



Social
Engineering



Identity Theft

ماژول 10

مهندسی اجتماعی و سرقت هویت



Certified Secure Computer User

Honors & Awards

- ❑ **MCSA2003-MCSA2003Security**
- ❑ **MCSE2003-MCSE2003Security**
- ❑ **Windows Server 2008 Network Infrastructure Configuration**
- ❑ **Windows Server 2008 Application Infrastructure Configuration**
- ❑ **Windows Server 2008 Active Directory Configuration**
- ❑ **MCITP Server Administrator**
- ❑ **MCITP Enterprise Administrator**
- ❑ **Microsoft Certified Information Technology Professional**
- ❑ **Installing and Configuring Windows Server 2012**
- ❑ **Administering Windows Server 2012**
- ❑ **Configuring Advanced Windows Server 2012 Services**
- ❑ **Microsoft Certified Solutions Associate 2008, 2012**
- ❑ **Microsoft Certified Solutions Expert 2012 - Server Infrastructure**
- ❑ **IT professional - Cyber Security Org – SANS – Cloud Security Org – Network Security Org**
- ❑ **Compia A+ - Compia Network + - Compia Security + - Compia Master Level Security (CASP)**
- ❑ **Mcp V1, 2- MCTS**
- ❑ **Microsoft Certified Solutions Expert 2012 - Cloud & Security**
- ❑ **Microsoft Certified Solutions Expert 2012 – MSG**
- ❑ **BA-IT , MS-MBA E.Commerce**

Best Regards,

Alireza Ghahrood

Pm: Security Products Manager

(Security Solution Provider : Cyber Space | BigData | Cloud | Virtualization

Sarv Co

Email: Ghahrood.A@Sarvrayaneh.com

Tel : +98 (21) 88027364 Ext.136 | Cell :+98 (912) 1964383 |



مشاور انفورماتيك شما . قابل اعتماد . قابل اتکا



آنچه در این فصل می آموزید



سرقت هویت



مهندسی اجتماعی



چگونگی شناسایی قربانی سرقت هویت



بعد از سرقت هویت چه کار باید کرد؟



گزارش تخلف



روش های جلوگیری

سرقت هویت



سرقت هویت یا جعل اطلاعات جرمی است که جعل کننده از اطلاعات هویت فرد سوءاستفاده میکند. اطلاعاتی همچون تاریخ تولد، شماره ملی، گواهینامه و ...



