ریاست جمهوری

سازمان مدیریت و برنامه ریزی

مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

مدرس: مهدی هدایت فر

جلسه اول

مفاهیم امنیت سایبری

جلسه دوم

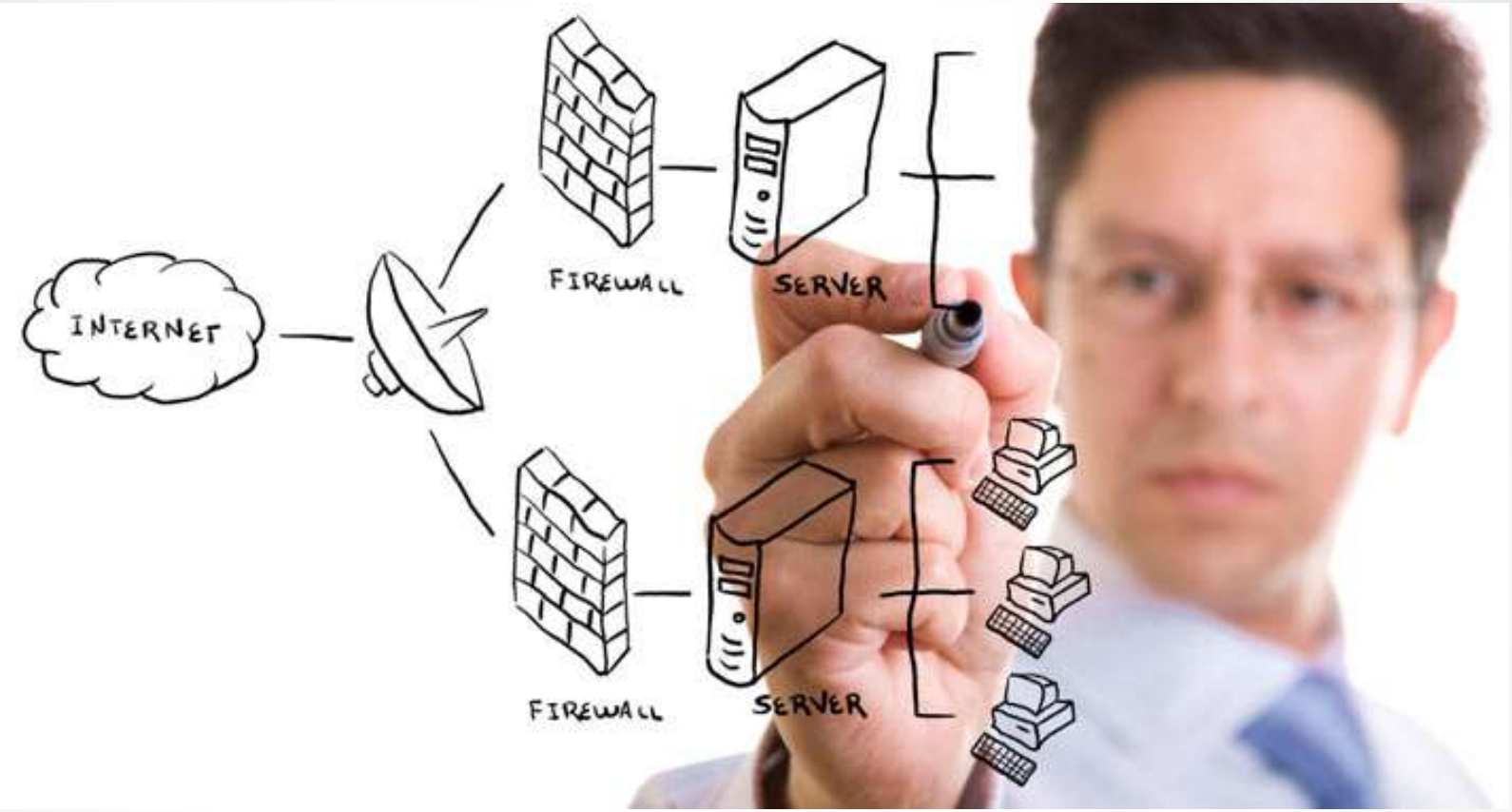
بهداشت سایبری و مفاهیم حقوقی

جلسه سوم

روشهای کنترل و مقابله

جلسه چهارم

نهادهای متولی و کار عملی



مفاهیم حقوقی امنیت فناوری اطلاعات

قانون جرایم رایانه ای

ریاست محترم جمهوری اسلامی ایران ،

عطف به نامه شماره ۲۱۹۵۳/۳۲۸۷۱ مورخ ۱۳/۴/۱۳۸۴ در اجراء اصل یکصد و بیست و سوم (۱۲۳) قانون اساسی جمهوری اسلامی ایران قانون جرائم رایانه-ای که با عنوان لایحه به مجلس شورای اسلامی تقدیم گردیده بود با تصویب در جلسه علنی روز سه-شنبه مورخ ۵/۳/۱۳۸۸ و تأیید شورای محترم نگهبان، به پیوست ابلاغ می-گردد.

رئیس مجلس شورای اسلامی ـ علی لاریجانی

10/4/1388

وزارت دادگستری

قانون جرایم رایانه-ای که در جلسه علنی روز سه-شنبه مورخ پنجم خرداد ماه یکهزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ ۲۰/۳/۱۳۸۸ به تأیید شورای نگهبان رسیده و طی نامه شماره ۱۶۳۰۶/۱۲۱ مورخ ۳/۴/۱۳۸۸ مجلس شورای اسلامی واصل گردیده است، به پیوست جهت اجرا ابلاغ می-گردد.

