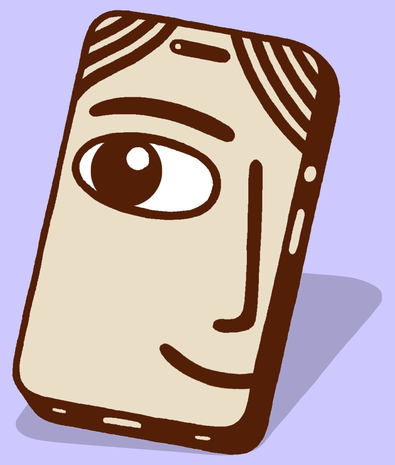
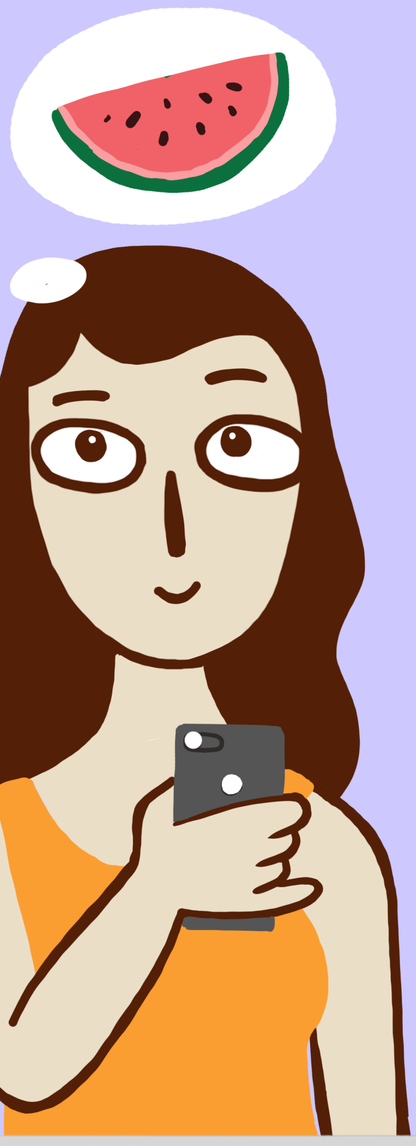


امنیت در فضای مجازی

مدیریت کلمه عبور (قسمت اول)

نبض ایران
تقویت صدای ایرانیان



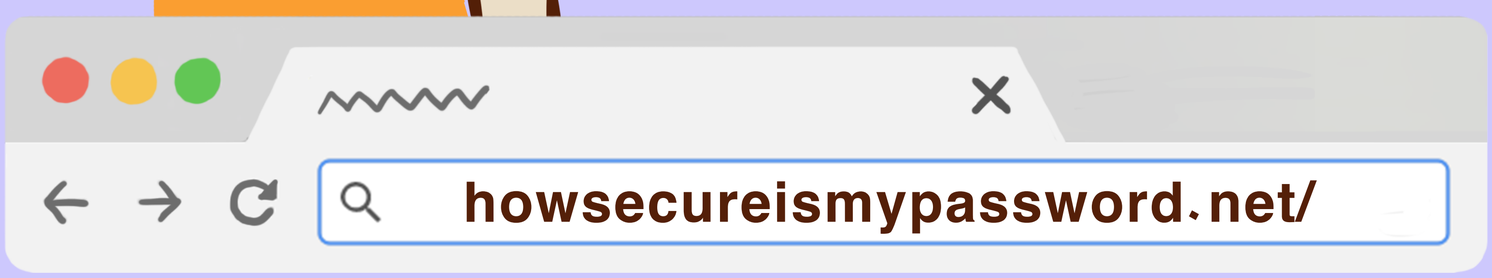
روشی برای ایجاد رمز عبور خوب

به جمله‌ای یا عبارتی فکر کنید، بعد حروفش را بزرگ و کوچک کنید یا عددی یا نمادی اضافه کنید.

می‌توانید خطی از ترانه‌ای انتخاب کنید یا عبارتی که دوست دارید. مثلا من الان به فکر این عبارت هستم «من صبحانه هندوانه خوردم» چون این کاری است که اخیراً انجام دادم. این عبارتی است مخصوص شخص من و در نتیجه یادم می‌ماند و بعید است کسی حدسش بزند (مگر این‌که نزد عموم معروف باشید به عشق هندوانه‌خوری برای صبحانه!).

مثلا به صورت رمز عبور می‌تواند این‌طوری باشد: H3nDOONEYEsobh00n3H!

