

مدیریت رمز عبور (Password Management)

رمز عبور، خط اول دفاعی شما در برابر دسترسی‌های غیرمجاز به حساب‌ها و اطلاعات حساس است. مدیریت صحیح رمزهای عبور، یکی از کلیدی‌ترین اصول امنیت سایبری است که هم در سطح فردی و هم سازمانی باید رعایت شود.

نکات کلیدی برای مدیریت رمز عبور

۱. رمز عبور قوی انتخاب کنید

- حداقل ۱۲ کاراکتر
- ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها (مانند: #@!)
- از واژه‌های قابل حدس مانند نام، تاریخ تولد یا «۱۲۳۴۵۶» استفاده نکنید
- مثال خوب: @Tg#2024!xyR

۲. برای هر حساب، رمز متفاوت داشته باشید

استفاده از یک رمز برای همه حساب‌ها، خطرناک است. اگر یکی فاش شود، همه حساب‌ها در معرض خطر قرار می‌گیرند.

۳. از نرم‌افزارهای مدیریت رمز عبور استفاده کنید

نرم‌افزارهایی مانند: LastPass , KeePass , Bitwarden به شما کمک می‌کنند رمزهای قوی تولید و به صورت ایمن ذخیره کنید.

۴. احراز هویت دو مرحله‌ای یا Two Factor Authentication (2FA) را فعال کنید

با فعال‌سازی 2FA، حتی اگر رمزتان دزدیده شود، ورود بدون تأیید هویت دوم (مانند کد پیامک یا اپلیکیشن Google Authenticator) ممکن نیست.

۵. رمز عبورها را به‌طور دوره‌ای تغییر دهید

اگر شک دارید که اطلاعات شما درز کرده، بلافاصله رمزها را تغییر دهید.

۶. از ذخیره رمز در مرورگر یا فایل‌های متنی پرهیز کنید

رمزها را در فایل‌هایی مانند Word یا Notepad ذخیره نکنید. اگر هم نیاز به یادداشت دارید، فایل را رمزگذاری کنید یا از نرم‌افزار مدیریت رمز استفاده نمایید.

هشدارها:

- به پیام‌ها یا ایمیل‌هایی که به ظاهر از بانک یا شبکه‌های اجتماعی هستند و رمز عبور می‌خواهند اعتماد نکنید (فیشینگ).
- از اتصال به شبکه‌های وای‌فای عمومی بدون VPN برای ورود به حساب‌های مهم خودداری کنید.