مهندسی اجتماعی

Social Engineering

نویسنده : پویا دانشمند

مقاله یا کتابچه پیش روی شما در آبان ماه سال ۸۷ توسط نویسنده محترم به رشته تحریر درآمده است اما بنابر دلایل بسیار که از ذکر آن معذورم در همان آبان ماه ۸۷ به لیست کارهای نیمه تمام نویسنده مذکور اضافه گشت و بدست فراموشی سپرده شد و زمان اکران عمومی آن به حال (مرداد ۹۲) موکول شد و در طی این سالها نیز نویسنده هیچ رغبتی برای کامل کردن آن از خود نشان نداد.

تمامی مطالب با همان نگارش سال ۸۷ و بدون هیچگونه ویرایش و بازبینی در مقاله گنجانده شده اند، با این تفاسیر اگر این مقاله را مورد مطالعه قرار دادید هرگونه مشکل نگارشی یا فنی را به بزرگی خود ببخشید.

قسمتی از نوشتار بخش زبان بدن مقاله از کتاب زبان بدنِ آلن پیرز با ترجمه سعید زنگنه الهام گرفته شده است.

تمامی اسامی ذکر شده در این مقاله مجازی و غیر حقیقی است

نگارشِ آبان ۸۷ - انتشار مرداد ۹۲

فهرست مطالب

سخنی با خواننده 3

مهندسی اجتماعی 4

مهندسی اجتماعی معکوس 15

منشا حملات 17

روان شناسی در حملات 18

زبان بدن 20

جعل هویت در مهندسی اجتماعی 28

مهندسی اجتماعی بر پایه اطلاعات فنی 30

نحوه دفاع در برابر مهندسی اجتماعی..... ۳۱

هیچ وصله برای حماقت انسان وجود ندارد[1]

[1] یکی از دانشمندان بنام گفته

مهندسی اجتماعی چیست

مهندسی اجتماعی به انواع و اقسام روش های گویند که در آن نفوذگر بدون استفاده از نرم افزار و یا سخت افزاری خاص و فقط به کمک بهره گیری از دو زبان[1] خود اقدام به بهره برداری از اشخاص مینماید ، این بهره برداری می تواند شامل دریافت اطلاعات ، کلمات عبور و یا هر نوع داده باشد .

در نفوذگری عام و معمولی شخص نفوذگر با استفاده از ابزاری مانند اسکنر ها ، سعی و خطا ، تروجان و اقسام دیگر روش های نفوذ اقدام به دستیابی به اطلاعات شخص یا شرکت مورد نظر می کند ، اما در روش مهندسی اجتماعی نفوذگر به جای جدل و جنگ با انواع دیواره آتش ، مانیتورینگ های مختلف و تمهیدات اندیشیده شده سخت افزاری و نرم افزاری به جنگ با افراد شبکه می رود. این نفوذ ممکن است با یک پیام الکترونیکی ، یک مکالمه ، یک برخورد اتفاقی و ... انجام شود .

یک مهندس اجتماعی خوب :

- از حس های طبیعی شما مانند : اعتماد ، ترس و یاری سوء استفاده می کند .
- با خلق شرایط و یا ورود ناگهانی به موقعیتی ، از آن وضعیت به بهترین شکل ممکن استفاده می کند .
- دارای اطلاعات کافی از شخص ، شرکت ، موقعیت زمانی و مکانی و کاری که درصدد انجام آن است باشد .
- خوب می بیند و خوب می شنود .

مهندسین اجتماعی به دو شاخه تقسیم می شوند :

- مهندسینی دارای اطلاعات فنی : این افراد با استفاده از حملاتی از طریق کامپیوتر ولی بر پایه مهندسی اجتماعی اقدام به نفوذ می کنند . به طور مثالی با ارسال یک ایمیل محرک شمارا وادار به کلیک رو لینکی خاص یا دانلود فایل مورد نظر خود می کنند .

- مهندسینی با نیرو و توان انسانی : این دسته از افراد با استفاده از تماس فیزیکی ، مکالمات و ... اقدام به برقراری ارتباط و سپس اعمال نقشه خود می کنند .

با یک مثال ساده شروع می کنیم :

سناریو 1 : دفتر کار منشی یک شرکت

منشی (با حالتی نالان) : نمیدونم چطور میشه با این نرم افزار جدول کشید !؟!

نفوذگر (ظاهرا یک ارباب رجوع) : ببخشید ، من به طور اتفاقی حرفتون رو با خودتون شنیدم ، حقیقتش من چند سالی با این نرم افزار کار کردم اگر اجازه بدید نگاهی بندازم شاید بتونم کمکی کنم .

منشی (لبخند زنان) : البته ! من که ازش چیزی سر در نمیارم .

البته مثال بالا دچار نقص و مشکل است ، معمولا منشی ها با شرایط خاص استخدام می شوند ولی خوب گاها" ممکن است منشی را با معیار های دیگری انتخاب کنیم .

زبان بدن : در قسمت های بعد به معرفی کامل این زبان و نحوه استفاده از آن خواهیم پرداخت ولی به طور خلاصه ، هر شخص در حین صحبت علائمی از خود بروز می دهد مثل : استفاده از دست ها ، پلک زدن ، خاراندن سر و ... این علائم را زبان بدن می نامند

همان طور که ما با زبانی که با آن تکلم می کنیم ، صحبت میکنیم با زبان بدن نیز صحبت میکنیم ، این زبان از آنجا مهم است که در بیشتر اوقاتی که شخص به دروغ یا فریب متوسل می شود فرد بیننده می تواند با ترجمه زبان بدن و از روی حرکات شخص مذکور به واقعی یا غیر واقعی بودن مطلب پی ببرد .

- در این مقاله جملاتی که در سناریوها و در داخل پرانتز () قرار می گیرند ، نشانه ی حالت فرد یا موقعیت مکانی می باشند .

---

1 : زبان تکلم ، زبان بدن

همان طور که در سناریو 1 دیدیم منشی شرکت به هیچ عنوان توجیه نشده است و به شخصی متفرقه اجازه استفاده از سیستم خود را می دهد .

در انتخاب افراد شبکه خود دقت کنید به افراد شبکه خود آموزش های اولیه را بدهید

در مثال بالا منشی بجای استفاده از یک شخص غریبه می توانست به یک کتابچه راهنما یا ساده تر از آن به اینترنت متوصل شود یا اگر شخصی به او پیشنهاد کمک و یاری می رساند ، منشی با صراحت از کلمه : نه ، خیر ممنونم و کلماتی با معنای رد درخواست آن شخص استفاده می کرد ، اغلب ما ایرانی ها از گفتن کلمه نه ! عاجز و در مانده ایم ، همین یک کلمه یکی از موثرترین راه ها برای مقابله با حملات مهندسی اجتماعی است .

باید توجه داشت که مهندسی اجتماعی شامل چهار مرحله است که هر مرحله به قبلی وابستگی شدید دارد و در صورت نیمه کار ماندن یکی از مراحل شما در ادامه راه با مشکل روبرو خواهید شد ، این مراحل عبارت اند از :

جمع آوری اطلاعات : بدست آورد اطلاعتی در مورد هدف مورد نظر ، این اطلاعات می تواند شامل اسم همسر ، شماره شناسنامه ، تعداد اولاد ، غذای مورد علاقه ، رنگ مورد علاقه و ... باشد . به طور کلی تمام سعی در این مرحله به این موضوع معطوف خواهد بود که اطلاعات دقیق و کاملی از مورد جمع آوری کنید.

برقراری ارتباط: برای برقراری اعتماد و دوستی باید راهی برای ارتباط یافت ، این راه می تواند یک پنچری ماشین ، تنه ناخود آگاه برای واژگونی محتویاتی که در دست شخص قرار دارد یا حتی گفتن جمله چه روز خوبی باشد !

بهره کشی: در این مرحله با جلب اعتماد از فرد کارهای مورد نظرمان را درخواست می کنیم .

