

امنیت سایبری پایه

فاز 0-6

چگونه از اطلاعات شخصی، مالی و کاری خود محافظت کنیم؟

جایی که عمران با هوش ملاقات می‌کند.



jaavdan.ir

چرا امنیت سایبری مهم است؟

امروزه تقریباً همه‌ی بخش‌های زندگی ما دیجیتال شده‌اند؛ از بانکداری و خرید اینترنتی گرفته تا فایل‌های کاری، پیام‌رسان‌ها و شبکه‌های اجتماعی.

پیامدها: ضرر مالی، افشای اطلاعات شخصی، سوءاستفاده از هویت، ایجاد مشکل در محیط کار.



امنیت سایبری چیست؟

مجموعه‌ای از روش‌ها، ابزارها و رفتارهایی است که برای محافظت از اطلاعات و دستگاه‌های دیجیتال استفاده می‌شود.

هدف آن محافظت از:

- اطلاعات شخصی
- حساب‌های بانکی و آنلاین
- ایمیل
- موبایل و لپ‌تاپ
- اسناد و فایل‌های کاری
- شبکه‌های سازمانی



مهم‌ترین تهدیدهای امروزی

فیشینگ (Phishing):
پیام یا ایمیل جعلی برای فریب.



بدافزار (Malware):
نرم‌افزار مخرب برای سرقت یا
خرابکاری.



باج‌افزار (Ransomware):
قفل کردن فایل‌ها برای اخاذی.



سرقت رمز عبور:
دسترسی غیرمجاز به حساب‌ها.



مهندسی اجتماعی:
فریب دادن انسان‌ها.



هکرها چگونه فکر می کنند؟

مهاجمان معمولاً ساده ترین و سریع ترین راه را انتخاب می کنند. آن ها از این موارد سوءاستفاده می کنند:

- عجله ی کاربران
- ترس از مسدود شدن حساب
- کنجکاوی
- بی دقتی در خواندن پیام ها

نکته کلیدی: ضعیف ترین حلقه ی امنیت معمولاً انسان است، نه کامپیوتر.



رمز عبور قوی چیست؟

حداقل

۱۲

کاراکتر

ترکیبی از حروف
بزرگ و کوچک

شامل عدد
و نماد

غیر قابل حدس

منحصربه فرد
برای هر حساب



jaavdan.ir

اشتباهات رایج در انتخاب رمز عبور

اطلاعات قابل حدس: تاریخ تولد، شماره موبایل، نام فرزند، نام شرکت.

رمز ضعیف



123456
Ali1380

رمز قوی



P@rvin!Blue#72
d!River9*Stone

خطر رمز عبور تکراری

چرا استفاده از رمز یکسان خطرناک است؟

اگر فقط یکی از حساب‌ها لو برود، مهاجم می‌تواند وارد بقیه‌ی حساب‌های شما هم بشود.



jaavdan.ir

مدیریت رمزهای عبور

به خاطر سپردن ده‌ها رمز قوی کار سختی است.
راهکار: استفاده از مدیر رمز عبور.

مزایا:

- تولید رمزهای قوی
- ذخیره‌ی امن رمزها
- ورود سریع به سایت‌ها
- جلوگیری از تکرار رمزها

نمونه‌های معتبر: Bitwarden, 1Password, KeePass



احراز هویت دومرحله‌ای (2FA)

فرض کنید رمز عبور شما لو برود. اگر احراز هویت دومرحله‌ای فعال باشد، مهاجم هنوز به کد دوم نیاز دارد.

نتیجه: 2FA یکی از مؤثرترین راه‌های جلوگیری از هک حساب‌هاست.



روش‌های کد دوم

- ۱. پیامک (SMS)
- ۲. اپلیکیشن احراز هویت (Authenticator App)
- ۳. بیومتریک (اثر انگشت یا Face ID)



فیشینگ چیست؟

فیشینگ یعنی جعل هویت یک سازمان معتبر برای دزدیدن اطلاعات شما.

مثال‌های رایج:

- پیامک بانکی جعلی
- ایمیل اداره مالیات
- لینک جایزه‌ی اینترنتی
- پیام «حساب شما مسدود می‌شود»



نشانه‌های پیام فیشینگ

اگر این نشانه‌ها را دیدید، شک کنید:

درخواست فوری
و عجولانه



لینک عجیب
یا کوتاه‌شده



غلط‌های
نگارشی



تهدید به مسدود
شدن حساب



جایزه‌ی
غیرمنتظره



درتاساتی
اطلاعات باتبی



درخواست رمزعبور
یا اطلاعات بانکی

مثال واقعی فیشینگ



ترس ایجاد می‌کند.

عجله تحمیل می‌کند.

کاربر را به کلیک روی لینک ناشناس تشویق می‌کند.

رفتار درست: مستقیماً با بانک تماس بگیرید یا از اپلیکیشن رسمی وارد شوید.

بدافزار چیست؟

بدافزار هر نرم افزار مخربی است که برای آسیب رساندن یا سرقت اطلاعات ساخته شده است.



ویروس



تروجان



جاسوس افزار



باج افزار

باج افزار چگونه کار می کند؟



وارد سیستم می شود.

فایل ها را رمزگذاری
می کند.

پیام درخواست پول
نشان می دهد.

قول می دهد فایل ها را
برگرداند (اما تضمینی
وجود ندارد).

دفاع در برابر باج افزار



مهم: داشتن نسخه پشتیبان (Backup) بهترین دفاع در برابر باج افزار است.

امنیت ایمیل

قبل از باز کردن هر ایمیل بررسی کنید:

- فرستنده واقعی کیست؟
- دامنه ایمیل درست است؟
- لینک به کجا می‌رود؟
- منتظر این فایل پیوست بوده‌اید؟



پس کلیک کن.

قانون طلایی:

امنیت تلفن همراه

فقط از فروشگاه‌های
معتبر برنامه نصب کنید.



سیستم عامل را به‌روز
نگه دارید.



قفل صفحه فعال
کنید.



قفل صفحه فعال
کنید.



از اثر انگشت یا ID
Face استفاده کنید.



مجوز برنامه‌ها را
بررسی کنید.



امنیت شبکه‌های اجتماعی

انتشار بیش از حد اطلاعات می‌تواند خطرناک باشد.

مثال‌های خطرناک:

- اعلام سفر و خالی بودن خانه 

- اشتراک شماره تماس 

- ارسال عکس کارت شناسایی 

- نمایش اطلاعات محل کار 



اگر قریانی شدیم چه کنیم؟ (بخش اول)

1

آرامش خود را حفظ کنید.

2

رمزهای مهم را تغییر دهید.

3

احراز هویت دومرحله‌ای (2FA) را فعال کنید.



jaavdan.ir

جاودان: تلاقی هوش و مهندسی در صنعت ساختمان



جایی که عمران با هوش ملاقات می‌کند

ادغام فناوری‌های هوشمند با مهندسی
دقیق برای خلق سازه‌های نسل آینده.



شرکت جاودان سازه گلستان

مرجع رسمی مهندسی هوشمند و مدیریت
پروژه‌های مدرن ساختمانی.

“مهندسی مستقیم، هوشمند و حرفه‌ای”
رویکردی داده‌محور که بر محاسبات دقیق و شواهد
مهندسی استوار است.

ما فقط ساختمان نمی‌سازیم؛ آینده را می‌سازیم

تمرکز بر ساخت و ساز هوشمند و تحول
دیجیتال در صنعت مهندسی.

برای اطلاعات بیشتر به jaavdan.ir مراجعه کنید
دسترسی به سوابق پروژه‌ها، استانداردها و سیستم هویت بصری برند