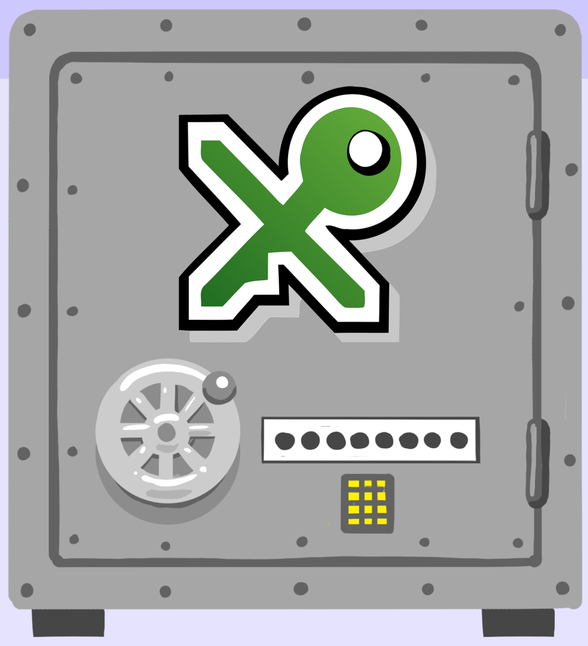
برای این‌که ببینید رمز عبورتان چقدر امن است می‌توانید آن‌را با وسیله‌ای مثل این بررسی کنید:



رمز عبورتان را چطور ذخیره کنید

از آن‌جایی که قرار است رمز عبورهای پیچیده متعددی مثل «H3nDOONEYEsobh00n3H» برای حساب‌های مختلف‌تان داشته باشید، بد نیست از یک نرم‌افزار مدیریت رمز عبور (Password Manager) استفاده کنید.

یک گزینه، نرم‌افزارِ KeePassX است. KeePassX چیزی است مثل گاوصندوقی برای تمام رمز عبورهایتان. ابزاری است رمزگذاری‌شده و متن‌آزاد (اپن سورس)! فقط کافی است یک رمز عبور مادر را بخاطر بسپارید و همان درِ گاو صندوقی که حاوی تمامی رمز عبورهای پیچیده‌تان هست باز می‌کند.



استفاده از نرم افزارهای مدیریت رمز عبور مانند Bitwarden و 1Password هم گزینه‌ای رایگان و قابل اعتماد است. صرف نظر از اینکه کدام نرم افزار را انتخاب می‌کنید، به خاطر بسپارید که پس از استفاده حتما از آن خارج شوید. بدین ترتیب اگر تلفن همراهتان به سرقت رفت دیگران به اطلاعات خصوصی شما دسترسی نخواهند یافت.

1Password

Bitwarden

رمز عبورتان را چطور ذخیره نکنید

- از رمز عبورهایتان استفاده مجدد نکنید. حواستان باشد که هر حساب رمز عبور مجزای خودش را داشته باشد.
- هیچ وقت رمز عبورتان را روی کاغذ نیاورید و آن را روی صفحه لپ‌تاپ و یا میز کارتان نچسبانید. این کار رمز عبور شما را در معرض سرقت و نگاه‌های کنجکاو قرار می‌دهد. همچنین به هیچ وجه رمز عبور خود را در تلفن همراه و سیستم‌های کامپیوتری ذخیره نکنید و برای این کار حتما از نرم افزارهای مدیریت گذرواژه استفاده کنید.
- اگر هکری توانست به یک رمز عبور دست پیدا کند، فقط یک حساب‌تان آسیب می‌بیند!
- رمز عبورهایتان را در برنامه کاوشگرتان ذخیره نکنید!

به کارانداختن تصدیق دومرحله‌ای

تصدیق دو مرحله ای (یا تایید دو مرحله‌ای) چیست؟ این یک لایه امنیتی اضافی است که از شما می‌خواهد اطلاعات بیشتری را برای ورود به حساب خود ارائه دهید. این می‌تواند کد تصدیق یک بار مصرفی باشد که از طریق پیامک یا برنامه‌های احراز هویت دریافت می‌کنید و یا حتی به صورت کلید امنیتی سخت افزاری باشد. کلیدهای امنیتی بهترین گزینه هستند اما رایگان نبوده و دسترسی به آن‌ها دشوار است. بهترین گزینه بعدی استفاده از برنامه های احراز هویت مانند Google Authenticator و Authy است.

از آن جا که پیامک را می‌توان به سادگی رهگیری کرد و شماره تلفن را می‌توان از طریق اپراتور تلفن همراه جعل یا هک کرد، دریافت کد تصدیق از طریق پیامک شکل بسیار ضعیفی از تصدیق دو مرحله‌ای است.