اجرای نقشه و عمل : در مرحله آخر نیز کار به پایان رسیده و منتظر نتیجه خواهیم ماند.

(سناریو 1 به طور کلی یک سناریو اتفاقی و از پیش تعیین نشده است)

به سناریو زیر دقت کنید :

سناریو 2 : آقای محمدی هر چه سریع تر سوار تاکسی شده تا به محل کار خود مراجعت کند ، در میان راه متوجه می شود کیف پول خود را در منزل جا گذاشته است .

وقتی شخصی متوجه نبود کیف پول خود یا نبود هیچ پولی شود در اولین قدم سعی به گشتن محل های می کند که امکان وجود پول در آنها باشد ، در این حال اکثر مردم حالتی نیمه پریشان و درمانده پیدا می کنند .
شخص نفوذگر در این مثال در نقش یک ناجی ظاهر میشود، او با لحن صمیمانه ی به آقای محمدی می گوید که کرایه او را نیز پرداخت خواهد کرد . (از نفوذگر اصرار و از محمدی انکار)
در صورت رد چند باره نفوذگر نا امید نخواهد شد ، برای محمدی خاطره از نبود پول و سوار شدنش به ماشین می گوید و اینکه شخص دیگری خواهان حساب کرایه شد ولی او قبول نکرد و در آخر با ناراحتی به خاطر جر و بحث با راننده تاکسی از آن پیاده شد و در همین حال به راننده همان تاکسی نیز حق می دهد .
در این شرایط محمدی در موقعیتی قرار می گیرد که اجتناب ناپذیر است و به احتمال قوی قبول خواهد کرد .

محمدی در جلوی شرکت پیاده می شود و تشکر کنان در ماشین را بسته و به درون شرکت می رود ، نفوذگر اندکی جلوتر پیاده می شود ، به بهانه وارد شرکت شده و اتاق محمدی را پیدا می کند با حالتی سراسیمه و دستپاچه وارد اتاق می شود ، محمدی از دیدن نفوذگر خوشحال خواهد شد و او را دعوت به صرف چای می کند (ممکن است برخورد به شکل دیگری انجام شود ، در اینجا یک برخورد رویایی را می بینیم !)
نفوذگر با تشکر می گوید که دسترسی به اینترنت ندارد و همین حالا باید برگه ثبت نامی را پر کرده و باید از طریق اینترنت ثبت نام را انجام دهد ، عاجزانه درخواست این را دارد که چند دقیقه اجازه استفاده از اینترنت را به او بدهد و ...

توجه کنید که هر چقدر سمت شخص پایین تر باشد اعتماد افزایش پیدا خواهد کرد .

مثال بالا یک نوع مثال فراگیر و عمومی و البته پر کاربرد است ، در مثال بالا حس جبران کاری ، هر چند کوچک در شخص هدف بر انگیخته می شود . (سناریو بالا شامل محرک روان شناسی معامله متقابل است)

اغلب افرادگمان می کنند که هیچوقت قربانیان اینگونه حملات نخواهند بود

در ادامه به بررسی حلمه بدون حضور فیزیکی می پردازیم :

سناریو 3 : تماس با یکی از افراد شبکه (نادری پور یکی از مسئولین واقعی شرکت است ، لحن صحبت و تن صدا کاملا شبیه شخص حقیقی است ، دستگاه های برای تغییر صدا در بازار وجود دارند)

نفوذگر : سلام خانم طاهری ، نادری پور هستم .
منشی: سلام ، خوبین آقای نادری پور ؟
نفوذگر : بله ، مرسی ممنون ، زیاد مزاحمتون نمیشم میدونم سرتون خیلی شلوغه فقط اگه میشه برید تو دفتر کارم کامپیوتر من رو روشن کنید و مراحلی رو که میگم دنبال کنید .
منشی : چشم حتما" ، یه چند لحظه گوشی دستتون باشه .

چطور بعضی از افراد به صدای هر چند شبیه صدای رئیس خود اعتماد می کنند ؟
یکی از راههای مقابله با این مشکل قرار دادن یکی کلمه عبور برای رایانه است .

در مثال بعدی با داشتن نام کاربری اقدام به کشف کلمه عبور می کنیم :

سناریو 4 : فردی با دیدن یوزر کاربری اینترنت یکی از افراد شرکت سعی در بدست آوردن پسورد دارد

نفوذگر : سلام ، واحد پشتیبانی ؟
پشتیبانی : بله ، بفرمایید امرتون
نفوذگر : من از صبحه که نتونستم وارد شبکه بشم ، حقیقتش کلمه عبورم رو اشتباها از حالت ذخیره در آوردم و حالا هر چی سعی میکنم یادم نمیاد ، ممنون میشم کمکم کنید ؟
پشتیبانی :اما ما نمی تو ..... (نفوذگر با فهمیدن امتناع شخص اقدام به قطع کردن صحبت مسئول واحد می کند)
نفوذگر :البته می دونم شاید با قوانین مشکلی داشته باشه ولی من باید یه گزارش رو از اینترنت دریافت کنم و پرینت بگیرم و تا 15 دقیقه دیگه به رئیس و مسئولم برسونم ، ممنون میشم اگه بهم کمک کنید ، تازه 1 ماهه کارم رو اینجا شروع کردم نمیخوام همین اول راهی رئیسم رو نا امید کنم ، می ترسم از اینکه دیدش نسبت به من عوض بشه .
پشتیبانی : خوب البته درک میکنم ، شماره کاربریتون رو بدید ؟
نفوذگر : 190023
پشتیبانی : کلمه عبور شما 12345600 است ، جایی یادداشتش کنید که دیگه به مشکل برنخورید.
نفوذگر : یک دنیا ممنونم ازتون ، بتونم جبران کنم .

اگر در سناریو بالا شخص تماس گیرنده خانم باشد و اندکی به لحن خود تمنا و خواهش بیشتری اضافه کند این مراحل چندین برابر سریع تر نسبت به قبل انجام خواهند شد ! (محرک روانشانسی در این سناریو بر انگیختن حس همیاری است)
مسئول قسمت پشتیبانی باید بر طبق وظیفه خود از دادن کلمه عبور خودداری می کرد و طبق ضوابط از شخص می خواست که به دفتر پشتیبانی مراجعه و کلمه عبور را دریافت کند (این دریافت می تواند بر حسب شناخت یا توسط نامه انجام گیرد)

اگر شرکت شما قانونمند است و چیزی به نام نظم و ترتیب در آن وجود دارد! پس همه موظف به پیروی از قانون هستند از پایین ترین فرد از نظر درجه در شرکت تا خود شما و مدیران اجرایی دیگر .

دو نکته بسیار مهم برای خنثی سازی این نوع از حملات :

در صورتی که کار شما مطابق با قوانین است از هیچکس نترسید ، حتی اگر آن فرد رئیس شما باشد

از پشت تلفن به هیچکس اعتماد نکنید حتی اگر آن فرد پدر شما باشد !