رئیس جمهور ـ محمود احمدی نژاد

قانون جرایم رایانه ای

بخش یکم ـ جرائم و مجازات ها

- فصل یکم ـ جرائم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی
  - مبحث یکم ـ دسترسی غیرمجاز
  - مبحث دوم– شنود غیر مجاز
  - مبحث سوم– جاسوسی رایانه ای
- فصل دوم ـ جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی
  - مبحث یکم ـ جعل رایانه ای
  - مبحث یکم–جعل رایانه ای
  - مبحث دوم– تخریب و احلال در داده ها یا سیستم های رایانه ای و مخابراتی
- فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه
- فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی
- فصل پنجم ـ هتک حیثیت و نشر اکاذیب
- فصل ششم ـ مسؤولیت کیفری اشخاص
- فصل هفتم ـ سایر جرائم
- فصل هشتم ـ تشدید مجازات ها

بخش دوم – آیین دادرسی

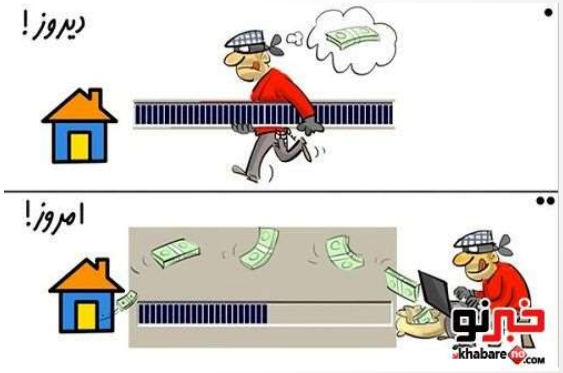
- فصل یکم– صلاحیت
- فصل دوم جمع آوری ادله الکترونیکی
  - مبحث اول– نگهداری داده ها
  - مبحث دوم ـ حفظ فوری داده های رایانه ای ذخیره شده
  - مبحث سوم ـ ارائه داده ها
  - مبحث چهارم ـ تفتیش و توقیف داده ها و سیستم های رایانه ای و مخابراتی
  - مبحث پنجم ـ شنود محتوای ارتباطات رایانه ای
- فصل سوم ـ استنادپذیری ادله الکترونیکی

بخش سوم ـ سایر مقررات

قانون جرایم رایانه ای

هزینه های رو به افزایش جرایم سایبری

توزیع جرایم رایانه ای				
دسترسی غیرمجاز به سیستم‌ها و داده‌های رایانه‌ای به شکل نفوذ به کارت‌های بانکی و ابزار الکترونیکی دراختیار مردم	هتك حیثیت افراد و نشر اکاذیب	کلاهبرداری های رایانه ای	تخریب داده های رایانه ای توسط مجرم	تکثیر غیر مجاز اطلاعات رایانه ای و سایر موارد
33 درصد از پرونده‌ها	30 درصد	16 درصد	6 درصد	10 درصد



قانون جرایم رایانه ای

قانون جرائم

فصل یکم: جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی

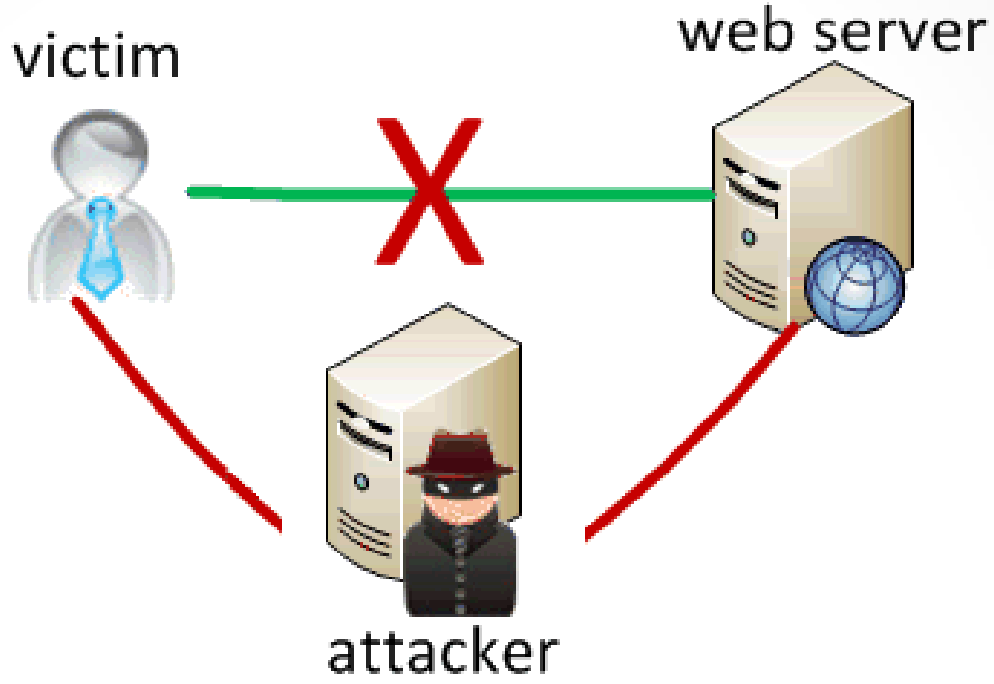
مبحث یکم: دسترسی غیرمجاز

مصداق قانونی جرم	ماده قانونی	جـــزا
بی احتیاطی/بی مبالاتی/عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده ها/حاملهای داده/سامانه های مذکور گردد.	**ماده ۵**	**حبس از ۹۱ روز تا ۲سال/ جزای نقدی از ۵میلیون تا ۴۰میلیون ریال/ هر دو +انفصال از خدمت از ۶ماه تا ۲ سال**

قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـــزا
دسترسی به سامانه های مخابراتی و رایانه ای محافظت شده	ماده ۱	حبس از ۹۱روز تا ۱سال/ جزای نقدی از ۵میلیون ریال تا ۲۰میلیون ریال/ هر دو
حدف یا مختل سازی یا تخریب داده های رایانه ای مخابراتی	ماده ۸	
مخفی کردن داده ها ، تغییر گذرواژه ها یا رمزنگاری داده ها مانع دسترسی اشخاص مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی	ماده ۱۰	
تولید/انتشار/توزیع/دردسترس قراردادن /معامله داده/ نرم افزار ها/ابزارهای الکترونیکی که صرفاً جهت ارتکاب جرائم رایانه کاربرد دارند	ماده ۲۵ بند الف	
فروش/انتشار/توزیع/دردسترس قراردادن گذر واژه/داده هایی که موجب دسترسی غیر مجار می گردد	ماده ۲۵ بند ب	
تولید/انتشار/توزیع/دردسترس قراردادن گذر واژه/داده هایی که موجب دسترسی غیر مجاز به داده ها یا سامانه های دیگران می گردد	ماده ۲۵ بند ج	

قانون جرایم رایانه ای



مصداق قانونی جرم	ماده قانونی	جـزا
دسترسی به داده های سری /تحصیل/شنود محتوی در حال انتقال/ذخیره شده در سامانه های رایانه ای/مخابراتی	**ماده ۳ بند الف**	**حبس از ۱تا ۳سال/ جزای نقدی از ۲۰میلیون تا ۶۰میلیون ریال/هر دو**

قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـــزا
مدیر شخص حقوقی مرتکب جرم رایانه ای گردد	ماده ۱۹ بند الف	شخص حقوقی مسئولیت کیفری دارد (مسئولیت شخص حقوقی مانع مجازات مرتکب نخواهدبود)
مدیر شخص حقوقی دستور ارتکاب جرم را دهد و جرم به وقوع به پیوندد	ماده ۱۹ بند ب	
یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه ای گردد	ماده ۱۹ بند ج	
تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یابد	ماده ۱۹ بند د	

قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـــزا
کارمندان و کارکنان ادارات/سازمانها/شوراها/شهرداریها/موسسات/شرکتهای دولتی یا وابسته به دولت/نهادهای انقلابی/موسسات زیر نظر ولی فقیه/دیوان محاسبات/موسسات کمک گیرنده مستمر از دولت/دارندگان پایه قضایی/بط.ر کلی اعضا و کارکنان قوای سه گانه/نیروهای مسلح/ماموران به خدمت عمومی/رسمی/غیر رسمی به مناسبت انجام وظیفه مرتکب جرم رایانه ای شده باشند.	ماده ۲۶ بند الف	تشدید مجازات: محکوم به بیش از ⅔ حداکثر ۱ یا ۲ مجازات مقرر
متصدی/متصرف قانونی شبکه های رایانه ای/مخابراتی به مناسبت شغل خود مرتکب جرم گردد	ماده ۲۶بند ب	
داده ها/سامانه های رایانه ای/مخابراتی متعلق به دولت/نهادها . مراکز ارائه خدمات عمومی	ماده ۲۶بند ج	
جرم بصورت سازمان یافته ارتکاب یابد	ماده ۲۶ بند د	
جرم در سطح گسترده ای ارتکاب یابد	ماده ۲۶ بند ه	

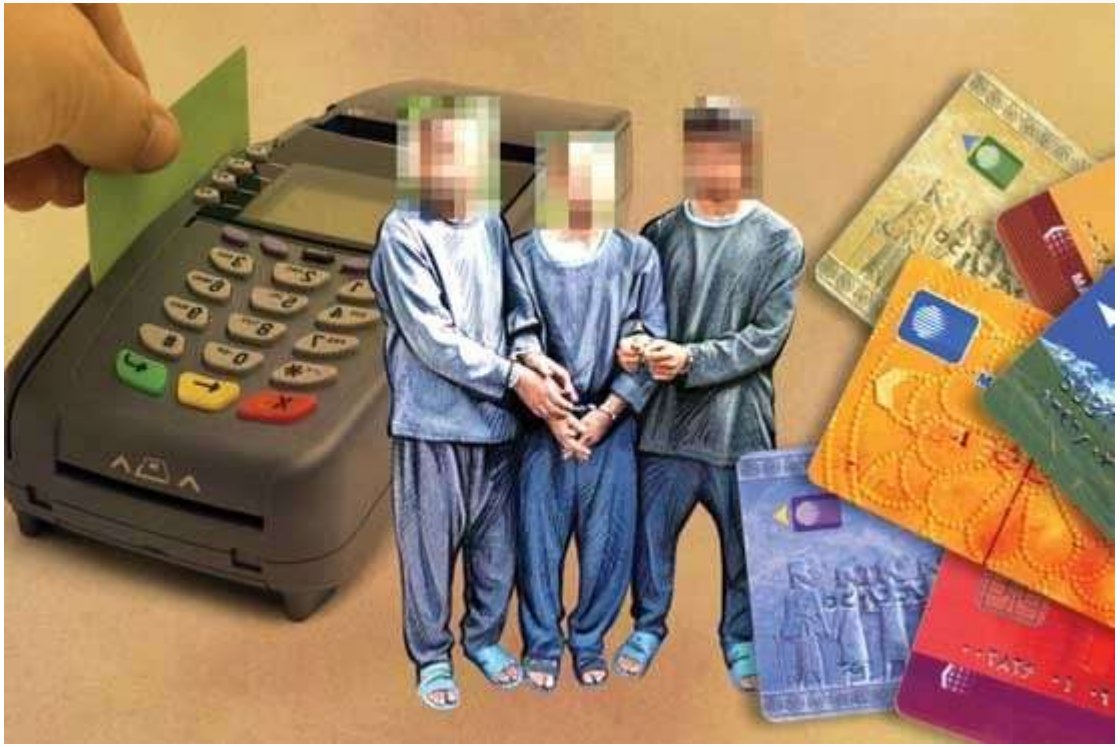
قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـــزا
تکرار جرم برای بیش از ۲ بار	**ماده ۲۷**	**محرومیت از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوریو بانکداری الکترونیکی**

قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـــزا
افشاء/دردسترس قراردادن داده ها برای دولت/سازمان/شرکت/گروه بیگانه/ عاملان آنها	**ماده ۳ بند ج**	**حبس از ۵ تا ۱۵سال**