زیان مالی

مجازات کیفری



اثرات سرقت هویت

سوء استفاده از اطلاعات سلامت،
اجاره نامه، حساب های بانکی و
اطلاعات کارمندی

مشکلات شرعی



اطلاعات قابل سرقت



روشهای سرقت هویت



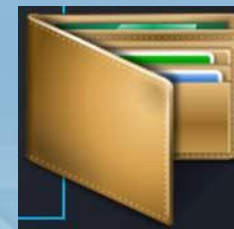
مهندسی اجتماعی

هک

کلاهبرداری فیشینگ



دزدی مدارک کارمندان



هکرها چه استفاده هایی از سرقت هویت می کنند



کلاهبرداری های بانکی

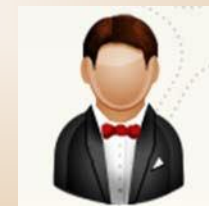
جعل اسناد دولتی

جعل کارت بانکی

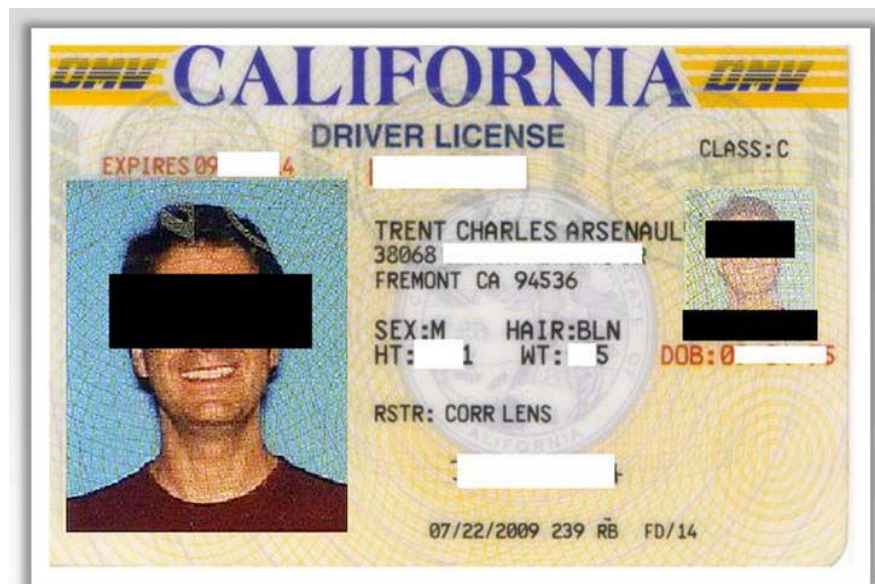


کلاهبرداری با تلفن

جعل مدارک کارمند



نمونه ای از جعل گواهینامه



مهندسی اجتماعی



مهندسی اجتماعی

مهندسی اجتماعی هنر وادار
کردن افراد به فاش کردن
اطلاعات شخصی است
این عمل سرقت اطلاعات حساس
افراد به کمک تکنیکهای انسانی
میباشد.



اطلاعات به دست آمده توسط مهندسی اجتماعی

اطلاعات حساس مانند
مشخصات بانکی

کلمات عبور

دیگر اطلاعات شخصی



انواع مهندسی اجتماعی

بر اساس تکنیک های انسانی
بر اساس تکنیک های کامپیوتری

نمونه های از مهندسی اجتماعی



سلام، ما شرکت نرم افزاری ... میباشیم. ما مایل به کسب نیرو برای تیم نرم افزاری خود میباشیم. شماره شما را از سایت های کاریابی پیدا کردیم. لطفا اطلاعات شغلی خود را به همراه اطلاعات از پروژه فعالیت خود به همراه شماره ملی و آدرس محل سکونت را برای ما ارسال نمایید

سرقت به عنوان متصدی بانکی



سلام. من قهرود متصدی بانک ملی هستم. با توجه به مشاهده موارد مشکوک در سیستم بانکی مون، باید اطلاعات امنیتی خود را بروزرسانی کنیم. لطفا اطلاعات بانکی خود را برای ما ارسال کرده تا از هویت شما اطمینان حاصل نماییم.

ممنون آقای ناصری. اطلاعات را ارسال کردم. مورد دیگری نیاز نیست؟

پشتیبانی حراست



سلام. من قهرود هستم. همکار مدیر حراست شما آقای
فلانی! ما از طرف سازمان، مامور بررسی پروسه مانور آماده
باش حوادث سایبری هستیم. بخش شما ده دقیقه زمان
برای مواجهه با کرش کردن سایت دارد

پشتیبانی فنی



مردی با help desk سازمان تماس گرفته و به اسم یکی از کارکنان چگونگی بازیابی کلمه عبور فراموش شده خود را میپرسد. سپس میگوید که در یک پروژه تبلیغاتی بزرگ فعال بوده و در صورت موفق نشدن، رئیس بخش او را اخراج میکند.

Help desk برای او احساس همدردی کرده و کلمه عبور او را به حالت اولیه برمیگرداند. این کار ناخواسته به نفوذگر اجازه دسترسی اولیه به شبکه سازمان را میدهد.



مهندسی اجتماعی براساس انسان

استراق سمع

استراق سمع گوش سپردن به صحبت‌های افراد بدون اجازه می‌باشد. استراق سمع در تمامی راه‌های ارتباطی مانند تلفن یا صحبت‌های مستقیم امکان پذیر است



Shoulder surfing

➤ به عمل نگاه کردن از روی شانه فرد برای دزدیدن کلمات عبور یا اطلاعات بانکی، shoulder surfing میگویند
سارق میتواند حتی از فاصله و به کمک دوربین این کار را انجام دهد



گشتن زباله

به عمل بررسی زباله های سازمان، پرینتر یا جستجوی کامپیوتر افراد برای نوت های مختلف میگویند
اطلاعات فاش شده میتواند شامل قبض های موبایل، اطلاعات شناسایی افراد و غیره باشد.