مثالی دیگر از این نوع حملات

سناریو 5 : در این قسمت نفوذگر خود را به جای رئیس یک بخش قرار می دهد *نفوذگر : سلام ، قسمت پشتیبانی شرکت ؟* *پشتیبانی : بله ، ظهرتون بخیر ، چه کمکی از دستم بر میآد ؟* *نفوذگر : بنده فاتحی هستم مدیرفروش شرکت از چند ساعت قبل ارتباطم با قسمت بایگانی شرکت قطع شده و همین الان نیازمند دریافت یک لیست از محصولات و تعدادی از اوراق هستم ، لطف کنید نام کاربری و یک کلمه عبور به من بدهید تا به سیستم وصل شوم .* *پشتیبانی :اما قربان این خلاف قوانین است .* *نفوذگر (لحنی تحدید آمیز) : ببینید من فورا به این مدارک احتیاج دارم ، همین الان مشتری ها در دفتر من هستند ، در صورتی که این مطالب به دست من نرسد این کوتاهی از طرف شخص شما بوده و مسئولیت و عواقب این کار هم به عهده خود شماست .* *پشتیبانی : پس من یک نام کاربری و کلمه عبور برای شما ایجاد می کنم ولی بعد از دریافت اطلاعات در صورتی که خواستار استفاده از اکانت هستید باید نامه از دفتر کل بیاورید .*

سناریو بالا نمونه بارز استفاده از یک نوع محرک روان شناسی (قدرت) است .
نفوذگر ، کارمند بخش پشتیبانی را با تهدید غیر مستقیم به رساندن ضرر و زیان به شرکت و همین طور عواقب آن می ترساند کارمند بر خلاف میل باطنی خود اقدام به ساخت اکانت می کند ، یکی از مهمترین دلایل آن نوع معرفی نفوذگر بوده است .

تا اینجا به معرفی عوامل تحریک پذیری چون : معامله متقابل ، اعمال زور و قدرت و بر انگیختن احساست درونی شخص پرداختیم در ادامه چند محرک روانشناسی دیگر را بررسی خواهیم کرد .

محرک هماهنگی یا یکپارچگی نیز یکی دیگر از محرک های مهم است ، در این نوع از حملات نفوذگر سعی می کند با قبولاندن این موضوع که بقیه افراد کار مورد نظر را انجام داده اند ، فرد را مجبور به انجام کار کنند .

سناریو 6 : تماس با هدف و متقاعد سازی از طریق یکپارچگی

نفوذگر : سلام ، کریمی پور از بخش پشتیبانی شبکه هستم .
کارمند : سلام ، بخش پشتیبانی شبکه ؟
نفوذگر : بله ، ما چند روزیست که کارمون رو شروع کردیم ، وظیفه این بخش اینه که با آزمون های مختلف و چکاب ها فنی مشکلات هر بخش رو بهشون گزارش کنیم ، تا الان هم چیزی حدود سیصد نفر از کارمندان رو مورد ارزیابی قرار دادیم ، که البته نتایج واقعا عالی هستند .
کارمند (سیصد نفر از کارمندان ! چرا من یکی از این آنها نباشم ؟) :اوه ، بله حتما ، برای ارزیابی چه مراحلی رو باید طی کنم ؟
نفوذگر : لازم به کار خاصی از طرف شما نیست ، ما در ابتدا با دریافت نام کاربری و کلمه عبور شما ، شروع می کنیم ، بقیه مراحل از طریق فرم های که تا چند ساعت دیگر در قسمت شما پخش خواهند شد پیگیری می شود .
کارمند : خوب نام کاربری من 902311 و کلمه عبورم هم 09123456است .
نفوذگر : ممنون و روز خوبی داشته باشید .

در سناریو بالا نفوذگر با گفتن اینکه بسیاری از کارمندان در این آزمون شرکت کرده اند و از آن سربلند بیرون آمده اند سعی به تحریک و ترغیب کارمند دارد .

حال به سناریو 7 توجه کنید :

سناریو 7 : در این سناریو شخص نفوذگر با اعمال زور و به طور مستقیم کلمه عبور را دریافت می کند

نفوذگر (جملات تند و خشن بیان می شوند) : سلام کافی نت سیب ؟
کارمند : بله ، بفرمایید
نفوذگر(جملات اندکی آرام تر بیان می شوند) : خانم این چه وضعشه ؟
کارمند : چی ؟ چه وضعشه ؟
نفوذگر : من دیشب از شما یک کارت اینترنت گرفتم و حالا عدد های پسوردش خونده نمی شه !
- در ادامه کارمند مسئول یا به شما کمک خواهد کرد که پسورد را بازیابی کنید یا ...
کارمند : خوب مشکلی نداره ، اگر امکانش رو دارید تشریف بیارید اینجا تا کارت رو براتون عوض کنیم
نفوذگر (لحنی بسیار خشن و نه تهدید آمیز) : تشریف بیارم اونجا که چی بشه ؟ من الان ثبت نام دارم تا الانش هم کلی دیر شده ، واقعا وضعی داریم ما ها ! این همه سال مشتری بودیم هیچ موردی نبود ، حالا که نوبت ثبت نام این رسیده ببین چی شده
- در صورتی که کارمند باز هم امتناع کند :
نفوذگر () : بابا الان واجدین شرایطش پر میشه ! من تا بیام اونجا کلی زمان میبره بخدا این وسط هزار و یک نفر جلو می افتن از من .

در سناریو 7 نفوذگر با اعمال پیاپی زور و خشونت و خواهش و عجز کارمند بخش را کلافه می کند و علاوه بر آن حس مسئولیت پذیری او را نیز بر می انگیزد .

کمک رسانی هدفمند یکی دیگر از راه های نفوذ به سازمان است به طور مثال :

سناریو 8 : کمک به یکی از کارمندان و نفوذ به اداره یا سازمان
کارمند (با دستی پر از پرونده و کیف و .. ناگهان به طور اتفاقی لیز خورده تمام پرونده ها پخش می شوند)
نفوذگر (دوان دوان به سمت کارمند می آید به او کمک کرده پرونده ها را جمع کرده و درخواست کمک به وی را می نمایید)
نفوذگر (خنده ملیح) :اوه این همه پرونده و کاغذ و پوشه و ... ! معلومه که سرتون حسابی شلوغه !
کارمند (با لبخند) : بله ، واقعا کار زیاده
نفوذگر :اجازه بدید کمکتون کنم و تا دفترتون اینارو بیارم
کارمند :زحمت میشه ، ممنون ، خودم ...
نفوذگر (ضمن نیمه کاره گذاشتن صحبت کارمند) : چه زحمتی !اجازه بدید کمکتون می کنم .
و در ادامه نفوذگر همراه با یکی از کارمندان وارد شرکت می شود !

در سناریو بالا نفوذگر بدون مصرف کالری اضافه و فقط با درخواست کمک به کارمند موفق به نفوذ به سازمان شد، در صورتی که کارمند زن باشد اوضاع به مراتب وخیم تر خواهد بود !
معمولا خانم ها از کمک های بدین شکل استقبال بیشتری می کنند تا مردان .

زنان در رویاء و دنیایی دگر سیر می کنند

شباهت یکی دیگر از عوامل روان شناسی است ، به طور کلی وقتی ما به مشکلی بر می خوریم به دنبال راه حل مشکل یا شخصی می گردیم که قبلا دچار آن مشکل شده باشد ، تا از او راه چاره بجوییم .
در این حمله نیز نفوذگر بین خود و شخص مربوط شباهت های ایجاد می کند تا بدین وسیله اعتماد شخص و همین طور همدردی و هم سطح بودن شخص را بر انگیزد .

سناریو 8 : فریب از طریق شباهت
مکان این صحبت می تواند هر جایی مانند پارک ، اتوبوس ، رستوران و ... باشد .
نفوذگر : می تونم اینجا بشینم ؟
کارمند :بله ، البته !
نفوذگر :عجب هوایی خنک و بهاری هست ! واقعا شش های آدم باز میشه !
کارمند (با لبخند) : بله ، حق با شماست
نفوذگر (به طور مستقیم به شخص نگاه می کند و در حالی که مثلا فکر میکند) :اووووم ! می تونم حدس بزنم که کار شما چیه ؟!

کارمند : فکر نمی کنم !
نفوذگر :اوه من یک غیب گوی خوب هستم ! سه تا حدس می زنم اگر اشتباه بود نوشیدنی مهمان من !
کارمند (با حالتی جذب شده به بحث) : قبوله !
نفوذگر : قصاب !
کارمند (خنده ی بلند !) :نه ! خیلی دورتر از چیزی که حدس می زنید هستم !
نفوذگر :اووووم ! خیلی دورتر .... ! یعنی مثلا کارمند !
کارمند : درسته ، ولی چطوری فهمیدید !
نفوذگر :گفتم که قدرت غیب گویی دارم !
کارمند : نه جدا"؟
نفوذگر : چون خود من هم یک کارمند هستم ! هم کیشان رو خوب میشناسم ! می تونم به جرات بگم از چند صد متری میتونم حدس بزنم !
کارمند (خنده) :اوه !
نفوذگر(در حال دست دادن) : حسین حسینی پور هستم .
کارمند (در حال دست دادن) : خوشوقتم ، کامران شهشایی .

