



کلیک شما



سؤالات خود را ب.clickhelp@jamejamonline.com ایمیل کنید تا پاسخگوی شما باشیم. ذکر نام، نام خانوادگی و شهریار و سوابی محل اقامت خود را فرموش نکنید.

محمد رضا:

آیا در ایران امکان دایریوت کردن پیامک به گوشی دیگری وجود دارد تا بتوانیم مانند انتقال مکالمه پیامک های اینترنال دهیم؟

کلیک:

ابتدا باید بگوییم متاسفانه این قابلیت به نحوی که شما می خواهید قابل انجام نیست و نمی توانید مانند تماس های عادی برای دایریوت کردن پیامک ها نیز اقدام کنید. البته راه های جانبی برای انجام این کار وجود دارد، ولی این راه ها به معنای دایریوت کردن مستقیم پیامک نیست. نرم افزارهایی مانند SMS forward می توانند پیامک را روی دستگاهی دریافت کرده و بلا فاصله آن را به شماره از پیش تعیین شده دیگری ارسال کنند. در شرایط دایریوت عادی، اگر گوشی اولی خاموش باشد، باز هم دایریوت انجام خواهد شد، ولی با استفاده از این نرم افزار باید همیشه تلفن همراه اولیه روشن باشد که این امر ممکن است با نیاز شما در تضاد باشد. اگر از کاربران سیستم عامل iOS هستید می توانید پیام های ورودی خود را به دیگر دستگاه های مجذب به این سیستم عامل که در اختیار دارید نیز فوروارد کنید. برای این کار به بخش Settings روید و سپس گزینه Messages را انتخاب کنید و در نهایت گزینه Text Message Forwarding را فعال کنید. مانند گزینه های شما که به همین حساب کاربری اپل وصل هستند، نمایش داده شود و با فعال کردن گزینه مقابله هر مورد می توانید پیام های خود را علاوه بر دستگاه مبدأ، روی این دستگاه نیز مشاهده کنید. البته باز هم مشکل اشاره شده در روش اول پارچه خواهد بود و این کار به معنای دایریوت کردن واقعی پیامک ها نخواهد بود، ولی ممکن است نیاز شما را بطرف کند.

استخدام سرایدار هتل

آقا متأهل (۳۰ تا ۵۵ سال) بومی متل قو
مازندران - با خامن معتبر - حقوق ۲/۵۰۰ ثابت
شماره: ۰۲۱۴۴۲۱۷۴۶۶

بدون سیله اعلام می گردد که گواهینامه های پایان تحصیلات دوره کارشناسی به شماره ۱۹۹۲۸ مورخ ۱/۲۲ و پایان تحصیلات دوره کارشناسی ارشد به شماره ۱۵۱۶۵ مورخ ۱۳۷۸/۰۱/۲۲ صادر شده از دانشگاه صنعتی شریف متعلق به اینجابت علی رضا یعقوبی کهنه‌گی فرزند حسینعلی به شماره نامه ۰۴۱ صادره از تهران متنو ۱۳۵۲/۱۱/۲۲ مفقود گردیده و از درجه اعتبار ساقط می باشد.

با چند روش برای سنجش قدرت رمزهای عبور خود آشنا شوید

امنیت داده های دنیای نامن اینترنت

امنیت تلفن های همراه هشمند رایانه های خانگی بسیار مهم هستند و با توجه به مشکلات مانند هک حساب های کاربری و تهدیدهای امنیتی، نیاز به داشتن رمزهای کاربری به ضرورت تبدیل شده است، ولی مشکل اینجاست که بسیاری از ما نمی دانیم رمز عبورمان چقدر امن است و به همین دلیل ممکن است رمزهای ضعیف را تاختاب کنیم. چنان راه کار آنلاین حرفا های برای سنجش قدرت رمزهای عبور وجود دارد که هیچ کدام نیازی به ارائه منبع رمز عبور ندارد و برای مثال لازم نیست به آئانشان دهدی که رمز عبور مد نظر شما به کدام حساب کاربری وصل است. به همین دلیل می توانید رمزهای عبور مختلف را در آنها بدون نگرانی امنیتی چک کنید.



احمد محمد حسینی

مدیر تیم

سیستم دانشگاه ایلینوی شیکاگو

This screenshot shows a password strength test interface. At the top, it says "Password strength test" and "This strength tester runs on your local machine and does not send your password over the network." Below this, there's a password input field containing "clickmagazine@gmail.com" and a complexity scale from "Very Strong" to "Weak". A table below details the password's complexity based on various criteria like length, character types, and randomness. The table also includes requirements for a strong password and common password patterns.