مهندسی اجتماعی بر اساس تکنیکهای کامپیوتری



ایمیل های hoax که شامل اخبار ویروس ها یا بدافزار ها میباشند

گفتگوی اینترنتی با فرد مورد نظر برای کسب اطلاعات شخصی



**Pop-up
Windows**

**Hoax
Letters**

**Chain
Letters**

**Instant
Chat
Messenger**

**Spam
Email**

پنجره ای که در زمان گشتو گزار در اینترنت نمایش داده شده و خواستار اطلاعات کاربری افراد میباشد

نامه ها یا ایمیل های که شامل کارت های هدیه شده و تقاضای ارسال ایمیل از طرف کاربر را دارد

ایمیل های ناخواسته یا مشکوک که تقاضای اطلاعات بانکی افراد را دارند

نمونه مهندسی اجتماعی بر اساس تکنیک های کامپیوتری Phishing

نامه ای به ظاهر قانونی که توسط مؤسسه معتبر ارسال شده و درخواست اطلاعات فرد را دارد

ایمیل ها یا پنجره های زمان گشت و گزاری که ناخواسته ظاهر شده و از طرف مؤسسات معتبر تقاضای تکمیل اطلاعات شخصی را دارند

Privacy | citi.com | Careers | Use Credit Wisely | citicards.com

Confirm Required Information

Your Profile Information

Full Name:*

Address:*

City:*

State:*

Zip:*

Your Personal Information

Social Security Number:*

Mother's Maiden Name:*

Date Of Birth:*

Your Account Information

ATM Card Number:*

Expire Date:*

Cw2 Code:*

Card Pin Code:*

Your Internet Banking Information

Account Type:*

Your User ID:*

Your Password:*

E-Mail:*

SECURE REGISTRATION
Your privacy and security are important.

Online Services

- View your statements and unbilled activity
- Pay Online
- Update your personal information or add an authorized user
- [Learn More](#)

Help / Contact Info

24 Hours a Day, 7 Days a Week:

- For Technical Assistance: 1-800-347-4934
- For questions about your Credit Card Account: 1-800-950-5114
- Outside the U.S., Canada and Puerto Rico Call Collect: 805-335-2222
- TDD/TTY for the hearing impaired: 1-800-325-2885
- [Email Profile](#)

Sign on

VeriSign
SECURE SITE
citigroup

citi
citi.com

A member of citigroup
Citigroup Privacy Promise
Terms, conditions, privacy and email opt out
Copyright © 2006, Citicorp

اخطارهای تلفنی

ایمیل های یا پاپ آپ هایی که تقاضای برقراری تماس از مؤسسات معتبر دارند

اخطارها معمولا شامل نکات امنیتی بوده و تقاضای نصب آنتی ویروس را دارند.