این مکالمه سر درازی خواهد داشت ! نفوذگر از خوش مشربی و خوش صحبتی خود استفاده خواهد کرد تا در ادامه به اطلاعات بیشتری دست پیدا کند ، این مکالمه می توانست به شکل های دیگری نیز انجام شود ، به سناریو 9 توجه کنید

در سناریو 9 نفوذگر از تعداد فرزندان کارمند اطلاع دارد .
مکان و موقعیت : کارمند بچه های خود را به پارک آورده ، در حال تماشای بازی آنهاست .
نفوذگر (در حالی که کتابی به دست دارد) : سلام ، میتونم بشینم ؟
کارمند : چرا که نه .
نفوذگر (بعد از اندک زمانی) : بچه های شما هستند ؟
کارمند : بله ، چطور مگه ؟
نفوذگر :چقدر زود بزرگ میشن ! راستش من سه تا بچه دارم ، (با حالتی خندان) قرار بود با هم بیایم پارک ولی به خاطر کاری که کردن تنبه شدن و باید امروز رو تو خونه سر کنند !
کارمند :اوه ! مگه چند سالشونه ؟
نفوذگر :از بچه های شما بزرگ تر اند و البته کم عقل تر !
کارمند (با لبخند) :نه !این چه حرفیه ، بچه اند دیگه ، الان اذیت نکنند کی اذیت کنند !
نفوذگر :اذیت ؟ اذیت ماله یک لحظشونه !

این مکالمه نیز به درازا خواهد کشید ، نفوذگر از شباهت بین فرزندان استفاده کرده و صحبتی را آغاز می کند .
همیشه به یاد داشته باشید که در ابتدای کار درخواست خود را بیان نکنید ، همیشه با موضوعی نا مربوط شروع کنید تا به اصل قضیه برسید .

اگر شخص کم طاقت و بی صبری هستید ، همین حالا از خواندن مقاله دست بکشید !

هنر مهندسی اجتماعی در صبر و مقاومت ، اطمینان و اعتماد بنفس و آگاهی متبلور می شود

یک مهندسی اجتماعی همیشه به دنبال کلمات عبور و اطلاعات یک شبکه نیست ، در پاره از مواقع او بدنبال اطلاعت فردی شماست ، به سناریو زیر توجه کنید :

سناریو 10 : برقراری یک تماس تلفنی و دریافت اطلاعاتی با ارزش و سودمند

نفوذگر : سلام ، از بخش مسابقات شبکه دو صدا و سیما تماس میگیرم
فرد : سلام ، صدا و سیما ؟
نفوذگر (با شور و هیجان) : بله ! چرا که نه ! فکر نمی کردید شانس در خونه شما رو هم بزنه نه ؟! خوب بذارید براتون توضیح بدم ، گروه ورزش و سرگرمی شبکه دو سیما در حال تدارک یک مسابقه بزرگه ، امشب از بین تعداد زیادی از شماره ها به صورت اتفاقی شماره شما در اومد و حالا هم ما در خدمتتونیم که هماهنگی های لازم رو انجام بدین ، البته اگر مایل باشید ؟
فرد : بله بله ، البته ! خوب مسابقتون چجوریه ؟ باید چیکار کنم ؟
نفوذگر : خوب فردا شب قسمت اول این مسابقه برگزار میشه و شما احتمالا اولین نفر هستید ! توضیحات رو در حین برگزاری مسابقه می دیم بهتون ، اگه میشه خودتون رو معرفی کنید تا من یادداشت کنم مشخصاتتون رو ؟
فرد : من ، کاظم گرجستانی هستم ، سنم و اینارم بگم ؟
نفوذگر : بله البته ؟ شهرتون و آدرس منزلتون برای ارسال جایزه مسابقه ؟
فرد : هجده سال سن دارم ، از شهرستان ..... و آدرسمون هم .....

در سناریو شماره ده نفوذگر به راحتی موفق به کسب اطلاعات شد ، این اطلاعات می تواند در بر گیرنده شغل و ... هم باشد .

سناریو 11 : دریافت اطلاعات سیاسی و شخصی فرد

مکان : تاکسی
نفوذگر : عجب وضعیه ها ! این شهردار معلوم نیست داره چیکار میکنه ! هر دو متر به دو متر یا چاه کندن ! البته ظاهرش به پرتگاه بیشتر شباهت داره !
مسافر : حق با شماست از زمانی که شهردار کلاوندی از این شهر رفته و آقای یاوری نژاد اومده وضع بدتر شده که بهتر نشده !
...

در سناریو کوتاه بالا نفوذگر با بروز اندیشه های درست خود به شکل کوبنده و صریح ، باعث تحریک احساسات مسافر شد و مسافر نیز در ادامه با او هم مسیر و هم صحبت شد .

و حالا وقت زباله گرد شدن یک مهندسی اجتماعیست !
شاید در ابتدا این عمل به نظر شما به دور از آداب و نزاکت باشد ، لیکن این هم جزئی از مهندسی اجتماعیست .

اولین نمونه از این نوع حملات در سال 2000 بر سر زبان ها افتاد ، گفته می شود که شرکت اوراکل که یکی از سر سخت ترین دشمنان و رقبای تجاری مایکروسافت از افرادی را اجیر کرده بود تا در کاغذ های باطله ، سطل های زباله و ... به دنبال کد ها ، کلمات عبور ، دیسک های معدوم بگردند ، تا شاید بتوانند به هر نوع اطلاعاتی دست پیدا کنند .

اکثر روش های نامبرده شده بر روی شبکه های بزرگ قابل اجرا است و بر روی شبکه های کوچک چندان کارآمد نخواهد بود .

مهندسی اجتماعی معکوس

خوب در تمامی سناریو های بالا نفوذگر به سمت هدف خود می رفت ، اما در مهندسی اجتماعی معکوس همان طور که از اسمش پیداست این چرخه بر عکس می شود ، یعنی اینبار هدف مورد نظر به سراغ نفوذگر می آید .

این حملات شامل سه مرحله است :

- کارشکنی : در این مرحله نفوذگر با استفاده از روش های شبکه یا سیستم کامپیوتری را دچار مشکل و اختلال می کند .

- بازار یابی : حال نفوذگر در نقش یک فرشته نجات ظاهر شده و به موقع خود را معرفی می کند : این معرفی می تواند به شکل جا گذاشتن کارت شرکت ، آشنایی ساده و ... باشد .

- پشتیبانی : در مرحله آخر نفوذگر به حل مشکلات بوجود آمده توسط خودش می پردازد و نقشه و عملیات خود را پیش می برد .

توجه کنید که کارشکنی و بازار یابی از لحاظ زمانی فرقی با هم ندارند ، یعنی چندان مهم نخواهد بود که کدام یک از این مراحل اول انجام شود و کدام در درجه دوم .

سناریو زیر یک نمونه از مهندسی معکوس است .

سناریو 12 : نفوذ به سیستم دانشگاهی به روش مهندسی معکوس
عموما دانشجویان یک رشته و یک کلاس از هم آگاهی نسبتا کاملی دارند ، در مورد تخصص ها و موارد دیگر .
در این سناریو یکی از دانشجویان کلاس برای کمک رسانی به دفتر استاد می رود تا کارهای رایانه او را انجام دهد ، در این بین نفوذگر با بارگذاری فلش ممووری که دانشجو برای کارها استفاده می کند عمل و نقشه خود را آغاز میکند .