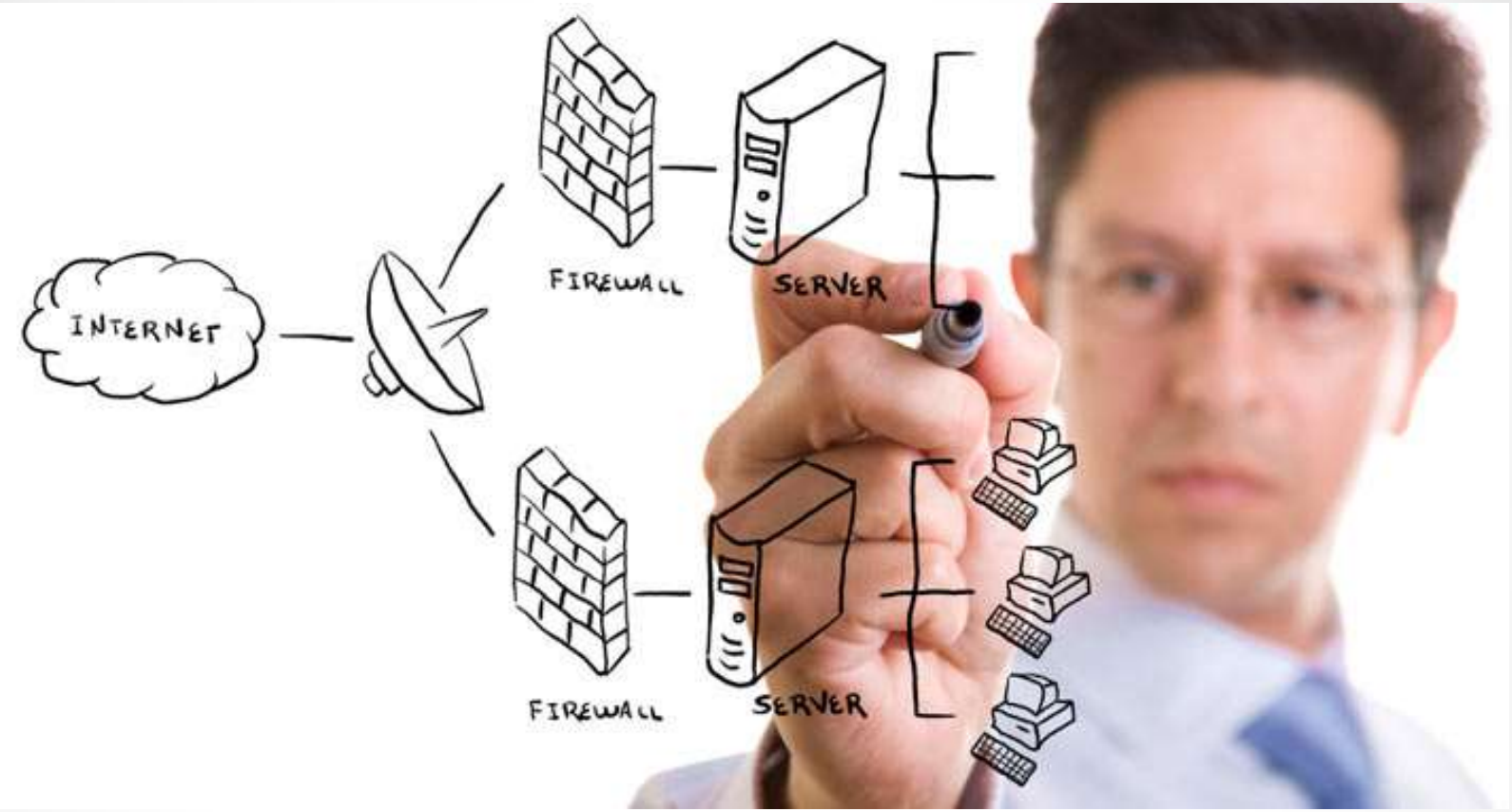
قانون جرایم رایانه ای



مصداق قانونی جرم	ماده قانونی	جـــزا
تغییر /ایجاد داده های قابل استناد/ایجاد یا وارد کردن متقلبانه داده به آنها	**ماده ۶بند الف**	**جاعل محسوب می گردد+ حبس از ۱تا ۵سال/ جزای نقدی از ۲۰میلیون تا ۱۰۰میلیون ریال/ هر دو**
تغییر داده/علائم موجود در کارتهای حافظه یا قابل پردازش /تراشه ها/ایجاد یا تغییر متقلبانه داده به آنها	**ماده ۶بند ب**	
با علم به مجعول بودن داده ها/کارتها/تراشه ها از آنها استفاده کند.	**ماده**	

قانون جرایم رایانه ای

مصداق قانونی جرم	ماده قانونی	جـزا
بدون مجوز از پهنای باند بین المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس	**ماده ۲۴**	**حبس از ۱تا ۳سال/ جزای نقدی از ۱۰۰میلیون تا ۱ میلیارد ریال/ هر دو**



مهندسی اجتماعی

مهندسی اجتماعی

مهندسی اجتماعی فریب کاران هنرمندی هستند که می خواهند شما را فریب دهند تا **اطلاعـات شخصی** یا **محرمانه ی** خود را در اختیار آن ها بگذارید. بیاموزید که چگونه ترفندهای مشترک مهندسین اجتماعی را شناسایی کنید تا به دام آن ها نیافتید.

- مهندسین اجتماعی با استفاده از غفلت انسان ها(عدم اطلاع)، ساده لوحی، تمایل به دوستی و تمایل آن ها به کمک به دیگران، طعمه های خود را انتخاب می کنند.
- در برابر ایمیل هایی که از شما اطلاعات صحیح شخصی یا محرمانه تان را سوال می کند، احتیاط کنید. اگر شک کردید، منبع ارسال را چک کنید.
- درباره ی آن چه به غریبه ها می گویید احتیاط کنید. ممکن است آن ها همان کسی نباشند.

فریب اطلاعـات آشکار را نخورید.

مهندسی اجتماعی

چرخه حملات مهندسی اجتماعی

تکنیک های مهندسی اجتماعی

تکنیک‌های مبتنی بر کامپیوتر

- پنجره‌های Pop-Up
- پیوست نامه‌های الکترونیکی
- هرزنامه‌های زنجیره‌ای و فریب‌آمیز
- وب‌گاه‌ها
- بازیابی و تجزیه و تحلیل ابزارهای مستعمل
- Phishing یا فیشینگ

تکنیک‌های مبتنی بر انسان

- رویکرد مستقیم
- جستجو در زباله‌ها
- جعل هویت
- سوءاستفاده از کاربران مهم
- کارکنان پشتیبان فنی
- کاربر درمانده
- Shoulder Surfing
- شایعه پراکنی
- جاسوسی و استراق سمع

تکنیک های مبتنی بر انسان

روانشناسی نفوذگران

احساسات و رفتارهای انسانی که اغلب نفوذگران از آن‌ها به عنوان بخشی از حملات مهندسی اجتماعی بهره می‌گیرند

ترس:

مسلماً ترس به عنوان یکی از قوی‌ترین محرک‌های ماست که بیشتر از همه‌ی دیگر احساس‌ها در حملات مهندسی اجتماعی مورد سوءاستفاده قرار می‌گیرد.

اطاعت:

از آنجا که ما از کودکی یاد گرفته‌ایم که به مقامات اعتماد کنیم، و تمایل داریم تا از دستورالعمل‌ها، درخواست‌ها و راهنمایی‌های آنان تبعیت کنیم. کلاهبرداران مهندسی اجتماعی اغلب به صورت مبدل از رایانامه، پیام کوتاه و یا حتی تماس تلفنی یا پست صوتی شخص یا گروه‌هایی نظیر مجریان قانونی یا مدیران اجرایی شرکت‌ها سوءاستفاده می‌کنند.

طمع:

به عنوانی تمایلی شدید و خودخواهانه برای رسیدن به ثروت یا قدرت و یا هر چیز دیگری تعریف شده است. معمولا بحث یک پاداش (معمولاً پاداش پولی) برای انجام یک کار مطرح است.

خیرخواهی:

به عنوانی تمایلی برای کمک به افراد دیگر تعریف شده است.

