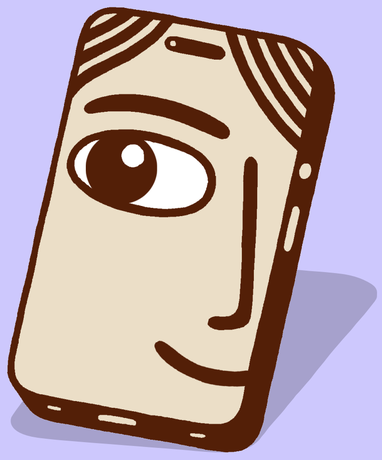


امنیت در فضای مجازی

مدیریت کلمه عبور (قسمت دوم)

نبض ایران
تقویت صدای ایرانیان

رمزعبورهای حساب‌های مشترک را چطور به اشتراک بگذاریم؟

هنگام مدیریت حساب‌های ایمیل و رسانه‌های اجتماعی درون یک تیم، مهم است که متوجه باشید این اطلاعات حساس را چگونه و کجا رد و بدل کنید.

برای حساب کاربری و شبکه اجتماعی گروهی حتما از رمز عبور قوی و تصدیق دو مرحله‌ای استفاده کنید. برای تسریع و کارآمدتر کردن مدیریت تصدیق دو مرحله‌ای می‌توانید نرم افزار احراز هویت مورد انتخاب خود را در تلفن همراه چند عضو مورد اعتماد گروه نصب کنید. از طرف دیگر مجموعه‌ای از کدهای پشتیبان تهیه کرده، آن را در یادداشتی که همه از طریق برنامه مدیریت گذرواژه گروه (مانند Bitwarden) به آن دسترسی داشته باشند ذخیره کنید که در صورت نیاز از آن استفاده شود.

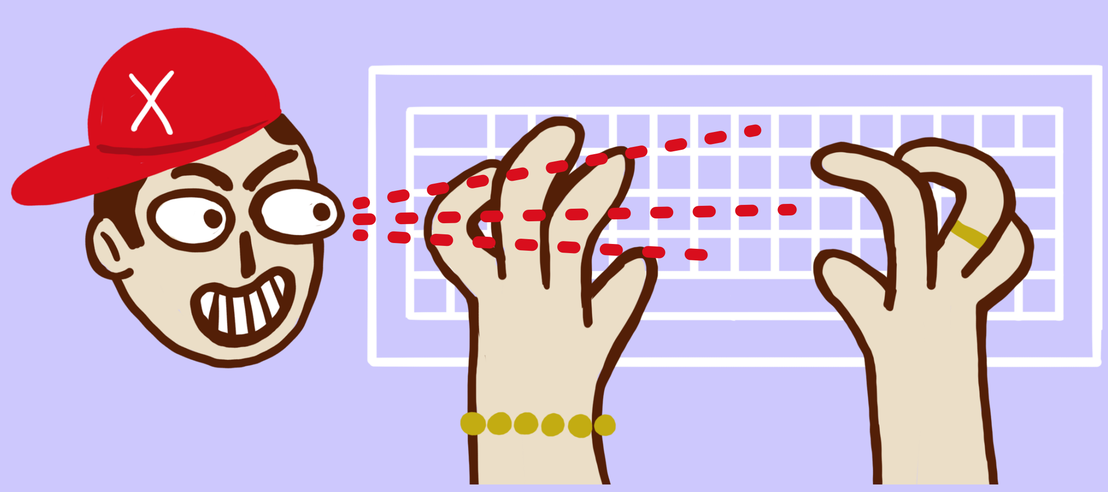
هنگام به اشتراک گذاشتن رمز عبور پیشنهاد می‌شود این کار را در مجاری امن انجام دهید. یکی از ابزارهای مورد دسترسی در ایران نرم‌افزار «وایر» است که با آن می‌توانید پیغام‌هایی بفرستید که بعد از رویت ناپدید می‌شوند و در آن می‌توان بدون شماره تلفن، حساب باز کرد.

حواستان باشد که هیچ دستگاهی هیچ کدام از رمز عبورها را حفظ نکند. رد پا را پاک کنید!

شیوه‌های احتمالی دزدیدن رمز عبور

- حمله فیشینگ: این زمانی است که مهاجم برایتان ایمیلی قلابی می‌فرستد و وانمود می‌کند یکی از شرکت‌هایی است که شما پیش‌شان حساب دارید (مثلا فیس‌بوک، گوگل، آوت‌لوک یا توئیتر).

- مهاجم شاید کار را تا جایی پیش ببرد که از عکس پروفایل شما در صفحه‌ای که باز می‌کنید استفاده کند. حواستان جمع باشد. از شیوه‌های خوبِ فهمیدن این‌که صفحه‌ای که وارد آن شدید صفحه فیشینگ قلابی است یا نه این است که ببینید در آدرس موجود در سمت چپ بالای صفحه https دارد یا نه (اگر نداشت، یعنی قلابی است.) اگر نوشته http و ازتان می‌خواهد رمز عبورتان را وارد کنید، همیشه باید از این کار خودداری کنید. رمز عبورتان را ننویسید!



- اگر فرستنده مشکوک است و مثلا آدرس ایمیلش به جای این‌که @accounts.google.com داشته باشد @gmail دارد قطعا تلاش فیشینگی است برای رسیدن به رمز عبور شما.
- نگاه به شما موقع تایپ کردن: این بخصوص در مواردی به کار می‌رود که رمز عبورتان ساده باشد. فرد ناظر به راحتی می‌تواند ببیند چه رمزی تایپ می‌کنید.