استاد (در کلاس درس) : از بچه ها کسی هست که به رایانه و اینجور چیزا وارد باشه ؟
عده از بچه ها : استاد زمانی کارش درسته و ...
استاد : نه غیر از آقای زمانی ؟
باز هم همان عده : جهان زاده هم کارش خوبه استاد
یکی دیگر از بچه ها : بله استاد ما تا حالا سه ، چهار تا سیستم براش بردیم راه انداخته .
استاد : آقای جهان زاده واردی به این مقولات ؟
جهان زاده (شخص حقیقی و نفوذگر) : بله استاد ، چطور مگه ؟
استاد : می خواستم بعد از کلاس یه سر بیای دفتر کارم این رایانه ما خراب شده از بس که دستیار ما (زمانی) باهاش ور رفته
نفوذگر : روی چشم استاد !

در سناریو بالا نفوذگر با استفاده از روش مهندسی اجتماعی معکوس در ابتدا اقدام به خراب کردن رایانه و سپس اقدام به تعمیر آن کرده است ، در این سناریو از نفوذگر رد پای نیز باقی نخواهد ماند ، همه کوتاهی ها از جانب استاد بوده است .

منشا" حملات

شاید یکی از مهمترین سوالات پیش آمده برای مدیران شبکه ها این باشد که چرا این حملات گریبانگیر و دامن گیر ما می شود ؟
در جواب باید گفت که هدف از اجرای این حملات یکی از دلایل زیر است :

- انتقام جویی
- کسب ثروت نا مشروع
- بدست آوردن اطلاعاتی مثل کد برنامه ها و ...
- ارضای حس کنجکاوی و غرور غلبه بر کارکنان شبکه (اغلب در جوانان و دانشجویان)

در اکثر موارد بالا این تهدیدات می تواند از طریق افراد داخلی و خارجی انجام شود .
حمله از داخل شرکت به مراتب خطرناک تر از حمله از بیرون شبکه است ، زیرا شخص متجاوز در ظاهر کارکنان شماست ولیکن که ستون پنجمی برای افراد خارجی باشد .

در اکثر موارد مهندسین اجتماعی به کارمندان ناراضی از ادارات و شرکت ها مراجعه می کنند .

روانشناسی در حملات

در تمامی سناریو های ذکر شده تا این قسمت از مقاله از محرک های روانشناسی متعددی استفاده شده است ، به طور کلی حملات مهندسی اجتماعی بدون استفاده از این محرک ها از درصد موفقیت کمی برخوردار خواهند بود .

همان طور که در ابتدای مقاله ذکر شد نفوذگر در این نوع از حملات از ترس و ترحم شما به نحو احسنت استفاده می کند ، پس لازم است ما با محرک های روانشناسی آشنا باشیم .

- اولین مورد بحث معامله متقابل است ، در این روش ما خود را نسبت به نفوذگر مدیون می بینیم مثل گاهی که شخصی برای تولد ما هدیه میآورد یا کمک میکند پنچری ماشین را بگیریم (این دو مثال خیلی از هم دور هستند اما هر دو دارای خاصیت معامله متقابل هستند) بعد از این عمل اگر شخص مورد نظر ما جایی ماشینش پنچر شود یا با مشکلی روبرو شود که از دست ما کمکی بر بیاید ما تمام توان خود را بکار میگیریم که کار او را جبران کنیم .

- محرک دوم ما قدرت و اعمال زور است ، طرز صحبت کردن شما با دوستان خود به شکلی خاص است و زمانی که با پدر و مادر خود صحبت می کنید به شکلی دیگر و در زمانی که با رئیس خود صحبت می کنید به شکلی دیگر است .
اگر رئیس شما از شما کاری را بخواهد به واسطه زور و قدرت او برایش آن کار را انجام خواهید داد ، ولی همان کار اگر توسط آبدارچی شرکت از شما خواسته شود ، شاید چندان مایل به انجام آن نباشید .

- محرک بعدی محرک کمیابی است ، این محرک در اکثر تبلیغات استفاده می شود ، کافیست به پیام های بازرگانی تلوزیون توجه کنید ، به کرات از این مطالب خواهید دید و شنید : آخرین مهلت ، تمدید شد ، محدود کردن تعداد (10 جایزه برای 10 نفر)
یک خرید استثنایی ، تعدادی واحد محدود آپارتمان و .... .
در این محرک اشخاص به علت محدود و کمیاب بودن جنس یا کالا جذب آن می شوند .

- محرک چهارم حس مسئولیت و وجدان اخلاقیست که یکی از پرکاربرد ترین محرک های روانشناسی است .
در این محرک شخص نفوذگر به گونه وانمود می کند که همه چیز به شما بستگی دارد ، شما در زندگی او نقش سرنوشت سازی دارید ، مسیر زندگی او توسط شما مشخص می شود ، نمونه های فراوانی از این نوع محرک توسط دانشجویان و خصوصا در پایان ترم تحصیلی استفاده می شود .
استاد فقط 1 نمره ، استاد اگه نمره ندید مشروط می شیم ، استاد یکی از اقوامون فوت کرده بود و ....

این نوع محرک کوچکترین تاثیری در اساتید مجرب ندارد ، گوش آنها از این سخنان پر است !

- شاید تا به حال نام کلمه Flood به گوشتان خورده باشد ، درست حدس زدید محرک بعدی سیلی از کلمات و جملات است که به صورت طوطی وار و پست سر هم بیان می شود ، این خیل عظیم از کلمات باعث طغیان شخص شنونده خواهد شد !

در این محرک شخص در ابتدا ، قضایا و موضوعاتی را بکار می برد که شخص موافق آنهاست و به طور زیرکانه در بین این جملات ، جملاتی که ممکن است شخص با آنها مخالف باشد قرار می دهد ، خواهید دید که شخص مقابل هیچ اعتراضی نخواهد کرد .

- زیبایی دوستی که دیگر از محرک های روانشناسی است ، جمله قدیمی عقل مردم به چشمشان است این محرک رو بطور تمام و کمال توضیح می دهد .
در این محرک شخص با ظاهر برازنده افکار و عقاید خویش را به افراد دیگر تلقین خواهد کرد .

- محرک بعدی هماهنگی و یکپارچگیست که در مقاله نیز به آن اشاره کردیم ، به طور کلی اکثر انسان ها دارای این محرک به شکل ذاتی هستند ، مصداق بارز این محرک گوسنفندانی هستند که بدنبال هم به راه می افتند ، اگر یکی از آنها از دره پرت شود بقیه نیز همراه او خواهند بود .
در این محرک کارمند یا شخص مورد نظر با دیدن اینکه اطرافیان او کاری اضافه انجام داده اند و شرایطی خاص دارند سعی می کند خود را نیز وارد دسته و گروه آنها کند ، از منزوی شدن می گریزد ، این انزوا ممکن است به هر شکل و شمایلی باشد .

- نقطه مشترک نیز یکی دیگر از محرک های روانشناسیت ، در این نوع از محرک ها نفوذگر می کوشد بین خود و شخص هدف نقاط مشابه پیدا کند ، اصطلاح ما درد هم رو بهتر می فهمیم ، بیانگر همین موضوع است .
مثلا شخصی که پایش شکسته یا ضرب دیده است سعی می کند از اشخاصی که این اتفاق برایشان افتاده راهنمایی بجوید و این یعنی آغاز یک دوستی جدید .