این حملات اغلب به بخش‌های پشتیبانی و خدمات صورت می‌گیرد، چرا که مهاجمان از تمایل این کارکنان برای درخواست‌های خود سوءاستفاده می‌کنند تا ادعا کنند که قصد شاد کردن افراد را داشته و آن‌ها را تشویق می‌کنند تا اطلاعات بیشتری از آنچه که باید را ارائه کنند.

تکنیک های مبتنی بر انسان (کلیه احساسات انسانی قابلیت سوء استفاده را دارند)

تخلیه تلفنی

دشمن همواره از طریق برقراری ارتباط تلفنی و استفاده از عناوین هویت جعلی بدنبال بدست آوردن اطلاعات مهم است. در ذیل به چند نمونه از این اطلاعات اشاره شده است.

تخلیه تلفنی

دشمن همواره از طریق برقراری ارتباط تلفنی و استفاده از **عناوین هویت جعلی** بدنبال بدست آوردن **اطلاعات مهم** است.

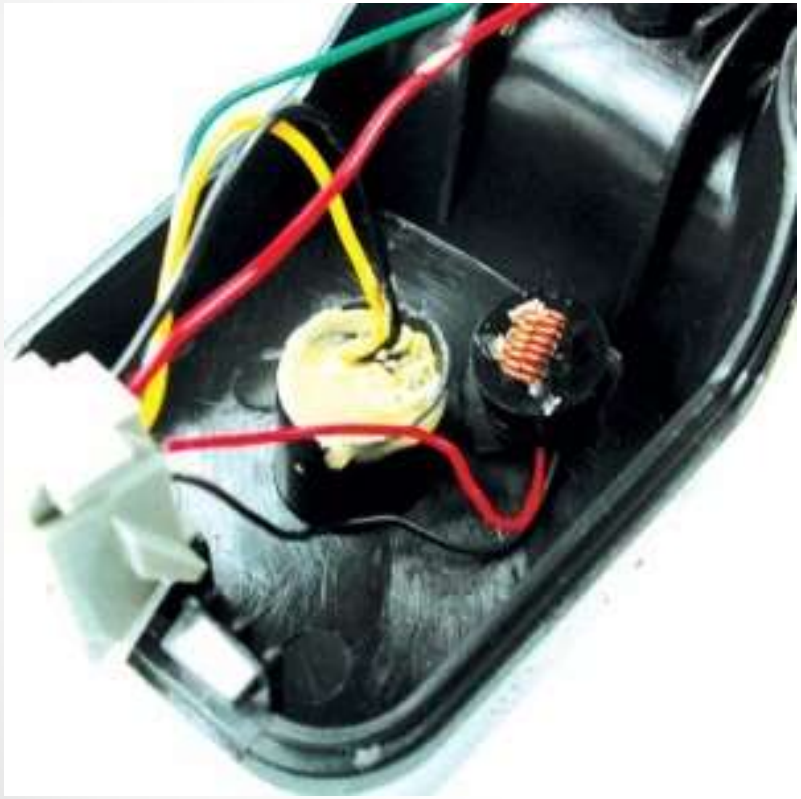
تخلیه تلفنی، عبارت است از **تلاشی آگا هانه** از طرف دشمن با **بهره‌گیری** از **غفلت** یا **فریب** عوامل **خودی**، به منظور **کسب اطلاعات** و **القای خواسته‌های** خود از طریق برقراری **ارتباط تلفنی.**

تخلیه تلفنی

شکل های تخلیه تلفنی:
اصولاً تخلیه تلفنی به دو شکل انجام می گیرد:

1) **کنترل تلفن ثابت یا تلفن همراه افراد با استفاده از وسائل و روش‌های مخصوص، که بیشتر جنبه ی جاسوسی و اطلاعاتی دارد**

2) **تماس تلفنی با اشخاص و گرفتن اطلاعات از آنها به شکل مستقیم**



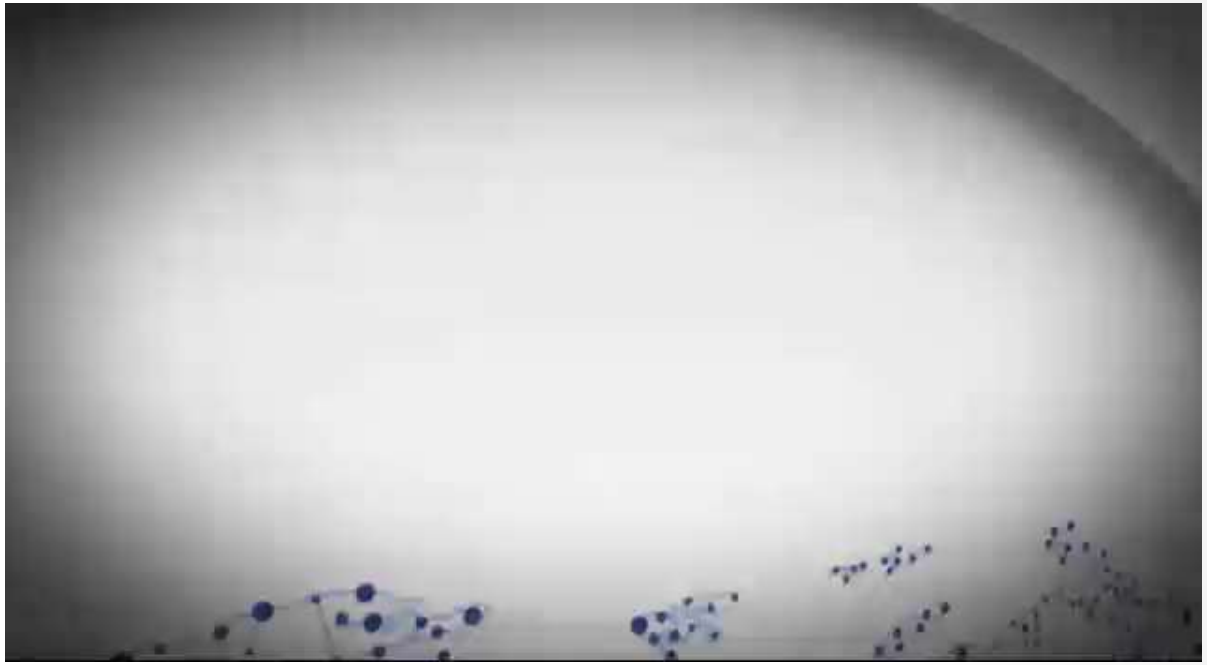
راه های مبارزه با تخلیه تلفنی و تلفن های مشکوک چیست؟ در مواجه با این موضوع چگونه رفتار کنیم؟

