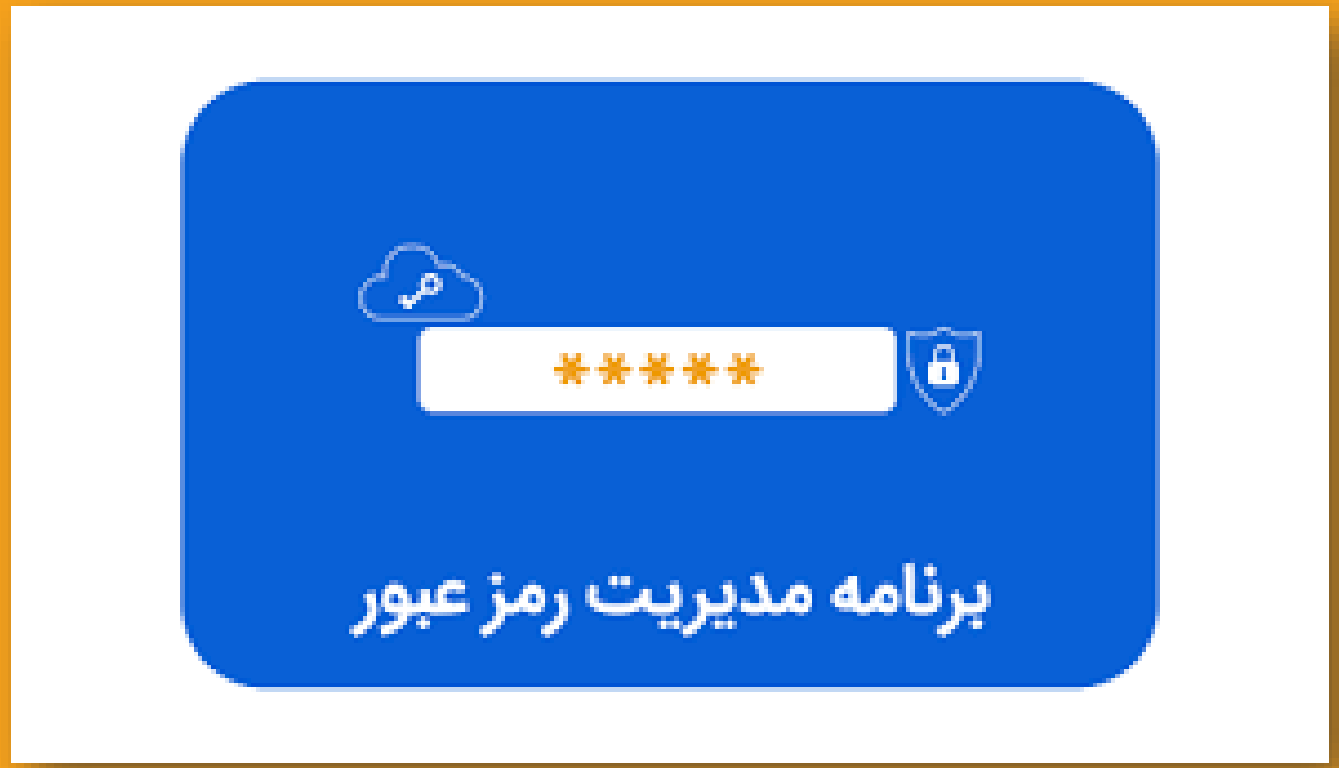
ارائه ۱ : PASSWORD MANAGER چیست؟

سید علیرضا بنی موسوی

پروژه Password manager

مباحث ویژه در برنامه نویسی کد ۱



نرم افزار مدیریت رمز عبور یک برنامه کاربردی است که اطلاعات کاربری آنلاین را ذخیره و مدیریت میکند و می توان آن را نوعی طاق ((vaultدر نظر گرفت که رمزهای عبور را به طور ایمن نگه می دارد. به علاوه برنامه مدیریت رمز عبور دسترسی به سایت ها و برنامه های کاربردی را ساده تر می کند زیرا به صورت خودکار اطلاعات ورود به سیستم را وارد میکند.

تمام کسانی که از یک کامپیوتر یا تلفن همراه هوشمند استفاده می کنند به احتمال زیاد با جابجایی بین برنامه ها و وب سایت ها در طول روز درگیر هستند. یکی از دلایل محبوبیت برنامه های مدیریت رمز عبور این است که در اکثر موارد به خاطر نمی آورید که کدام اعتبارنامه مربوط به کدام سامانه یا وب سایت است. در واقع با برنامه مدیریت رمز عبور افراد به جای مدیریت چندین اعتبارنامه تنها لازم است یک رمز عبور را به خاطر بسپارند.

این موضوع کاربران را تشویق به استفاده از رمزهای عبور پیچیده می کند. به عبارت دیگر زمانی که تنها لازم است کاربران یک رمز عبور را به خاطر بسپارند، احتمال کمتری وجود دارد که از رمزهای عبور ساده و قابل حدس استفاده کنند. با این وجود با برنامه مدیریت رمز عبور از دست دادن یا دسترسی هکرها در یک لحظه به تمام اعتبارنامه های ورود به سیستم شما ساده تر است. بنابراین، با وجود اینکه بسیاری از افراد و سازمان ها برنامه های مدیریت رمزعبور را مفید می دانند مهم است که بپرسیم "برنامه های مدیریت رمز عبور چقدر ایمن هستند و چه جایگزین هایی دارند؟"

چرا به برنامه مدیریت رمز عبور نیاز داریم؟

افراد اغلب نگران فراموش کردن گذرواژه های خود هستند و در نتیجه برخی از شیوه های ناامن را برای به خاطرسپاری آنها در پیش می گیرند. یک گزارش نشان داده است که ۳۴ درصد از کاربران از رمزهای عبور یکسانی برای چندین حساب استفاده می کنند، ۲ درصد از آنها رمزهای خود را روی کاغذ یادداشت کرده و ۱۷ درصد آنها رمزهای عبور را بر روی تلفن همراه یا رایانه خود ذخیره می کنند. همچنین هر فرد باید به طور متوسط روزانه ۱۰ رمز عبور را به خاطر سپرده و به طور متوسط سه رمز عبور را در یک ماه فراموش می کند.

این موضوع نه تنها برای افراد، بلکه برای سازمان هایی که در آنها کار می کنند مشکل ساز است. بر اساس گزارش بررسی های نقض داده های Verizonهشتاد و یک درصد از تخلفات مربوط به هک در سال ۲۰۱۸ ناشی از گذرواژه های ضعیف، سرقت شده یا استفاده مجدد از گذرواژه ها بوده است. نتایج یک نقض داده می‌تواند فاجعه بار باشد. به طور میانگین هزینه یک رکورد به سرقت رفته ۱۴۸ دلار است در حالی که کل هزینه یک نقض داده به طور متوسط ۳/۸۶ میلیون دلار است.

با در نظر گرفتن همه موارد گفته شده، واضح است که افراد و سازمان ها به طور یکسان به راهکارهای بهتری برای ذخیره گذرواژه های خود و همچنین درک بیشتر نحوه ذخیره ایمن رمزهای عبور خود نیاز دارند.

سپاس از همراهی شما 🌹

بن مایه : authin.ir/password-manager/