- روابیط فریبنده نیز یکی دیگر از محرک های مهم روان شناسی است و همه روزه کارایی این محرک را میبینیم و میشنویم که یکی از برجسته ترین نمونه ها کلیپ های صوتی به نام مزاحم تلفنیست ، در این محرک نفوذگر با یک تماس تلفنی و کش دادن صحبت ها و خوش و بش اقدام به جلب اعتماد شخص می نماید .
به طور مثال مدتی قبل برای بدست آوردن اطلاعاتی با منشی شرکتی تماس گرفتیم ، در این سناریو نقش ما یک ارباب رجوع است که حال می خواهد موجودی واریز شده توسط شرکت مذکور به حساب بانکی خود را بررسی کند ، بعد از حدود سی دقیقه صحبت ، خنده از لبان منشی مذکور دور نمی شد ! بعد از آن تنوانستیم با دادن نام و نام خانوادگی شخص مورد نظر به راحتی به اطلاعات مالی او دست پیدا کردیم ، در ادامه صحبت ها نیز موفق به دریافت شماره شناسنامه ، آدرس محل سکونت و ... گشتیم ، کل مکالمه چیزی نزدیک به چهل دقیقه طول کشید .
روابط فریبنده یکی از انواع مهندسی اجتماعیت که در صورت موفقیت آمیز بودن تنایج بسیار فوق العاده را در پیش دارد .

زبان بدن

بدن از بررسی تمام مقولات به یکی از موثر ترین زبان ها در مهندسی اجتماعی می پردازیم ، و این زبان چیزی جزء زبان بدن نیست ، در بخش قبلی توضیح دادیم که همان طور که تکلم می کنیم و منظور خود را انتقال می دهیم بدنمان نیز حرف می زند و اطلاعاتی را منتقل می کند .
نمونه این عمل را می توان در فروشندگان دید .
به طور مثال وقتی به بنگاهی مراجعه می کنید برای اجاره یا خرید مسکن اگر با این صحنه مواجه شوید چه فکر میکنید ؟
بعد از توضیحات مبلغ موجودی خود و ... بنگاهدار دست های خود را به هم میمالد ! و می گوید یک مورد مناسب برای شما سراغ دارم ! یا اینکه خیلی جالبه ، دقیقا موردی که می خواید رو سرغ دارم !
یا اگر بنگاهدار بعد از شنیدن صحبت های شما دست را زیر چانه گذاشته و چانه خود را بمالد ، ابروان خود را کج کند و دهن خود را به شکل حسرت آمیزی درآورد ، اشتباه نکنید ، او دلقک نیست !
این حرکات و علائم فقط برای رساندن مطلب به شکلی مطلوب تر و گیرا تر است ، بعد از انجام این حرکات او قادر به مانور بیشتر لفظی روی مورد است .

نمونه جالبتری از این عمل را می توان در مامورین نیروی انتظامی دید زمانی که شخصی را مشغول ور رفتن با در ماشینی می بینند ، خوب توجه کنید :

مامور : مشغول چه کاری هستید ؟
رباینده (در حالی که دستی به پس کله اش می کشد): بعد از اندکی مکث و من-من کردن می گوید که سوئیچش خراب شده و باید برای باز کردن در ماشین مقداری تلاش کند .

این شخص قطعا یک رباینده ماشین است !
فرض کنید سر جلسه امتحانی نشسته اید ، سوالی که پیش روی شماست سوالیست که شما دیشب چندین بار آن را خوانده اید ولی هر چقدر فکر می کنید جواب را به یاد نمی آورید ، به کدامیک از قسمت های سر خود ضربه می زنید ، آیا آن قسمت پیشانی و جلوی سر شما نیست ؟
درست حدس زدید ، اکثر رباینده‌گان از این موضوع بی خبر هستند که یکی از ساده ترین شگردها برای پی بردن به اصل قضیه این است که وقتی در حال فکر هستید به کدامین قسمت سر ضربه می زنید ، در پس و بالای کلی چیزی برای فشار دادن و بخاطر آوردن وجود ندارد .
یا یکی از ساده ترین نمونه های این مورد وقتیست که کسی به شما پیشنهاد کاری می دهد ، شما در صورت رد درخواست علاوه بر گفتن کلمه نه با تکان دادن سر به طرفین این موضوع را به شخص می رسانید و در بسیاری از موارد همین تکان دادن سر منظور شما را خواهد رساند .
پس تا اینجا متوجه نقش موثر زبان بدن در مهندسی اجتماعی شدید ، در زبان بدن حرکات دست ها ، پاها و صورت بسیار موثر است و نقش بسزایی در فریب افراد دارد و اگر در این موضوع ریزتر شویم از حرکات پلک ها و ضربان قلب و ... می تواند اطلاعاتی بسیار مهم بدست آورد ، ماشین دروغ سنج نیز بر همین اساس کار می کند .

اولین قسمتی که باید به آن توجه داشت دست هاست ، حرکت دست ها باید کاملا حساب شده باشد ، یادتان باشد که دست های رو به جلو و با کف دست باز نشانه صداقت و راستگویی است .

من !؟ نه باور کن که کار من نبوده .
من هیچ اطلاعی از قضیه ندارم
بذار صادقانه جواب بدم

وقتی در همین حرکت از شانهای بالا انداخته و ابرون بر آمده استفاده شود ، مفهومی که شخص مقابل درک می کند این است که شخص مقابل واقعا از قضیه بی اطلاع است .

از حرکاتی که ممکن است در بیننده تاثیر منفی بگذارد خودداری کنید ، مثال نشان دادن شست دست ، ممکن است این عمل برای شخص مقابل مساوی همان معنی برای شما نباشد و به جای یک اثرپذیری خوب شاهد جدال فیزیکی و لفظی باشید !

در رم مثل یک رومی عمل کن

به حرف های خود دقت کنید اگر شکل دستان به حالت دست به سینه در آمد یا یک دست روی چانه قرار گرفت به طوری که قسمتی از دست دهان را می پوشاند آگاه باشید که شنونده به هیچ عنوان حرف شما را نپذیرفته است و قانع نشده .

همین دستان می تواند دروغ شما را فاش کند ! در موقعه دروغ گویی معمولا اشخاص جلوی دهان و بینی خود را به شکل تقریبا غیر کاملی می گیرند یا با آنها بازی می کنند .

البته باید بگم که تو ترافیک گیر کرده بودم ...
کارهای اداره واقعا" سنگین شده ...

عامل بعدی یکی از مهمترین عوامل در نزدیک شدن به اشخاص است ، قبل از شروع توضیحات مطلبی رو بازگو می کنم که خودم در شرح جریان و واقعه آن بوده ام .
در ترم دوم دانشگاه ما برای گرفتن اکانت اینترنت دانشگاه و همین طور پرینت بعضی از مطالب به یکی از کارمندان خانم دانشگاه مراجعه می کردیم ، چند باری که با دوستان و همکلاسی ها به اتاق ایشون رفتیم ، ایشون رو بدور از هرگونه مهر و محبت عاطفه دیدم ! به هیچ عنوان لبخند روی لبان این شخص ظاهر نمی شد ، بعد از مدتی متوجه برخورد عجیبش با خودم شدم (در اولین برخورد ها من معمولا با فاصله حدودا 3-4 متری از ایشون وایمیستادم) وقتی من وارد اتاق میشدم شکل نگاه و حرف زدنش کاملا با من فرق داشت ، حقیقتا قضیه برای خودم هم جالب شده بود ! که چرا با من بدین شکل و با بقیه بدان شکل ، در اواخر ترم دوم در حین رفت و آمد متوجه تغییر رفتار کاملش با خودم شدم وقتی وارد اتاق میشدم لبخندی به نشانه خوش آمد گویی برلب داشت و تقریبا صحبت ها بین دو طرف صمیمی شده بود ، من در تابستان همان سال کتابی از آلن پیز خواندم با عنوان « زبان بدن » ، در قسمت دوم این کتاب متوجه چرایی تغییر رفتار شخص مقابل شدم و این نکته که از دید همه مخفی بود حریم نام داشت .
بله همان طور که می دانید حیوانات برای حفاظت از قلمرو و محدوده خود منطقه متعلقه خود را با انواع و اقسام کارها علامت گذاری می کنند ، در انسان ها نیز چیزی به نام حریم وجود دارد ، حریم هر انسان نسبت به شهری بودن یا روستایی بودن و بسیاری از عوامل دیگر بررسی می شود ، وقتی شما وارد این حریم بشید ممکن است در یکی از رده های زیر قرار بگیرید :

1. محدوده خصوصی : این قسمت جایگاه افرادیست که شخص با آنها رابطه عاطفی و صمیمی فوق العاده دارد ، وسعت این فضا چیزی بیشتر از پانزده سانتی متر و کمتر از چهل و شش سانت است .