1. اساس جاسوسی تلفنی بر غفلت و فریب است، مواظب غفلت خود و فریبکاری دشمن باشید.
2. بهتر است صحبت کردن با تلفن را کم و کوتاه نمائید.
3. هنگام استفاده از تلفن به این موضوع بیندیشیم که نفر سومی در حال شنیدن مکالمه است.
4. همواره تلاش نمایید که مطالب مهم و دارای طبقه بندی حفاظتی را از طریق تلفن بازگو نکنید.
5. تا جای ممکن از پاسخ گویی تلفن به وسیله کودکان جلوگیری نمائیم.
6. آموزش‌های لازم به کودکان و اعضای خانواده داده شود تا به هیچ عنوان شماره تلفن یا آدرسی را به هنگام صحبت با تلفن بازگو نکنند.
7. از ارائه شماره تلفنهای غیر عمومی به افراد ناشناس خودداری کنید.
8. یکی از راه های پیشگیری از جاسوسی تلفنی، رعایت اصل حیطه بندی است، با رعایت این اصل، هرکس اطلاعاتی را در اختیار دارد، که در راستای وظایف شغلی خود به آن نیازمند است. پس تا شخصی را نشناخته ایم و اطمینان حاصل ننموده ایم، به هیچ سئوالی پاسخ ندهیم.
9. لازمه مقابله با عناصر جاسوسی تلفنی، بدخُلقی و تندگویی با تماس گیرندگان نیست، بلکه ضمن هوشیاری و دقت در پاسخ به سؤالات، میتوان اصول اخلاقی را نیز به طور کامل رعایت کرد.

راه های امنیتی جهت کنترل و کم کردن خطرات احتمالی سوءاستفاده از گوشی تلفن همراه:

1. از همه کد ها، رمز ها و قفل ها در مورد گوشی تلفن و سیمکارت استفاده شود.
2. از شماره گیری سریع استفاده نشود.
3. توصیه می شود از تلفن هایی با حافظه ی کمتر استفاده گردد. مانند گوشی های ساده و ارزان قیمت.
4. هیچ وقت با دکمه ستاره * و مربع # بازی نکنید. چرا که کنجکاوی مخاطب (سازمان های اشاره شده در بالا) را، از جهت اینکه احتمال ورود صاحب تلفن همراه به رمز یا کدی که جنبه سری و اطلاعتی وجود دارد، جلب خواهد نمود.
5. هر از چندگاهی سیم کارت را از گوشی جدا کنید و با یک فاصله زمانی مجدداً استفاده نمائید.
6. بهتر است شماره های مهم و حساس را در گوشی موبایل ذخیره نکنید و سایر شماره ها را به اسامی ای که خودتان متوجه می شوید ذخیره نمائید. دست کم از اسامی به جای نام فامیلی استفاده کنید.
7. سعی کنید تلفن همراهتان را به کسی جهت تماس قرض ندهید. در صورت الزام به این کار، خودتان شماره گیری نمائید. زیرا ممکن است آن شخص کدی روی گوشی شما وارد نماید که حساسیت بر روی شما در خصوص کنترل و مکان یابی شما افزایش یابد.
8. از گوشی های هدیه شده استفاده نکنید و قبل از هر کاری اقدام به تعویض آن نمائید.
9. بعد از گذشت مدت زمانی مشخص گوشی خود را تعویض نمائید.
10. همچنین از لحاظ پزشکی توصیه می شود در هنگام صحبت از گوش چپ استفاده نمائید و سعی نمائید گوشی را به صورت عمودی کنار گوش نگهدارید تا خطرات کمتری شما را تهدید نماید.

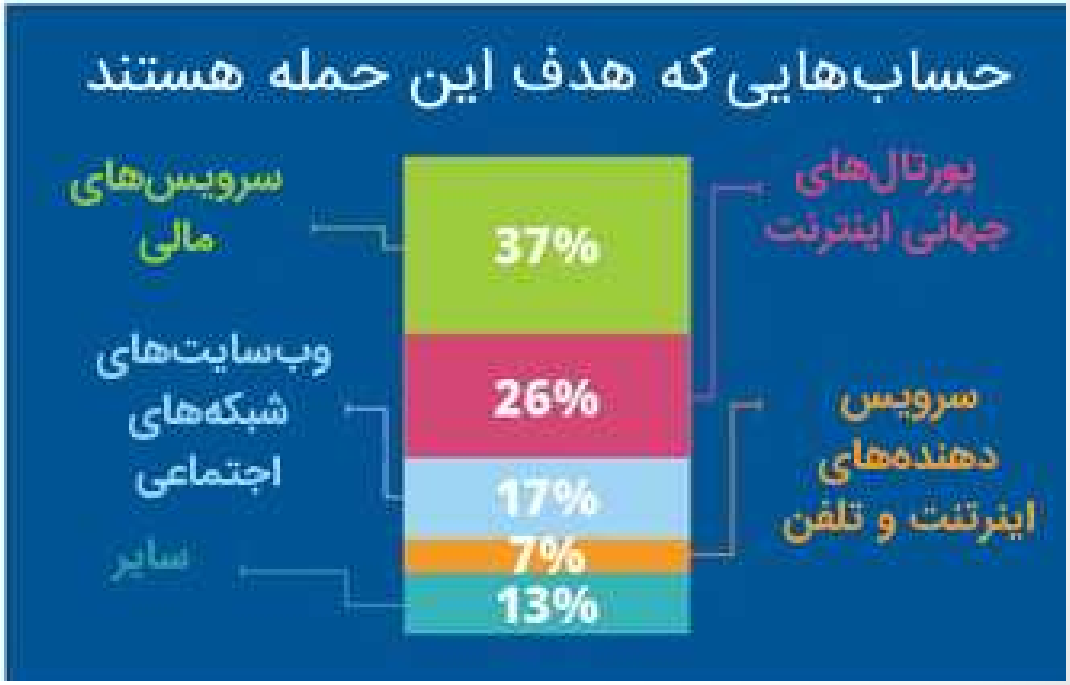
نمونه های حملات از طریق تلفن



انواع حمله های مهندسی اجتماعی

فیشینگ

ایمیل‌هایی که تظاهر می‌کنند از طرف دوست، همکار، موسسه و ... ارسال شده‌اند اما هدف آنها بدست آوردن اطلاعات کاربر است.