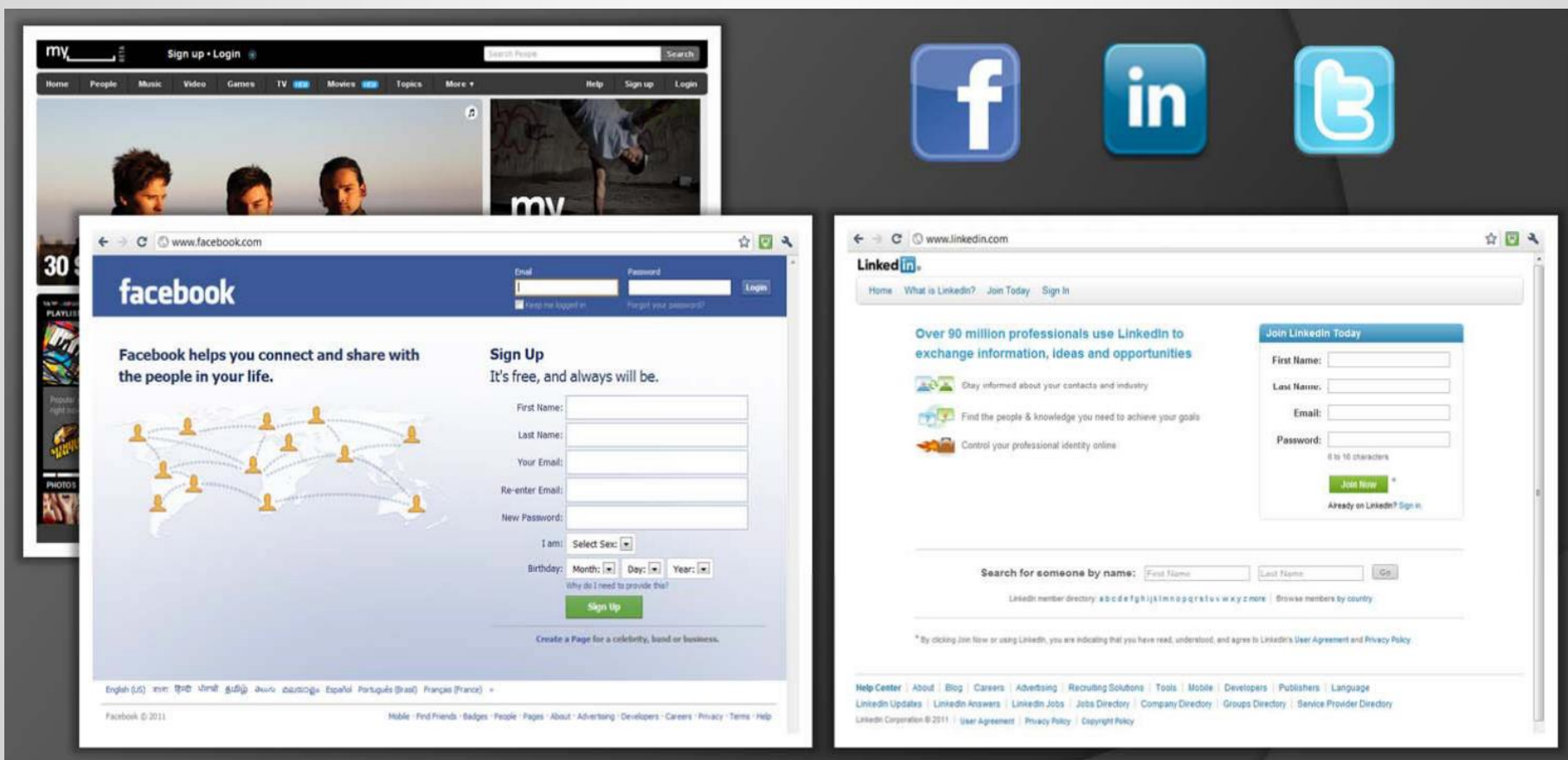
ایمیل ها تقاضای نصب آنتی ویروس را به کاربر میدهند

نکته قابل توجه حضور بدافزار ها در فایل های نصبی ارائه شده میباشد.



مهندسی اجتماعی از طریق سایتهای شبکه های اجتماعی

این عمل توسط جعل سایتهای شبکه های اجتماعی مانند فیسبوک، لینکدین یا توئیتر انجام میشود.
سارق به کمک جعل این سایت ها اقدام به سرقت اطلاعات شخصی افراد میکند.



چگونه متوجه شویم که قربانی هستیم؟



شرکت ها با شما تماس گرفته و از صحت فعالیت شما اطمینان حاصل میکنند.



دریافت ایمیل برای خرید یا انجام عملی که خود انجام نداده اید.



عدم دریافت ایمیل های بانکی



متوجه از بین رفتن بعضی از ایمیل های خود میشوید



تقاضای اجاره شما به خاطر سابقه بد پرداختی شما قبول نمیشود.