2. محدوده شخصی : محدوده دوستان ، اقوام ، بین چهل و شش سانتی متر تا یک متر و نیم

3. محدوده اجتماعی : اشخاصی که اجبارا باید آنها را تحمل کرد مثلا نقاش خانه یا لوله کش یا خدمتکار و ... ، بیش از یک و نیم متر و کمتر از سه متر و نیم

4. محدوه عمومی : افراد ناشناس ، افراد حاضر در یک خیابان ، بیش از سه متر و نیم

معمولا این اندازه ها برای همه یکی نیست ، فاصله ها در شهر ها و روستاها تفاوت بسیار فاحشی دارند ، در روستا به دلیل باز بودن فضا محدوده شخصی افراد گاها" به بیش از پنج متر می رسد .

پس حالا متوجه رفتار کارمند دانشگاه با من می شوید ، من مدتی در محدوده عمومی قرار داشته ام تا کم کم شخص مورد نظر اجازه ورود به محدوده اجتماعی و شخصی را برای صادر کرد .
بقیه افراد به خاطر این ناموفق بودند که در همان ابتدای کار وارد محدوده شخصی شخص می شدند و برای همین کارمند مذکور از خود واکنش دفاعی نشان می دهد .

وقتی دست به سمت چشم یا گوش حرکت کند ، روی چشم را بپوشاند یا گوش را مالش دهد نشانه این است که شخص مورد صحبت شما از نطق های شما به هیچ عنوان راضی نیست و ترجیح می دهد آنها را نشود . همین طور اگر شخص مقابل در حین صحبت های شما به خارش گردن و معمولا زیر گوش بپردازد بیانگر مطمئن نبودن شخص و تردید داشتن است .
اگر دست شخص زیر چانه خود باشد نشانه بی میلی به بحث است و در حالتی که دست به صورت مشت در کنار صورت قرار گرفته با انگشت اشاره رو به بالا نشانگر علاقمند بودن فرد به بحث است .

علاقمندی به بحث

بحث گریزی (بی حوصلگی)

خاراندن چانه هم نشانه تصمیم گیری و تفکر شخص است در این گونه از موارد شخص مورد نظر احتیاج به تلنگری برای قبول درخواست شما دارد .

هووووم.... شاید حق با اون باشه
فکر نکنم ضرری داشته باشه

به حالات زیر توجه کنید :

حالت استاندارد دست به سینه

حالتی خصمانه

حالتی کاملا جدی

حالا به بررسی حالات پاها می پردازیم :

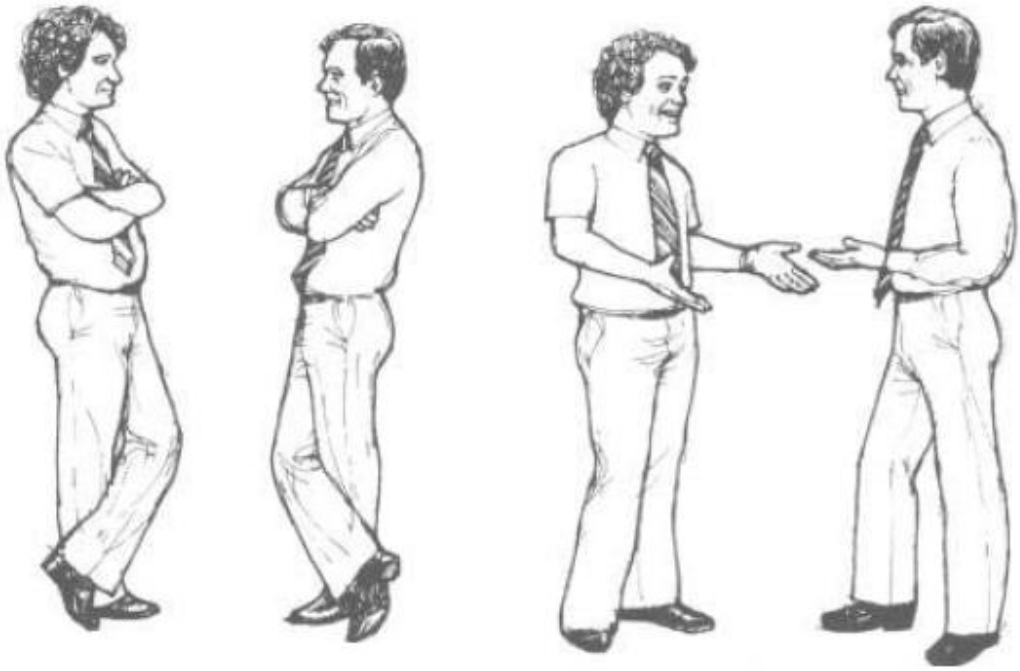
حالت استاندارد روی هم قرار دادن پاها

حالت گیره پا به شکل 4

حالت گیره پا به شکل عدد 4 نشان دهنده سرسخت بودن و خودرای بودن شخص است .

حالت نارضایتی خانم ها ، شما در اغلب سریال های تلوزیون این حالت را دیده اید

پاهایی روی هم در حالت ایستاده نشانه برخوردار نبودن شخص از صمیمی بودن و آشنا بودن با افراد است



شکل سمت راست نشانه باز بودن افراد (صمیمی بودن) و شکل سمت چپ نشانه بسته بودن (غریبه بودن) است

زبان بدن به همین چند مثال و تصویر ختم نمی شود ، بلکه هزاران صفحه مطلب و تعداد بسیار زیادی کتاب در باب آن نوشته شده است . هدف از توضیحاتی پیرامون زبان بدن در این مقاله آشنایی جزئی با آن است ، در پایان مقاله نام تعدادی از کتاب های زبان بدن آورده شده است که حتما به شما توصیه می کنم آنها را بخوانید .

برای آشنایی هر چه بیشتر با این زبان به مجلات دقت کنید ، پای تلوزیون نشسته و حرکات مجریان ، بازیگران و ... را مورد ارزیابی قرار دهید .

جعل هویت

جعل هویت دیگر از هنرهای یک مهندس اجتماعیست .
در جعل هویت ابتدا باید به اطلاعات کافی در مورد سازمان ، نوع کارت های شناسایی و .... پی ببریم .
بعد از آن به یک نمونه از کارت شرکت احتیاج داریم .
بطور کلی تعداد زیادی از کاربران در فضای اینترنت عضو سایت های سرگرمی ، دوستیابی و بحث و تبادل و نظر هستند ، در نمونه اول با رفتن به سایتی که یکی از کارمندان شرکت مورد نظر در آن عضو بود اقدام به ساخت موضوعی با نام «شغل شما چیست؟» می کنیم ، سپس در تاپیک توضیح دادیم که علاوه بر شغل اگر کارت شناسایی هم دارید برای بازدید کننده ها قرار بدید تا تاپیک فعالتر باشد و برای جلب اعتماد بیشتر یک عکس از کارت یکی از پرسنل یک شرکت نامربوط به موضوع را قرار می دهید .
در صورت موفق بودن این روش ما توانسته ایم یک نمونه از کارت را در اختیار بگیریم و در صورتی که شخص مورد نظر مشخصات و همین طور شماره پرسنلی و ... را از روی کارت حذف کرده بود می توانیم با هنر فتوشاپ اقدام به ساخت یک کارت جعلی کنیم .

