ستمبر ۲۰۱۷ OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

پاس ورڈ مینیجرز

جائزہ

آن لائن اپنی حفاظت کے لیئے سب سے اہم ترین اقدامات میں سے ایک قدم یہ ہے کہ آپ اپنے ہر اکاؤنٹ اور ایپلیکیشن کے لیئے ایک منفرد اور مضبوط پاس ورڈ بنائیں- بد قسمتی سے آپ کے لیئے ہر اکاؤنٹ کے مختلف پاس ورڈ کو یاد رکھنا تقریباً ناممکن ہے- اس وجہ سے ہی لوگ اپنے پاس ورڈ کو دوبارہ استعمال کرتے ہیں- بدقسمتی سے اپنے پاس ورڈ کو مختلف اکاؤنٹس کے لیئے دوبارہ استعمال کرنا بہت خطرناک ہوتا ہے کیونکہ اگر کسی کو آپ کے ایک اکاؤنٹ کا پاس ورڈ پتہ چل جائے تو وہ آپ کے ان باقی تمام اکاؤنٹس تک رسائی حاصل کر سکتے ہیں جن کا وہی پاس ورڈ ہے- اس کا آسان حل پاس ورڈ مینیجر کا استعمال ہے جسے پاس ورڈ والٹ بھی کہتے ہیں- یہ وہ پروگرامز ہوتے ہیں جو آپ کے تمام پاس ورڈز کو محفوظ طریقے سے ذخیرہ کرتے ہیں جس کی وجہ سے آپ کے لیئے ہر اکاؤنٹ کا الگ پاس ورڈ رکھنا آسان ہوتا ہے- پاس ورڈ مینیجرز اس عمل کو آسان بنا دیتے ہیں کیونکہ آپ کو ہر اکاؤنٹ کا پاس ورڈ یاد رکھنے کے بجائے صرف پاس ورڈ مینیجر کا ماسٹر پاس ورڈ یاد رکھنا پڑتا ہے-

مہمان ایڈیٹر

کرس کرسچینسن کیلی فورنیا میں مقیم ایک انفارمیشن سکیورٹی کنسلٹنٹ ہیں- وہ اس صنعت میں ۲۰ سال کا تجربہ رکھتے ہیں اور ان کے پاس کئی ٹیکنیکل سرٹیفیکیشنز بھی ہیں- انہوں نے کافی کانفرنسز سے خطاب کیا ہے اور اس صنعت کے لیئے کئی مضامین بھی لکھے ہیں- آپ کرس تک **@cchristianson** اور **https://ismellpackets.com** کے ذریعے رسائی حاصل کر سکتے ہیں-

پاس ورڈ مینیجرز کام کیسے کرتے ہیں؟

پاس ورڈ مینیجرز کام اس طرح کرتے ہیں کہ وہ آپ کے تمام پاس ورڈز کو ایک ڈیٹا بیس میں ذخیرہ کر دیتے ہیں، جو کہ والٹ بھی کہلاتا ہے- پاس ورڈ مینیجر والٹ میں موجود تمام مواد کو انکرپٹ کر دیتا ہے اور وہ اس ماسٹر پاس ورڈ کے ذریعے اس کی حفاظت کرتا ہے جس کا صرف آپ کو علم ہوتا ہے- جب آپ کو کوئی پاس ورڈ نکالنا ہو جیسے کہ آن لائن بینکنگ یا ای میل میں لاگ ان ہونے کے لیئے، تو آپ کو والٹ کو کھولنے کے لیئے صرف اپنے ماسٹر پاس ورڈ کو اپنے پاس ورڈ مینیجر میں لکھنا ہو گا- زیادہ تر پاس ورڈ مینیجر خودکار طور پر ہی پاس ورڈ نکال لیتا ہے اور آپ کو محفوظ طریقے سے لاگ ان کر دیتا ہے- اس طرح آپ کے لیئے درجنوں پاس ورڈز بنانا آسان ہو جاتا ہے کیونکہ آپ کو انہیں یاد نہیں رکھنا پڑتا ہے-

