاس فریزیز کا اشتراک اپنے خاندان کے قابلِ بھروسہ شخص سے کر سکتے ہیں- ایک طریقہ یہ ہے کہ آپ اپنے اہم ذاتی پاس فریزیز کو کہیں لکھ دیں (اس بات کو یقینی بنائیں کہ وہ آپ کے دفتر سے متعلق نہیں ہو)، اور اسے کسی محفوُظ جگہ پر ذخیرہ کر دیں، اور اس جگہ کا اشتراک خاندان کے کسی انتہائی قابلِ بھروسہ فرد سے کریں- اس طرح اگر آپ کے ساتھ اگر کچھ ہو جاتا ہے اور آپ کو مدد کی ضرورت ہوتی ہے تو آپ کے پیارے ان اہم اکاؤنٹس تک رسائی حاصل کر سکتے ہیں-

۳. آپ عوامی کمپیوٹرز، جیسے کہ ہوٹلز یا انٹرنیٹ کیفے، کو اپنے اکاؤنٹس تک رسائی کے لیئے استعمال نہیں کریں- چونکہ ان کمپیوٹرز کو کوئی بھی استعمال کر سکتا ہے اس لیئے ہو سکتا ہے کہ یہ مُتاثرہ ہوں اور آپ کے تمام ‹کی اسٹروکس› کو محفوُظ کر رہے ہوں- آپ اپنے اکاؤنٹس کو صرف قابلِ بھروسہ کمپیوٹرز اور موبائل آلات کے ذریعے ‹لاگ اِن› کریں-

۴. آپ ان ویب سائیٹس سے ہوشیار رہیں جو آپ سے ذاتی سوالات کا جواب مانگتی ہوں- یہ وہ سوالات ہوتے ہیں جن کی ضرورت آپ کو پاس فریز بھولنے کی صوُرت میں اُسے ‹ری سیٹ› کرنے کے لیئے پڑتی ہے- مسئلہ یہ ہے کہ ان سوالات کے جوابات اکثر انٹرنیٹ یا شاید آپ کے فیس بُک پیج پر پر موجود ہوتے ہیں- آپ اس بات کو یقینی بنائیں کہ اگر آپ ذاتی سوالات کا جواب دیتے ہیں تو اس میں صرف ایسی معلوُمات ہونی چاہیئے جو کہ انٹرنیٹ پر موجود نہ ہو یا وہ فرضی معلوُمات ہوں جو کہ آپ نے خود بنائی ہو- کیا آپ اپنے سکیورٹی سوالات کے تمام جوابات یاد نہیں رکھ سکتے ہیں؟ اس کے لیئے آپ کسی موضوُع کا انتخاب کریں جیسے کہ فلم کا کوئی کردار، اور پھر اپنے جوابات اس کردار کو سامنے رکھتے ہوئے دیں- ایک اور طریقہ یہ ہے کہ آپ پھر سے پاس ورڈ مینیجر کا استعمال کریں کیونکہ کئی پاس ورڈ مینیجرز آپ کو اضافی معلوُمات ذخیرہ کرنے کا اختیار دیتے ہیں-

پاس فریزز

۵. کئی آن لائن اکاؤنٹس آپ کو ایک سہولت فراہم کرتے ہیں جو کہ ٹو-فیکٹر اوتھنٹیکیشن یا ٹُو-اسٹیپ ویریفیکیشن کہلاتی ہے- اس طریقہ کار میں آپ کو ‹لاگ اِن› کرنے کے لیئے پاس فریز کے علاوہ بھی کُچھ چاہیئے ہو گا جیسے کہ آپ کے اسمارٹ فون پر بھیجا گیا پاس کوڈ- یہ اختیار صرف پاس فریز استعمال کرنے سے کہیں زیادہ محفوُظ ہے- جب بھی مُمکن ہو آپ اس طرح کے مضبوط اوتھنٹیکیشن کے طریقوں کو فعّال کر دیں اور اُنہیں استعمال کریں-

۶. اکثر موبائل آلات تک رسائی PIN کے ذریعے محفوُظ کی گئی ہوتی ہے- یاد رہے کہ PIN بھی ایک پاس ورڈ کے سوائے کچھ بھی نہیں ہے- آپ کی PIN جتنی لمبی ہوگی، آپ کے آلات اُتنے ہی زیادہ محفوُظ ہوں گے- کئی موبائل آلات آپ کو PIN نمبر کو کسی پاس فریز یا بایومیٹرک، جیسے کہ فنگر پرنٹ، سے تبدیل کرنے کی اجازت فراہم کرتے ہیں-

۷. اگر آپ کوئی اکاؤنٹ مزید استعمال نہیں کر رہے ہیں تو اس بات کو یقینی بنائیں کہ آپ اُسے بند، ڈیلیٹ یا غیر فعّال کر دیں-

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:

پاس ورڈ مینیجر: https://securingthehuman.sans.org/ouch/2015#october2015

ٹُو-اسٹیپ ویریفیکیشن: https://securingthehuman.sans.org/ouch/2015#september2015

اپنے لاگ اِن کو لاک کرنا: https://lockdownyourlogin.com

SANS SEC301 - سائبر سیکورٹی کی بنیاد کا ۵ دن کا کورس: https://sans.org/sec301

ایڈیٹوریل بورڈ: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley۔

ترجمہ: شعیب ہاشمی