در نمونه دیگر به دو شخص برای بدست آوردن نمونه کارت نیاز است ، شخص اول از نگهبان درخواست می کند که با او یک عکس یادگاری بیاندازد و شخص دوم دست به دوربین منتظر است ، پس از راضی شدن نگهبان و گرفتن ژست و خنده بر لب ، شخص دوم بزرگنمایی کامل دوربین را بر روی کارت آویز شده به سینه نگهبان قرار داده و در نتیجه صاحب یک عکس با کیفیت و دارای اطلاعات جزئی تر از کارت می شوند .

در موارد دیگر نیز بهمین شکل ، در حین حرف زدن با یکی از کارمندان شرکت وانمود می کنیم گوشی موبایلمان زنگ می خورد گوشی را درآورده در حالتی که مانیتور گوشی به سمت ماست و دوربین به سمت شخص مذکور اقدام به گرفتن عکس از کارت می کنیم .

به نمونه از کارت ملی جعلی نگاه کنید :

بعد از جعل کارت ملی یا شناسنامه دست شخص متخاصم برای بسیاری از کارها باز می شود که از آن جمله می توان به :
1. صدور کارت بانکی (عابر بانک)
2. گرو گذاشتن کارت در شرایطی خاص

3. نفوذ به مکانهایی که شخص سعادتمند مورد اعتماد آنهاست

و ....

برای بوجود نیامدن هیچگونه مشکلی چه برای خودم و چه برای اشخاصی دیگر لازم به ذکر است که همه موارد کارت بالا به غیر از شماره ملی و شماره پایین کارت ، جعلی و کاملا ساختگی می باشد .

با ساخت کارت ملی بدین شکل می توان وارد مرحله جدیدی از کار شد ، می توانید به بانکی که شخص اولیه در آن حساب دارد مراجعه کرد و اذعان کرد که کارت خودپرداز بانک را گم کرده اید و درخواست ابطال و مجددا صدور آن را دارید ، بعد از طی شدن مراحل شما صاحب کارتی جدید و با موجودی بادآورده خواهید شد !

البته در کارت بالا مشکلاتی نیز بچشم می خورد مانند :

1. رنگ نور تابیده شده به لباس ها (در کارت سمت چپ کاملا رعایت شده است ولی روسری فرد راست کاملا با حالت نور مغایرت دارد)
2. تاریخ تولد !
3. حالت برش کارت (در گزینه سمت راست کاملا رعایت شده ولی در کارت سمت چپ در گوشه راست و چپ مشکلاتی دارد)

که این موارد از تازه کار بودن جاعل خبر می دهد!

به نمونه دیگر توجه کنید :

مهندسی اجتماعی برپایه اطلاعات فنی

همان طور که گفته شد در این مقاله موضوع اصلی مهندسی اجتماعی بر پایه روابط می باشد اما توضیح مختصری در مورد مهندسی اجتماعی بر پایه اطلاعات فنی نیز خالی از لطف نخواهد بود .
در سناریو های بخش اول دیدیم که نفوذگر با استفاده از روش های فریبکارانه و با استفاده از تلفن و روابط رو در رو و ... وارد مراحل مختلف نفوذ میشد اما در این نوع از حملات نفوذگر با استفاده از اینترنت و ... شما را فریب می دهد .
به طور مثال تا به امروز بارها اسم ویروس های را شنیده اید که بر روی هنر پیشه ها ، سیاستمداران و حتی اتفاقات گذاشته اند ، این گونه از مهندسین اجتماعی با ارسال مثلا یک پیام الکترونیکی با متنی محترمانه و جذاب از شما دعوت می کنند که اطلاعاتی را برای آنها ارسال یا روی لینکی کلیک و یا نرم افزاری را دانلود کرده و از آن استفاده کنید .

روش های مرسوم مورد استفاده در این حملات شامل :
نامه الکترونیکی
گفتگوهای جاندار و زنده اینترنتی
وب سایت ها

نامه الکترونیکی : احتمالا تا بحال به نام های با مضمون های و موضوعات عجیب روبرو شده اید که به شما وعده یک جایزه ، پیروزی در یک مسابقه یا برنده بانک می نامند یا حتی نامه های از طرف اشخاص سیاسی ، حزب های مختلف و خبرهای خلاف واقع ، بدون شک شما هم تا بحال بر روی آنها کلیک کرده اید و شاید تا امروز به بعضی از آنها جواب نیز داده باشید !
اکثر این پیام ها جعلی و فقط با هدف دریافت اطلاعاتی از شما می باشند .

شما در بانک پرپول برنده شدید ! این ممکن است متن و تیتر یک پیام الکترونیکی باشد با باز کردن آن خواهید دید که بعد از ستایش شما به عنوان فردی خوش شانس در میان تمام عالم و گذاشتن تعداد زیادی هنداونه در زیر بازوانتان از شما می خواهند که مشخصات خود را برای آنها بفرستید تا در اسرع وقت جایزیتان را برایتان ارسال کنند یا به صورت حضوری جایزه را به شما تقدیم کنند .
در اولین قدم ببینید که چرا شما برنده شدید ؟ اصلا در آن بانک حسابی دارید ؟ چرا بانک مشخصاتی را از من می خواهد که در موقع باز کردن هر حسابی انها را از من دریافت می کند ؟ پس دفاع در برابر اینگونه حملات چندان کار سختی نیست .
از جمله موضوعاتی دیگر که می تواند متحرک اذهان باشد جملاتی مانند : عکس های لو رفته فلان بازیگر ، فیلم فلان شخصیت در مهمانی و به طور کلی جدیدترین اتفاقات روز است ، یعنی به محض پیشآمد حرف و حدیثی حتی در صورتی که شایع نبوده باشد ، این نفوذگران با ارسال انبوهی از ایمیل ها با مضمون همان اتفاق اما با محتوای دیگر اقدام به شکار طعمه های خود می کنند .
حال محتوای این پیام ها ممکن است یک عکس ، یک فایل یا آدرسی باشد که از شما بخواهد بر روی آن کلیک کنید ، که هر سه این موارد از درجه خطر بالایی برخوردارند .
فایل ضمیمه شده در پیام ممکن است به انواع بد افزار ها آلوده باشد ، آدرس ممکن است شما را به سمت بد افزارها هدایت کند یا اینکه با استفاده از روش های دیگر اقدام به بهره برداری از شما کند .

همچنین در حملاتی از همین دست نفوذگران از عضویت شما در وب سایت خاص استفاده کرده از طرف وب سایت ایمیلی را برای شما ارسال می کنند و می خواهند که بر روی لینک کلیک کرده و در سایت وارد شوید و مشخصات اکانت خود را چک کنید ، یا اکانت شما معلق شده است و از شما می خواهند برای فعال سازی دوباره به لینک رجوع کنید و ...
این گونه حملات فیشینگ نام دارند ، در این نوع نفوذگران با استفاده از آدرسی مشابه و همین طور صفحه مشابه از وب سایتی که در آن عضو هستید شما را فریب داده و اطلاعات واقعی شما را می ربایند .

همچنین نفوذگران با استفاده از سرویس های گفتگوی زنده اقدام به برقرای تماس با شما می کنند و در خلال این تماس ها اقدام به جلب اعتماد شما می کنند ، ازدواج اینترنتی جزو مهندسی اجتماعی محسوب می شود .

اغلب نفوذگران برای فریب از طریق آدرس های اینترنتی به یکی از روش های زیر متوصل می شوند :

- استفاده از IP سایت بجای آدرس مثلا :

Ping Lbankiran.ir >>>> 209.178.169.128

آی- پی سایت بانک همان طور که مشاهده می کنید 209.178.169.128 است ، هکر از این قضیه استفاده می کند صفحه قلابی خود را بر روی آدرسی مشابه به فرض 209.178.110.128 قرار می دهد .

- استفاده از آدرس های کد شده نا معلوم حتی اگر آدرس سایت واقعی باشد
- استفاده از آدرس بار و استاتوس بار جعلی

و ...