چگونه متوجه سرقت اطلاعاتمان شویم؟

شما ایمیلی دریافت میکنید مبنی بر خانه ای
که اجاره نکرده اید یا کاری که انجام نداده اید

کیف پول یا گواهی نامه خود را گم
میکنید

موارد مشکوک در تراکشنهای بانکی

دریافت سند شماره حساب بانکی
جدید



عدم پذیرش سرویس های
اجتماعی مبنی بر استفاده قبلی از
آنها

زمانی که اطلاعاتمان به سرقت رفت چه کنیم؟



Contact the credit reporting agencies

1

<http://www.experian.com> ➤

<http://www.equifax.com> ➤

<http://www.transunion.com> ➤



2

به سرعت به مؤسسات بانکی اطلاع رسانی کنید.

3

درخواست تراکنشهای بانکی



4

تراکنشهای خود را بررسی کرده و موارد مشکوک را گزارش کنید

5

مسدود کردن کارت



6

با تمامی شرکتهای قراردادی خود تماس گرفته و به آنها اطلاع دهید.

7

عوض کردن تمامی رمزهای عبور



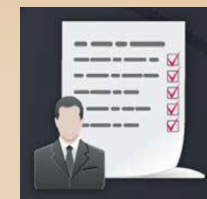
8

بستن حساب نفوذ شده





تحويل گزارش سرقت به همراه مستندات به پلیس



با شرکت های طرف قرار داد تماس گرفته و آنها را از وضعیت سرقت اطلاعات خود آگاه کنید.



بررسی چگونگی مقابله با سرقت های آینده



درخواست شماره حساب یا کارت جدید



تحويل گزارش تکمیل شده به پلیس فتا



درخواست از بانک یا مؤسسه مالی برای اخطار سرقت اطلاعات به مؤسسات طرف قرارداد

پلیس فتا



پلیس فتا وظیفه دریافت و رسیدگی به جرائم اینترنتی را دارد.

پلیس فتا مرجع قانونی برای رسیدگی به این نوع جرایم میباشد

فوانین جرایم رایانه ای:

<http://www.cyberpolice.ir/page/42981>

پیگرد قانونی سرقت اطلاعات

5

پیگیری دوره ای شکایات



4

تماس با یک وکیل معتبر
برای پیگیری ادامه رویه
های قانونی



3

تهیه کپی از گزارش
برای اثبات به شرکتها
مبنی بر بی گناهی
شما



2

تهیه شکایت به کمک
کمپسیون تجارت
فدرال و تکمیل
مستندات مبنی بر بی
گناهی شما در موارد
وقوع جرم توسط
سارق



1

تماس با پلیس فتا،
بانکها و هر مؤسسه ای
که ممکن است کمک
کند.

تهیه گزارش رسمی به
کمک مؤسسات و
مراجع قانونی



خلاصه فصل

- ☐ سرقت اطلاعات به معنی استفاده از اطلاعات شخصی افراد بدون آگاهی آنها میباشد.
- ☐ مجرمان در سطل های زباله یا دیگر کاغذهای موجود به دنبال اطلاعات میباشند.
- ☐ مجرمان از طرف سازمان های شناخته شده توسط فرد با او تماس گرفته و تقاضای فاش کردن اطلاعات را دارند.
- ☐ کامپیوتر و دیگر برنامه های خود را به روز نگاه دارید.
- ☐ به ایمیل های مشکوک پاسخ ندهید و اعمال درخواستی آنها را انجام ندهید.
- ☐ کلمه عبور معتبر و طولانی انتخاب کنید.
- ☐ به صورت دوره ای تراکنش های مالی خود را بررسی کنید.
- ☐ هیچ گاه اطلاعات مالی و شخصی خود را تلفنی بیان نکنید. مگر مواقعی که از امنیت خط ارتباطی اطمینان حاصل کرده باشید
- ☐ کارت ملی و اسناد خود را به درستی و با امنیت بالا نگه داری کنید.
- ☐ پاسخ ندادن به ایمیلهایی که تقاضای فاش سازی اطلاعات کاربری را دارند