این دانشگاه به رویکرد تحقیقاتی خود رزمیه امنیت مشهور است و به همین دلیل نیز یک سیستم بررسی قدرت رمز عبور رایگان را طراحی و عرضه کرده است که برای استفاده از آن باید وارد این وب سایت شوید: <https://www.uic.edu/apps/strongpassword/> پس از ورود به این صفحه، یک کادر قابل مشاهده است که می توانید رمز عبور مدنظر خود را در آن مدهد و در ادامه می توانید مشاهده کنید و ضعیت رمز شما چطور است. همچنین زنگ بندی این صفحه را نیز رمزهای نیرومند را از رمزهای ضعیف (بازگر قرمز) تفکیک می کند. از جمله بهترین قابلیت های این بخش این است که پایین بخش بررسی رمزگزینه های جالب زیر وجود دارد:

- Time it takes to crack your password
- Has this password been previously exposed in data breaches?
- Is this password strong enough?

این گزینه نشان دهنده زمانی است که یک سیستم خودکار رایانه ای برای حدس زدن رمز عبور شما به آن نیاز دارد. بنابراین اگر رمز شما در چند ساعت قابل شناسایی باشد، باید به فکر رمزی جدید و نیرومندتر باشید.

Has this password been previously exposed in data breaches?

این گزینه می دهد که آیا در هیچ یک از افشا های عمومی رمزهای عبور هکرهای این رمز در فهرست رمزهای لو رفته وجود داشته با خیر که اگر گزینه Noleaks found! برای شناسایی داده شود به این معنی است که رمز شما از این نظر مشکل ندارد.

سیستم Nordpass

This screenshot shows the Nordpass online strength checker interface. It displays the password "Click_magazine@2020" and its strength as "STRONG". Below the password, it lists several password requirements such as "At least 12 characters", "Lowercase letters", "Uppercase letters", "Numbers", and "Symbols". It also indicates that the password is not based on a name, date, or words found in a dictionary. A note at the bottom states that this password has not been exposed in data breaches.

برای استفاده از ابزار آنلاین Nordpass ابتدا وارد این سایت شوید:

<https://nordpass.com/securepassword>

در ادامه از بین دو گزینه ای که در مرکز صفحه مشاهده می کنید روی گزینه No Use Online strength checker کلیک کرده تا به بخش دیگر از صفحه انتقال پیدا کنید. در این بخش یک کادر وجود دارد که می توانید رمز مدنظر خود را در آن وارد کنید. لازم نیست هیچ دکمه ای را فشار دهید و تنها باید یک ثانیه صبر کنید تا نتیجه برای شما نمایش داده شود و در ادامه می توانید مشاهده کنید و ضعیت رمز شما چطور است. همچنین زنگ بندی این صفحه را نیز رمزهای نیرومند را از رمزهای ضعیف (بازگر قرمز) تفکیک می کند. از جمله بهترین قابلیت های این بخش این است که پایین بخش بررسی رمزگزینه های جالب زیر وجود دارد:

Time it takes to crack your password

Has this password been previously exposed in data breaches?

این گزینه نشان می دهد که آیا در هیچ یک از افشا های عمومی رمزهای عبور هکرهای این رمز در فهرست رمزهای لو رفته وجود داشته با خیر که اگر گزینه Noleaks found! برای شناسایی داده شود به این معنی است که رمز شما از این نظر مشکل ندارد.

Comparitech سیستم

This screenshot shows the Comparitech Password Generator interface. It features a "Test my Password Strength" button and a "Password Generator" button. Below these are fields for "Enter Password" and "Generated Password". A note states that generating a unique random password for each of your accounts will significantly reduce your chances of being tracked. The tool is described as safe and simple to use.

می کنیم تیک مقابل گزینه Avoid Ambiguous Characters را فعال کنید. زیرا موجب می شود علائمی که بافت آنها را صفحه کلید بسیار دشوار ساخت. در مجموع می دهد بین حروف کوچک، بزرگ، اعداد و نشانه های گزینه های مدنظر خود را انتخاب کرده و تعداد حداقل مورد نیاز از دو مورد آخر را نیز تعیین کنید. در ادامه با تعیین تعداد کاراکتر های رمز عبور و کلیک روی دکمه generate، رمز عبور پیشنهادی شما ایجاد و برایتان نمایش داده خواهد شد. البته پیشنهاد

یک وب سایت رایگان دیگر برای بررسی قدرت رمز شما که قابلیت جانی جذابی نیز دارد: Comparitech مانند گزینه های دیگری که معرفی کردیم به شما اجازه می دهد با وارد کردن رمز عبور خود در کادر موردنظر به میزان قدرت آن پی ببرید. این سایت حتی مدت زمان مورد نیاز برای هک شدن رمز شما را نیز می گوید، ولی نکته جذاب این است که با ویژگی دیگری به نام Password generator می توانید با وارد کردن قوانین مدنظر خود برای رمز عبور، شاهد ایجاد رمز عبور مناسب تو سط این سیستم باشید. در حقیقت این قابلیت به شما اجازه می دهد بین حروف کوچک، بزرگ، اعداد و نشانه های گزینه های مدنظر خود را انتخاب کرده و تعداد حداقل مورد نیاز از دو مورد آخر را نیز تعیین کنید. در ادامه با تعیین تعداد کاراکتر های رمز عبور و کلیک روی دکمه generate، رمز عبور پیشنهادی شما ایجاد و برایتان نمایش داده خواهد شد. البته پیشنهاد

