

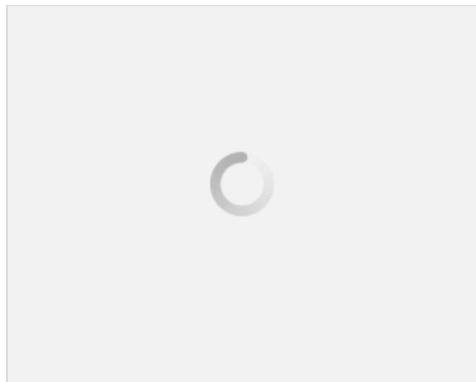
معرفی انواع حملات مهندسی اجتماعی مبتنی بر انسان (Human Based) (نسخه PDF)

در بخش پیش یاد گرفتیم که مهندسی اجتماعی مبتنی بر هنرهای فردی انسان در برقراری رابطه مستقیم چیست و فرآیندی را که مهاجم برای آن طی میکند، شامل چه قواعدی است. همانطور که گفته شد، مهندسی اجتماعی را میتوان به دو بخش تقسیم کرد: **روش مبتنی بر انسان (Human-based)** و **روش مبتنی بر کامپیوتر (Computer-based)**.

در قسمت پیش روش Human-Base گفته شد و در این بخش ادامه مطلب را با روش Computer-Base دنبال میکنیم. مهندسی اجتماعی بر پایه استفاده از کامپیوتر و ابزارهای مرتبط، به اتک هایی اتلاق میشود که با استفاده از نرم افزار کامپیوتری بتوانیم به اطلاعات مورد نظمان دست پیدا کنیم. این نوع اتک نیز خود دارای انواع مختلفی است که در ادامه به مهمترین آن ها اشاره میشود:

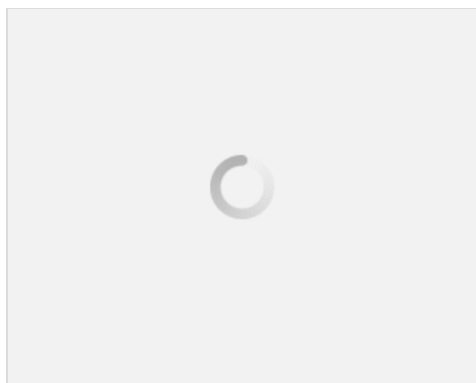
Pop-up windows

در واقع پنجره هایی که بصورت پاپ آپ باز میشوند، کاربران را به کلیک بر روی لینکی که داخلشان است فریب میدهند. این لینک معمولا کاربران به صفحه مورد نظر اتکر redirect میکند و آنجا از کاربران با عناوین مختلف خواسته میشود که اطلاعات شخصی خود را وارد کنند و یا انکه از آن صفحه نرم افزاری را دانلود کنند که به ان ها ویروس و یا تروجان بایند شده است.



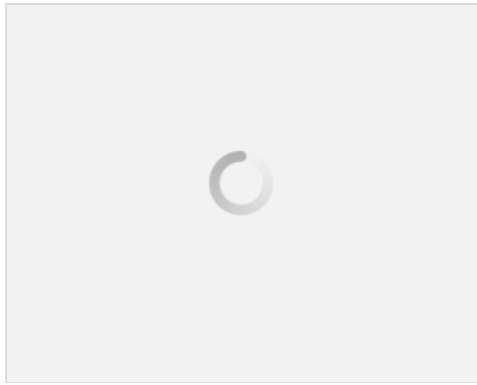
Insider attack (حمله داخلی)

طراحی و اجرای موفقیت آمیز این نوع حمله بصورتی است که باید از داخل شبکه ای که هدف در آن قرار دارد، صورت بپذیرد. در اغلب موارد، چنین حملاتی با هماهنگی و همکاری کارمندان ناراضی که از موقعیت شغلی خود راضی نیستند و یا انکه با کارمند دیگری و یا رئیس خود مشکل شخصی دارند، رخ میدهد.



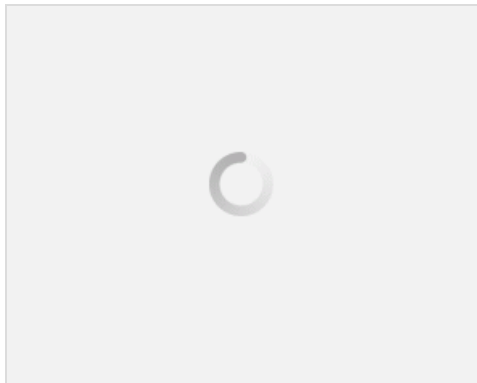
Phishing

اسپمرها (اشخاصی که هرزنامه میفرستند) معمولا ایمیلی را بصورت انبوه به گروه بزرگی از اکانت های ایمیل ارسال میکنند. مثلا در ایمیل خود ادعا میکنند که شما در لاتاری برنده شده اید و صاحب ۱ میلیون دلار هستید. در اعدامه از شما میخواهند که بر روی لینک داده شده کلیک کنید و و در صفحه مورد نظر مشخصات حساب بانکی و یا اطلاعات هویتی خود را وارد کنید. با استفاده از این روش، میتوانند اطلاعات هویتی شما و تعداد زیادی از اشخاص حقیقی را سرقت کنند.



کلاهبرداری به روش ۴۱۹ Nigerian

در روش کلاهبرداری نیجریه ای، اتکر با عناوین مختلف از قربانی میخواهد تا پولی را پرداخت کرده و یا با آن ها یک گردش مالی داشته باشد. به این خاطر به ان ۴۱۹ گفته میشود که "۹-۱-۴" بخشی از کد مجرمانه ای است که خلافکاران از آن برای انجام این عمل استفاده میکنند. اتکر ها معمولا ایمیل ها یا نامه هایی را برای اهداف خود ارسال میکنند که حاوی پیشنهاد هایی وسوسه کننده و سودآور است.



حمله مهندسی اجتماعی از طریق SMS جعلی

در این نوع حمله، اتکر به هدف خود SMS ای را ارسال کرده و ادعا میکند که این SMS از طرف بخش امنیت بانک است و هرچه زودتر با شماره مشخص شده باید تماس گرفته شود. اگر قربانی، شخص تکنیکالی نباشد، از طریق تماس تلفنی شخص مهاجم براحتی میتواند اطلاعات مورد نظر را از هدف بگیرد.

مانا باشید.

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

هرگونه نشر و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی می باشد.

AZARAKHSH

بسیار عالی و مفید

مطلب اصلی