禪

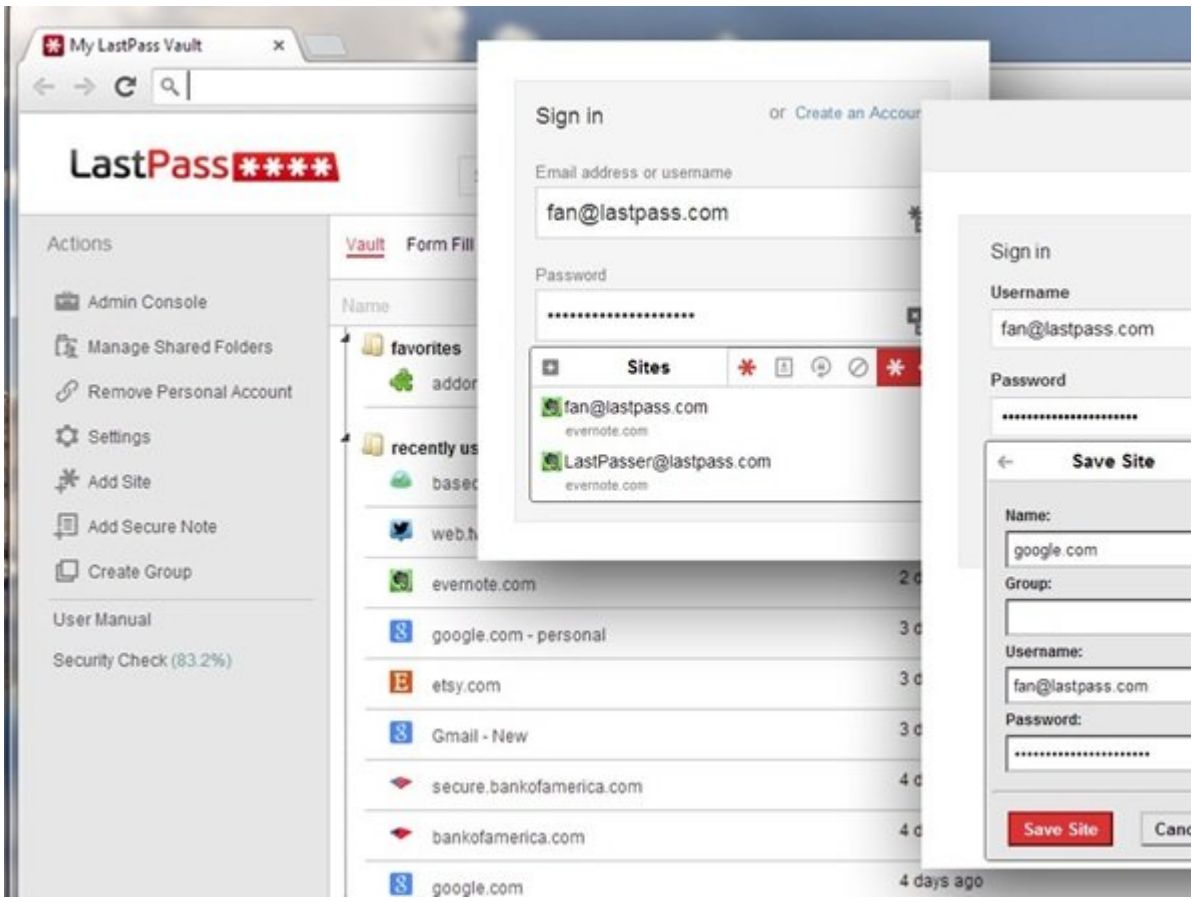
چند راهکار ساده امنیتی

به این چهار نکته توجه کنید تا هک نشوید !

جرایم سایبری باعث به وجود آمدن یک بازار چند میلیارد دلاری شدهاند. بهطوری که هم به سازمانها و هم به افراد عادی صدمات جبرانناپذیری را وارد میکنند. اما اگر به این چند راهکار ساده توجه کنید، این توانایی را پیدا خواهید کرد که از خود در برابر این حملات محافظت به عمل آورید.

کایل لیدی محقق و مهندس توسعه در Duo Security در این ارتباط گفته است: «اگر شما یک هدف باشید که البته صادقانه بگویم، شرکتها هدف اصلی هستند، با اتکا به یکسری اقدامات زیربنایی هم به خود و هم به شرکت مطبوعتان در این زمینه کمکهای فراوانی خواهید کرد.» Tech Insider به تازگی گفتگویی با لیدی در این ارتباط انجام داده است. گفتگویی که دو محور اصلی در آن مورد توجه قرار گرفتهاند. هکرها چگونه به سیستمها نفوذ میکنند و چگونه میتوان با رعایت چند توصیه ساده این مدل حملات را متوقف کرد. در ادامه توصیههای ارائه شده از سوی این کارشناس امنیتی را خواهیم خواند.