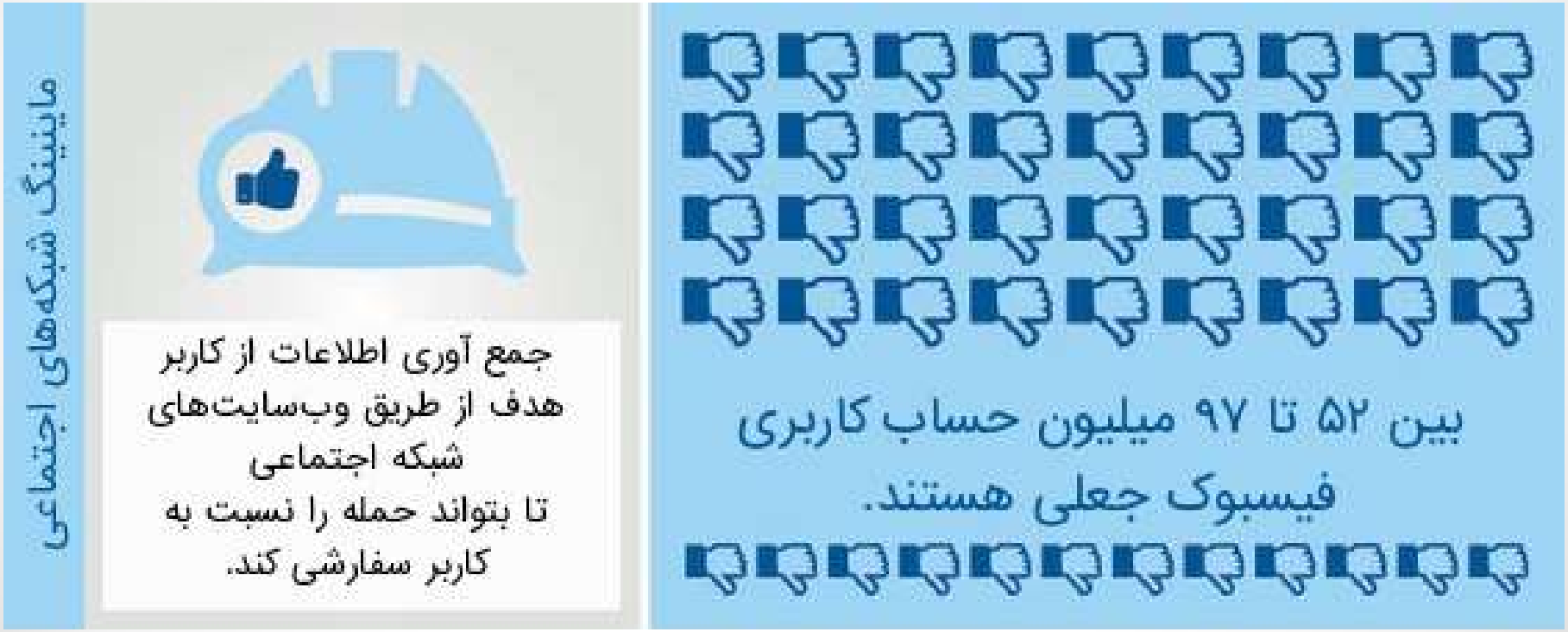


انواع حمله های مهندسی اجتماعی

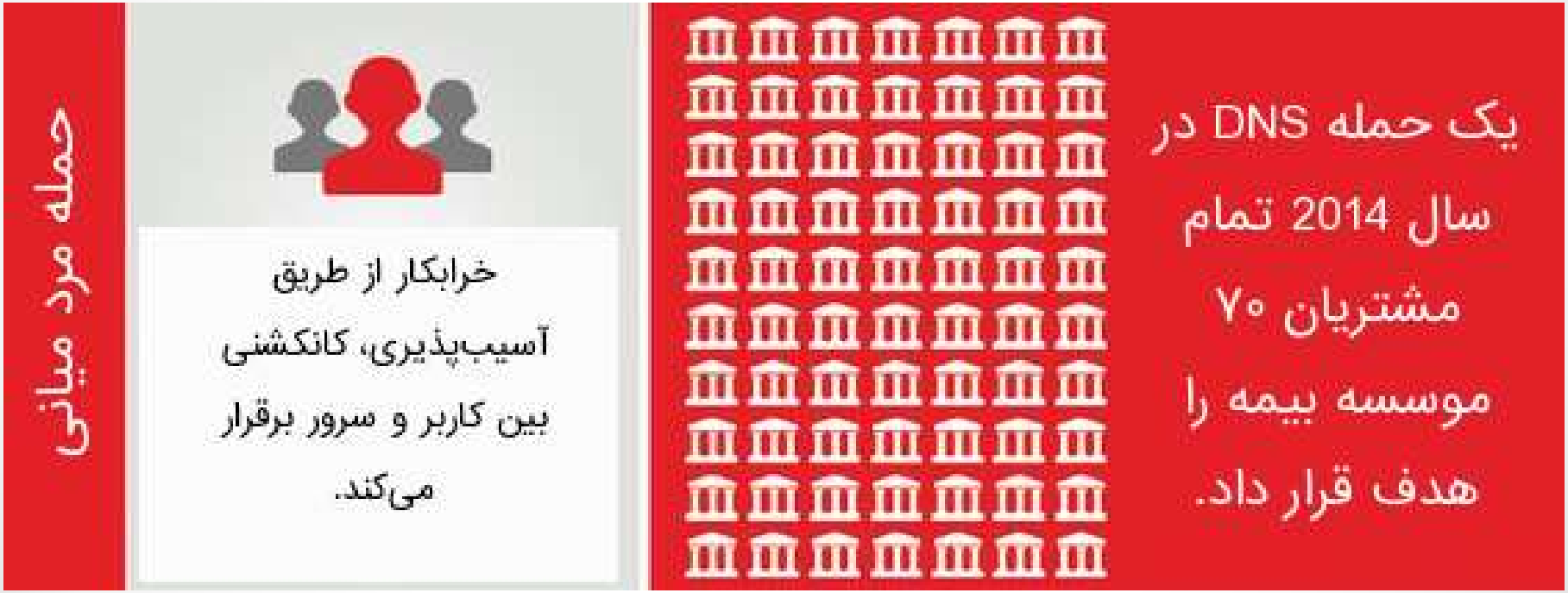
انواع حمله های مهندسی اجتماعی

انواع حمله های مهندسی اجتماعی

انواع حمله های مهندسی اجتماعی

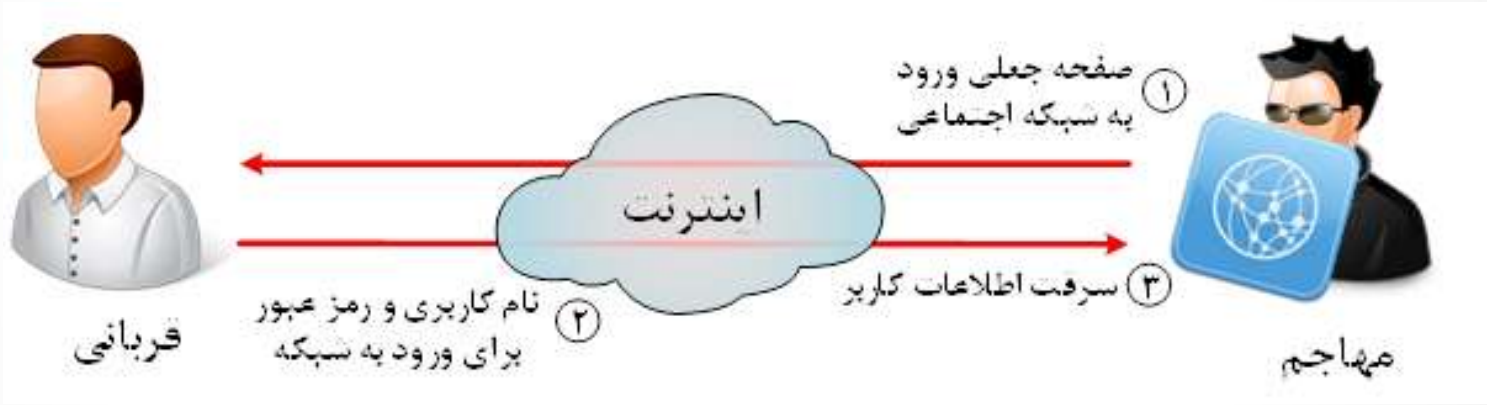


انواع حمله های مهندسی اجتماعی



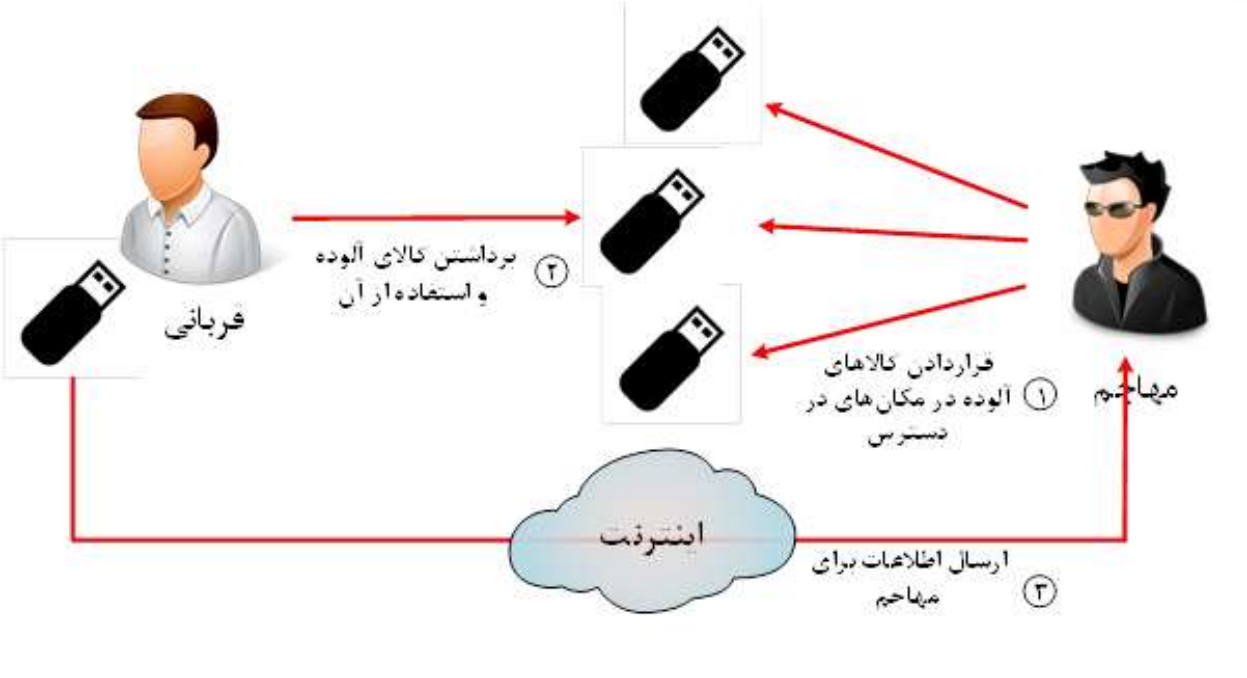
