امنیت کلمه عبور (پسورد) پایه

علیرغم تکراری بودن، نکات پایه امنیتی در مورد پسورد همچنان از اثرگذارترین فاکتورها در حفاظت از امنیت شما و دوستانتان است. نکات مقدماتی که باید در نظر گرفته شود به شرح زیر است:

1. تعداد کاراکتر: پسوردهای با تعداد کاراکتر کم به راحتی قابل شکستن هستند چون نرم‌افزارهایی وجود دارد که پسوردهایی با ترکیبی از تمام کاراکترها ساخته و امتحان می‌کند اما این استفاده از این نرم‌افزارها برای پسوردهای طولانی (مثلا بالای ده کاراکتر)بسیار دشوار و زمان‌گیر است
2. ترکیبی بودن پسورد: کاراکترهای پسورد نباید تنها حرف، عدد یا کاراکترهای خاص (مثلا !@#$%^&*) باشد بلکه باید ترکیبی از موارد زیر باشد:
    a. حروف کوچک
    b. حروغ بزرگ
    c. کاراکترهای خاص
    d. اعداد
3. عدم استفاده از پسوردهای قابل پیش‌بینی مثل تاریخ تولد، شماره تلفن و یا نام دوستان و اعضای خانواده
4. عدم استفاده از حروف و اعداد کنار هم روی کیبورد
5. از پسوردهای همسان برای حساب‌های کاربری متفاوت استفاده نکنید. این کار باعث می‌شود که اگر یکی از پسورد هایتان لو رفت، حریم خصوصی و امنیت دیجیتال تان در تمام سایت‌ها که حساب کاربری با پسورد مشابه دارید به خطر بیفتد، پس حتما سعی کنید از پسوردهای متفاوت استفاده کنید.
6. اگر همراه با فردی دیگر پشت کامپیوتر نشسته‌اید و می‌خواهید وارد حساب کاربری خود شوید و نیاز دارید پسورد خود را وارد کنید از او بخواهید به صفحه کلید نگاه نکند یا با دست جلوی دید او را بگیرید تا پسوردتان را حفظ نکند. هیچ وقت از اینکه امنیت و حفاظت از حریم خصوصی خود را جدی می‌گیرید خجالت نکشید و به دیگران هم توصیه کنید همین کار را بکنند.
7. همیشه و در همه جا از سیستم تایید هویت دو مرحله‌ای استفاده کنید. شاید دردسر اضافی به نظر برسد که برای ورود به حساب کابری‌تان در گوگل، اینستاگرام یا فیسبوک مراحل اضافی را طی کنید اما مطمئن باشید که ارزشش را دارد. شما برای تایید هویتتان علاوه بر پسورد می توانید از روش‌های زیر برای تایید هویت‌تان استفاده کنید:
    a. برای گرفتن رمز دوم به جای پیامک از نرم افزار authenticator استفاده کنید. امکان دارد که گوشی شما تحت کنترل باشد و نهادهای امنیتی همزمان با شما رمز دوم را دریافت کنند و وارد اکانت‌تان شوند.
    b. سرویس‌های مختلف می‌توانند با شما تماس تلفنی برقرار کنند و رمز دوم را در اختیارتان قرار دهند.
    c. شما می‌توانید در هنگام فعال کردن سیستم تایید هویت دو مرحله‌ای لیستی از رمزهای پیچیده رو دریافت کنید که بتوانید در صورت عدم دسترسی به تلفن همراه از آنها برای ورود به حساب کاربری‌تان استفاده کنید. توجه داشته باشید که این لیست از رمزهای دوم را در جایی امن و دور از دسترس دیگران نگه دارید تا امنیت‌تان به خطر نیفتد.
    d. استفاده از فلش درایوها که مثل کلید فیزیکی برای ورود به حساب کاربری‌تان استفاده می‌شود روش دیگری برای تایید هویتتان پس از وارد کردن پسوردتان است. به یادداشته باشید که از این

روش تنها در مواردی استفاده کنید که روش‌های دیگر گرفتن رمز دوم برایتان مقدور نباشد. یک فلش درایو که نقش کلید فیزیکی ایمیل‌تان را ایفا می‌کند می‌تواند حساسیت نهادهای امنیتی را برانگیزد. همچنین حفظ امنیت فیزیکی فلش درایو از نکات مهمی است که باید حتما به آن دقت کنید، اگر فلش درایو دست فرد دیگری بیفتد می‌تواند امنیت‌تان را به خطر بیندازد.

8. پسوردهای حساس خود را در اختیار فردی مطمئن، ترجیحا در خارج از کشور قرار دهید تا در صورت بازداشت شدن آن فرد بتواند پسوردتان را عوض کند و اطلاعات حساس‌تان را پاکسازی کند تا نیروهای امنیتی نتوانند با استفاده از محتوای ایمیل و مکاتبات علیه‌تان پرونده‌سازی کنند و یا در بازجویی شما را تحت فشار قرار دهند.
9. یکی از روش‌هایی که هکرها و نهادهای امنیتی برای پیدا کردن پسورد کاربران استفاده می‌کنند، فیشینگ است به نحوی که آنها شما را به صفحه‌ای شبیه به ورود به حساب کاربری هدایت می‌کنند اما آن صفحه جعلی است و فقط برای دزدیدن پسوردتان ساخته شده هر چند می‌تواند خیلی طبیعی نشان دهد و بعد از وارد کردن پسورد شما را به صفحه حساب کاربری‌تان هدایت کند تا همه چیز طبیعی جلوه کند اما در واقع پسوردتان را بدزدند. برای جلوگیری از این کار به نکات امنیتی زیر توجه کنید:
   a. هیچ وقت از طریق لینکی که برای‌تان ارسال شده وارد حساب کاربری خود نشوید، در عوض همیشه خودتان آدرس سایتی که می‌خواهید واردش شوید را وارد کنید.
   b. دقت داشته باشید که پیش از ورود به حساب کابری‌تان مثلا در جیمیل قفل امنیتی ssl به درستی فعال شده باشد.
   c. در حملات فیشینگ شاید به صفحه‌ای هدایت شوید که آدرسی شبیه با صفحه اصلی داشته باشد، مثلا mail.gooogle.com اما در واقع این آدرسی جعلی است که در آن گوگل با سه o نوشته شده است پس همیشه پیش از وارد کردن مشخصاتتان از درست بودن آدرس مطمئن شوید.