مطلب پیشنهادی



5 علامت هشداردهنده هک شدن یک برنامه وب

گذرواژههای 14 کاراکتری

گذرواژهای مورد استفاده توسط کاربران حداقل باید از 14 کاراکتر تشکیل شده باشد . گذرواژههایی که در لغتنامهها نتوانید آنها را پیدا کنید . اگر نگاهی به 25 مورد از بدترین گذرواژههای سال 2015 داشته باشیم، به کلماتی همچون 123456 ، football و Password برخورد خواهیم کرد . گذرواژههایی که به آسانی توسط یک هکر ممکن است حدس زده شوند. ما در اینجا درباره یک هکر که سعی میکند، گذرواژههای مختلفی را مورد آزمایش قرار دهد، صحبت نمیکنیم، بلکه صحبت از نرمافزارهایی میکنیم که این توانایی را دارند تا در یک دقیقه صدها یا هزاران گذرواژه را حدس بزنند . در نتیجه بهتر است از گذرواژههایی استفاده کنید که بیش از اندازه عجیب باشند . لیدی در این ارتباط گفته است : «اگر من بتوانم گذرواژه شما را در یک لغتنامه شناسایی کنم، در نتیجه یک هکر نیز توانایی انجام چنین کاری را خواهد داشت.» لیدی توصیه میکند از گذرواژههایی استفاده کنید که حداقل طول آنها 14 کاراکتر باشد . (خودش از گذرواژههایی با طول 24 کاراکتر استفاده میکند .) گذرواژههایی که از ترکیب حروف بزرگ و کوچک و سمبلها ساخته شده است. یک گذرواژه پیچیده چیزی شبیه به Syd#2n3l_!4pss است؛ ترکیبی که معنای واقعی نداده و سمبلهای مورد استفاده در آن یک هکر را گیج میکنند . در نتیجه به عنوان یک گذرواژه ایدهآل به شمار میروند . از طرفی به کارگیری یک جمله شبیه به "this password security thing words" یک گذرواژه گمراه کننده برای یک هکر به شمار میرود . لیدی میگوید : «حدس زدن این چنین گذرواژههایی برای یک هکر واقعا مشکل خواهد بود . شخصی که در نظر داشته باشد چنین گذرواژههایی را بشکند باید زمان و منابع مختلف زیادی را بارها و بارها مورد آزمایش قرار داده تا بتواند فرضیه خود را آزمایش کند .» اما در طرف مقابل این چنین گذرواژههایی برای کاربران مشکلساز هستند، به دلیل اینکه به خاطرسپاری یک گذرواژه طولانی از کاراکترهای عجیب و غریب کار مشکلی خواهد بود . به کارگیری یک مدیر گذرواژه، شما را از حفظ کردن این چنین گذرواژههایی بی نیاز میکند . یک مدیر گذرواژه شبیه به LastPass یا 1Password به شیوه کاملا ایمن همه گذرواژههایی که توسط سرویسهای مختلف از ایمیل گرفته تا حساب بانکی را در یک مکان ذخیره میکند . در نتیجه حفظ کردن گذرواژههای مختلف ضرورتی نخواهد داشت.

My LastPass Vault
LastPass****
Actions
Admin Console
Manage Shared Folders
Remove Personal Account
Settings
Add Site
Add Secure Note
Create Group
User Manual
Security Check (83.2%)
Vault
Form Fill
Name
favorites
recently us
Sign in
or Create an Accour
Sites
Save Site
Save Site
Canc

Email address or username: fan@lastpass.com
Password: ••••••••••••••••••••

fan@lastpass.com evernote.com
LastPasser@lastpass.com evernote.com

evernote.com 2 d
google.com - personal 3 d
etsy.com 3 d
Gmail - New 3 d
secure.bankofamerica.com 4 d
bankofamerica.com 4 d
google.com 4 days ago

Username: fan@lastpass.com
Password: ••••••••••••••••••••

Name: google.com
Group:
Username: fan@lastpass.com
Password: ••••••••••••••••••••

[illegible]

[illegible]

Google
2-Step Verification
A text message with your code has been sent to: (***) ***-**95
123456
Verify
Don't ask for codes again on this computer

[illegible]

[illegible]

[illegible]

میشوند که واقعی به نظر میرسند . در نتیجه قضاوت در مورد آنها در نگاه اول به سختی امکانپذیر است . یک کلاهبردار ممکن است ایمیلی برای شما ارسال کند مبنی بر این موضوع که حساب پیپال شما هک شده است و شما باید گذرواژه خود را بهروزرسانی کنید . اما زمانیکه روی لینک مربوطه کلیک میکنید، شما گذرواژه خود را به او تقدیم خواهید کرد . در حالی که مشاهده میکنید، هیچ چیز تغییر پیدا نکرده است . لیدی در این ارتباط گفته است : «برای آنکه اطمینان حاصل کنید که یک صفحه معتبر و قانونی شبیه به Paypal.com و نه به یک سایت جعلی با آدرس www.paypalsecurity.xyz وارد شدهاید باید به دقت به آدرس توجه کنید . اگر هرگونه شکی در این ارتباط پیدا کردید، ضروری است که موضوع را به دقت بررسی کنید .»

ضد مهندسی اجتماعی

همانند مشکل شماره سه، باید مراقب تماسهای مشکوک باشید. هکرها اغلب با استفاده از مهندسی اجتماعی سعی میکنند شما را متقاعد سازند که قصد کمک کردن به شما را دارند . (بدافزار صفحه آبی مرگ، قربانیان خود را فریب میدهد). بنابراین مهم است که یک شک و تردید نسبت به تماسهایی داشته باشید که در آن ادعا میشود از نمایندگی خدمات مشتریان تماس گرفتهاند و از شما گذرواژهتان را درخواست میکنند . تقریبا هیچ شرکتی در تماس تلفنی از شما درخواست نمیکنند گذرواژه خود را برای او بازگو کنید . اگر چنین تماسهایی داشتید، باید مشکوک شوید .»

شاید به این مقالات هم علاقمند باشید :

هکهای ترسناک باجافزارها رو به افزایش است

One Time Password:
53078219
Submit

رمزعبورهایی از جنس آیکون و الگوها

[5]

[ ]

[+]

[7]







:
:
:
:
10:35 - 25/11/1394
:
- - - -

:https://www.shabakeh-mag.com/security/2867