انواع حمله های مهندسی اجتماعی

مهندسی اجتماعی
روش صیادی(Phishing)

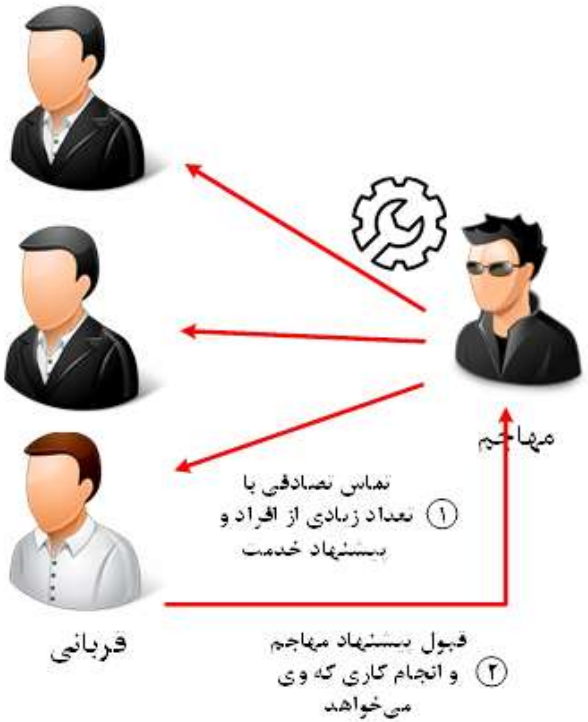


مهندسی اجتماعی
روش دستاویزسازی (Pretexting)

مهندسی اجتماعی
روش طعمه گذاری (Baiting)



مهندسی اجتماعی
روش جبران کردن (Quid Pro Quo)



مهندسی اجتماعی
روش کول کردن (Piggybacking)