کچھ پاس ورڈ مینیجرز والٹ کو آپ کے کمپیوٹر یا موبائل آلہ پر ذخیرہ کرتے ہیں جبکہ دوسرے اسے کلاؤڈ پر ذخیرہ کرتے ہیں- مزید یہ کہ زیادہ تر پاس ورڈ مینیجرز میں آپ کے پاس ورڈ والٹ کے مواد کو ان مختلف آلات میں جن کو آپ نے اجازت دے رکھی ہے، خودکار طور پر سنکرونائز کرنے کی صلاحیت موجود ہوتی ہے- اس طرح جب آپ اپنے لیپ ٹاپ کے پاس ورڈ کو اپڈیٹ کرتے ہیں تو یہ تبدیلی آپ کے باقی تمام آلات میں سنکرونائز ہو جاتی ہے- اس بات سے قطع نظر کہ ڈیٹابیس کس جگہ موجود ہے، آپ کو پاس ورڈ مینیجر کی ایپلیکیشن کو استعمال کرنے کے لیئے اسے اپنے سسٹم یا آلہ پر انسٹال کرنا پڑتا ہے-

پاس ورڈ مینیجرز

جب آپ پہلی بار پاس ورڈ مینیجر انسٹال کرتے ہیں تو آپ کو اپنے ہر اکاؤنٹ کے لاگ ان اور پاس ورڈ کو لکھنا پڑتا ہے یا امپورٹ کرنا پڑتا ہے- اس کے بعد جب بھی آپ کسی نئے اکاؤنٹ کو رجسٹر کرتے ہیں یا کسی موجودہ اکاؤنٹ کا پاس ورڈ اپڈیٹ کرتے ہیں تو پاس ورڈ مینیجر اس کی شناخت خود ہی کر لیتا ہے اور والٹ بھی خودکار طور پر اپڈیٹ ہو جاتا ہے- یہ اس لیئے ممکن ہوتا ہے کہ زیادہ تر پاس ورڈ مینیجرز آپ کے ویب براؤزر کے ساتھ کام کرتے ہیں- اس انٹیگریشن کے ذریعے پاس ورڈ مینیجرز آپ کو خودکار طور پر ان ویب سائٹس پر لاگ ان کر دیتا ہے-

ایک اہم بات یہ ہے کہ جو ماسٹر پاس ورڈ آپ پاس ورڈ مینیجر کے مواد کی حفاظت کے لیئے استعمال کرتے ہیں وہ بہت مضبوط ہو اور دوسروں کے لیئے اس کا اندازہ لگانا مشکل ہو- بلکہ ہمارا مشورہ یہ ہے کہ آپ کسی جملے کو اپنا ماسٹر پاس ورڈ بنا دیں، جو کہ پاس ورڈز کی مضبوط ترین قسم میں سے ایک ہے- اگر آپ کا پاس ورڈ مینیجر ٹوُ اسٹیپ ویریفکشیوں کی حمایت کرتا ہے تو آپ اُسے ضرور پاس ورڈ مینیجر کے لیئے استعمال کریں- آخری بات یہ کہ آپ اپنے ماسٹر پاس ورڈ کو یاد رکھیں کیونکہ اگر آپ اُسے بھُول گئے تو آپ اپنے کسی بھی پاس ورڈ تک رسائی حاصل نہیں کر سکیں گے-

پاس ورڈ مینیجرز آپ کے مختلف پاس ورڈز کو محفوظ طریقے سے ذخیرہ کرنے کا ایک بہت آسان طریقہ ہے-

پاس ورڈ مینیجرز کا انتخاب کرنا

آپ کئی پاس ورڈ مینیجرز میں سے کسی کا بھی انتخاب کر سکتے ہیں- ہم نے وسائل والے حصّے میں ایک لنک فراہم کیا ہے جہاں پاس ورڈ مینیجرز کے تبصرے موجود ہیں- اپنے لیئے سب سے بہترین پاس ورڈ مینیجر کا انتخاب کرتے وقت مندرجہ ذیل باتوں کا خیال رکھیں:

