

## عنوان مقاله:

مهندسی اجتماعی؛ تهدید نرم علیه امنیت اطلاعات شخصی و حرفه ای: تعریف جامع و مدل بنیادی حملات مهندسی اجتماعی

## محل انتشار:

دومین کنفرانس حوادث و آسیب پذیری های امنیت فضای تبادل اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 6

## نویسندگان:

محسن قاسمی - کارشناس ارشد امنیت اطلاعات، دانشگاه تهران، تهران، ایران

محمد سادات - کارشناس نرم افزار، دانشگاه خیام مشهد، مشهد، ایران

## خلاصه مقاله:

امنیت یک کار پاره وقت و پروژه‌هایی نیست؛ بلکه باید در همه حال امنیت در نظر گرفته شود. در حال حاضر مهندسی اجتماعی بزرگترین تهدید علیه امنیت اطلاعات است؛ زیرا پایه های انسانی امنیت را هدف قرار میدهد. پزشکان، روانشناسان و درمانشناسان اغلب از عناصری استفاده میکنند که تکنیکهای مهندسی اجتماعی است؛ تا بیماران خود را درمان نمایند. مهندسی اجتماعی از مهندسی اجتماعی برای ضرر زدن به یک فرد یا سازمان استفاده میکند. با وجود اینکه هدف این دو از استفاده تکنیکهای مهندسی اجتماعی متفاوت است؛ اما شیوه کارشان خیلی شبیه هم است. راحتترین راه مقابله با حملات مهندسی اجتماعی، محافظت در برابر این حملات، کاهش اثرات حملات و توقف آنها، آگاهی است و این مقاله دانش خوانندگان خود را دربارهی بزرگترین ضعف در یک سیستم امنیتی که همان عنصر انسانی است توسعه میدهد. تعریف جامع و کامل مهندسی اجتماعی؛ به گونهایی که نقایص تعریفهای قبلی را برطرف میکند، در این مقاله ارائه میشود. مطلب جدید دیگری که در این مقاله ارائه میگردد، نحوه پیادهسازی حملات مهندسی اجتماعی؛ که از آن به عنوان مدل حملات یاد میشود، به صورت کامل و بهینه شده است. مدل حملات مهندسی اجتماعی بیانگر عنصرهایی است که در یک حمله مهندسی اجتماعی استفاده میشوند. آشنایی با مدل حملات باعث آشنا شدن ذهن مردم با ساختار یک حمله مهندسی اجتماعی و آگاهی آنان خواهد شد.

## کلمات کلیدی:

مهندسی اجتماعی، امنیت اطلاعات، مدل حمله مهندسی اجتماعی، چهارچوب حمله مهندسی اجتماعی، حریم خصوصی، عنصر انسانی

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/691450>

