

## نیازمند

مهندسی اجتماعی  
لزوماً فنی نیست

بسیاری از حملات مهندسی اجتماعی نیازی به اطلاعات فنی تخصصی ندارند و لازم نیست تا یک متخصص رایانه و یک هکر حرفه‌ای به شما حمله کنند. باید نسبت به محیط اطراف اگاه باشد؛ چرا که هر یک از افراد جامعه می‌تواند نقش یک مهاجم را بپذیرد.

مهاجم شما را در حالت‌های  
خاص روانی قرار می‌دهد

حملات مهندسی اجتماعی شما را در حالت‌هایی نظری اضطراب، هیجان، ترس و به صورت کلی حالات خاص روانی قرار می‌دهند تا تمکن و توان تصمیم‌گیری شما را کاهش دهند. لذا باید از تصمیم‌گیری‌های شتاب‌زده پرهیز کنید.

حملات مهندسی اجتماعی  
فریبنده هستند

در اکثر حملات مهندسی اجتماعی، پیشنهاداتی به شما ارائه می‌شود که در نگاه اول، سیار پرسود و جذاب به نظر می‌آیند. باید تلاش کرد تا برو وسوسه پاسخگویی به این دسته از پیشنهادات غلبه کرد؛ چراکه برخی از آنها، طعمه‌هایی برای حملات مهندسی اجتماعی هستند.



## دستاوریزسازی

- در حملات دستاوریزسازی، اولین گام مهاجم، هدف قرار دادن افراد خاص و کسب اطلاعات در مورد آن هاست.
- گام بعد، ارتباط با قربانی است. مهاجم با زیگوی اطلاعاتی که از قربانی به دست آورده است، اعتماد وی را جلب کرده و به او تلقین می‌نماید که دارای اشتراکات زیادی با یکدیگر هستند. در نهایت، اعتماد جلب شده از قربانی سبب می‌شود تا وی، اطلاعاتی که در اختیار افراد غیریقه قرار نمی‌دهد را در به سادگی در اختیار مهاجم بگذارد.



## طعمه‌گذاری

- طعمه‌گذاری با استفاده از ابزارهای فیزیکی انجام می‌شود.
- مهاجم وسایلی نظری لوح فشرده و فلاش دیسک که حاوی بدافزار هستند را به عنایون مختلفی نظری هدایای تبلیغاتی و مطالب مفید و جذاب در اختیار قربانی قرار می‌دهد.
- در مرحله بعد، قربانیان این وسائل را به رایانه‌های خود متصل کرده و با این کار، بدافزارهای مهاجم را اجرا می‌نمایند. به این ترتیب، مسیر دسترسی مهاجم به اطلاعات موجود بر روی این رایانه‌ها فراهم می‌شود.

مهندسي  
اجتماعي

Social Engineering



## حملات صیادی و هرزنامه

- در یک حمله صیادی، ابتدا مهاجم طعمه خود را که معمولاً پیامی جعلی با ظاهری مشابه پیامهای یک نهاد معتبر (نظیر بانک) است را برای تعداد زیادی از کاربران ارسال می‌نماید.

- در گام بعد مهاجم منتظر می‌ماند، به این امید که افراد هدف حمله، فریب خورده و خود را در دام وی گرفتار نمایند. حال ممکن است این کار با کلیک بر روی یک پیوند باشد یا ارسال مشخصات فردی.

سیاست‌های امنیتی  
تعیین کنید

یکی از راهکارهای مؤثر که برای افزایش قدرت و دقت تصمیم‌گیری افراد وجود دارد، آن است که اعضای یک مجموعه همگی از سیاست‌های مشخص و مدونی نمایند. برای مثال، اگر یک سازمان سیاست‌های امنیتی مشخصی را به کارمندان خود ارائه نماید و آنان نیز از سیاست‌های مذکور پیروی نمایند، اشتباها فردی کاهش یافته و کل مجموعه در برابر حملات مهندسی اجتماعی امن‌تر می‌شود.

## چطور از حملات مصون بمانیم؟!

داشته‌های خود  
را بشناسید

نکته مهمی که برای مقابله با حملات مهندسی اجتماعی باید به آن توجه داشت، شناخت اطلاعات ارزشمند و داشته‌های فردی و سازمانی است. در صورتی که هر فرد بداند کدامیک از اطلاعات وی می‌تواند چه ارزشی برای مهاجمان داشته باشد، در زمان ارائه این اطلاعات به دیگران با احتباط بیشتری عمل کرده و در نتیجه، احتمال موقتی حملات مهندسی اجتماعی کاهش می‌یابد.

آگاه باشید چه چیزی را  
منتشر می‌کنید

مهمنترین منبع اطلاعاتی مهاجمان در حملات مهندسی اجتماعی، مطلبی است که در مورد افراد در متابعی نظری اینترنت قرار دارد و به سادگی قابل دسترس است؛ بهویژه اطلاعاتی که خود فرد در شبکه‌های اجتماعی منتشر می‌کند. در صورتی که افراد با مطلب شخصی خود آگاهانه رفتار کرده و آنها را در معرض دید عموم قرار ندهند، امکان استفاده از این اطلاعات در حملات مهندسی اجتماعی نیز کاهش خواهد یافت.

آموزش مهمترین  
اصل است

ساده‌ترین و کارآمدترین راه کار برای مقابله با حملات مهندسی اجتماعی، آموزش افراد و افزایش آگاهی آن‌ها است. در صورتی که نکته افراد، آگاهی کافی نسبت به محیط خود داشته باشند، در لحظات حساس به درستی و بر اساس اصول تصمیم‌گیری کنند و فریب وسوسه‌های مهاجمان را نخورند. دیگر هیچ حمله مهندسی اجتماعی موافقی نداشته باشد!