- آپ کا پاس ورڈ مینیجر آپ کے استعمال کے لیئے آسان ہونا چاہیئے- اگر آپ کو اُسے سمجھنے میں دُشواری پیش آ رہی ہے تو آپ کوئی ایسا حل تلاش کریں جو آپ کی ضروریات اور مہارت کے عین مُطابق ہو-
- پاس ورڈ مینیجر کو ہر اُس آلہ پر کام کرنا چاہیئے جس میں آپ کو پاس ورڈز لگانے کی ضرورت ہو- یہاں اس بات کا بھی خیال رکھیں کہ اُس پاس ورڈ مینیجر کے ذریعے آپ کے تمام آلات کے پاس ورڈز کو سنکرونائز کرنا آسان ہو-
- آپ صرف معروف پاس ورڈ مینیجرز کا استعمال کریں- اُن مصنوُعات سے ہوشیار رہیں جنہیں آئے ہوئے زیادہ عرصہ نہیں گزرا ہو یا جن کے بارے میں کمیونیٹی نے کم یا کوئی بھی آراء نہیں دی ہوئی ہو- سائبر مُجرمان آپ کی معلومات چُرانے کے لیئے جعلی پاس ورڈ مینیجرز بنا سکتے ہیں- آپ ان وینڈرز سے بھی بہت ہوشیار رہیں جو اس بات کو فروغ دیتے ہیں کہ اُنہوں نے کوئی اپنا انکرپشن کا حل بنایا ہے-
- آپ اُن پاس ورڈ مینیجرز سے اجتناب کریں جو یہ دعوہ کرتے ہوں کہ وہ آپ کا ماسٹر پاس ورڈ ریکوؤر کر سکتے ہیں کیونکہ دراصل اس کا مطلب یہ ہے کہ اُنہیں آپ کے ماسٹر پاس ورڈ کا علم ہے اور یہ آپ کے لیئے خطرناک ثابت ہو سکتا ہے-
- آپ اس بات کی یقین دہانی کر لیں کہ آپ جس وینڈر کا بھی انتخاب کرتے ہیں، وہ فعال طور پر پاس ورڈ مینیجر کو اپڈیٹ اور پیچ کرتا ہو اور اس بات کو بھی یقینی بنائیں کہ آپ ہمیشہ اُس کا جدید ترین ورژن استعمال کر رہے ہوں-

پاس ورڈ مینیجرز

- پاس ورڈ مینیجر میں آپ کے لیۓ خودکار طور پر مضبوط پاس ورڈ بنانے کی صلاحیت موجود ہونی چاہیۓ اور اسے آپ کے منتخب کیۓ ہوۓ پاس ورڈ کی لمبائی بھی دکھانی چاہیۓ-
- پاس ورڈ مینیجر کو آپ کی دوسری حسّاس معلومات کو ذخیرہ کرنے کا اختیار دینا چاہیۓ جیسے کہ آپ کے خفیہ سوالات کے جوابات، کریڈٹ کارڈز یا فریکوئنٹ فلایر نمبرز-

پاس ورڈ مینیجرز آپ کے تمام پاس ورڈز اور حسّاس معلومات کو محفوظ طریقے سے ذخیرہ کرنے کا بہت زبردست طریقہ ہے- البتہ چونکہ یہ بہت اہم معلومات ذخیرہ کرتا ہے اس لیۓ آپ اس بات کو یقینی بنائیں کہ آپ کا ماسٹر پاس ورڈ مضبوط اور مُنفرد ہے اور نہ صرف کسی حملہ آور کے لیۓ اس کا اندازہ لگانا مشکل ہو بلکہ آپ کے لیۓ اسے یاد رکھنا بھی آسان ہو-

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:

۲۰۱۷ کے بہترین پاس وورڈز:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
پاس فریزیز:	https://securingthehuman.sans.org/ouch/2017#april2017
ٹُواسٹیپ ویریفیکیشن:	https://securingthehuman.sans.org/ouch/2015#september2015
اپنے لاگ اِن کو لاک کرنا:	https://lockdownyourlogin.com
SANS کی آج کی سیکورٹی تجویز:	https://www.sans.org/tip-of-the-day

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

ترجمہ: شعیب ہاشمی