ریاست جمهوری
سازمان مدیریت و برنامه ریزی
مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

مدرس: مهدی هدایت فر

فشرده و خلاصه مطالب دوره

تعریف امنیت

اَمنیّت حالت فراغت نسبی از تهدید یا حمله یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. امنیت از ضروری‌ترین نیازهای یک جامعه **است.**

دانشنامه سیاسی- داریوش آشوری-نشر مروارید- چاپ شانزدهم ۱۳۸۷- ص۳۸

امنیت=به فارسی برابر زنهار است

لغت نامه دهخدا

از هر طرف که رفتم جز وحشتم نیفزود
زنهار از این بیابان وین راه بی‌نهایت

حافظ

پیامدهای منفی وجود حفره های امنیتی در سازمان

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت یک سازمان
- از دست دادن داده و اطلاعات مهم
- اختلال در فرآیندهای جاری یک سازمان
- پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تاثیر جانبی منفی بر فعالیت سایر سازمان ها
- سلب اعتماد مشتریان
- سلب اعتماد سرمایه گذاران

جنگ و نبرد اطلاعاتی

نبرد تدافعی(Defensive)

شامل کلیه استراتژی ها و فعالیـت هـای دفـاعی در برابر حملات بر روی دارایی های ITC می باشد.

نبرد تهاجمی (Offensive)

شامل حمله به دارایی های ITC دشمن می باشد.

حمله چیست؟

Motive(Goal) + Method + Vulnerability

نقطه آسیب پذیــری + روش + انگیــزه ذهنــی(هدف)

تعاریف و مفاهیم اولیه

- **آسیب‌پذیری (Vulnerability):** ویژگی یا نقطه ضعفی در سیستم که می توان از آن سوءاستفاده کرد و امنیت سیستم را نقض کرد.
- **حمله (Attack):** تلاش برای یک نفوذ عمدی در یک سیستم اطلاعاتی/ ارتباطی، حمله گفته می‌شود (معمولاً با بهره‌گیری از آسیب‌پذیری‌های موجود).
- **نفوذ (Intrusion):** نتیجه یک حمله موفق و نقض امنیت سیستم.
- **مکانیزم امنیتی (Security Mechanism):** به هر روش، ابزار و یا رویه‌ای که برای اعمال یک سیاست امنیتی به کار می‌رود، یک مکانیزم امنیتی گویند.
- **خطمشی (سیاست) امنیتی(Security Policy):** نیازمندیهای امنیتی یک سازمان و یا یک سیستم اطلاعاتی/ ارتباطی را بیان می‌نماید.

تعاریف و مفاهیم اولیه

- **محرمانگی (confidentiality):** جلوگیری از افشای اطلاعات به افراد غیرمجاز
- **جامعیت (integrity:** جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات
- **دسترس پذیری (availability):** اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند.

انواع حملات

شنود یا Interception
در این روش نفوذگر به شکل مخفیانه از اطلاعات نسخه برداری می کند.

تغییر اطلاعات یا Modification
در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد.

افزودن اطلاعات یا Fabrication
در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

وقفه Interruption
در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

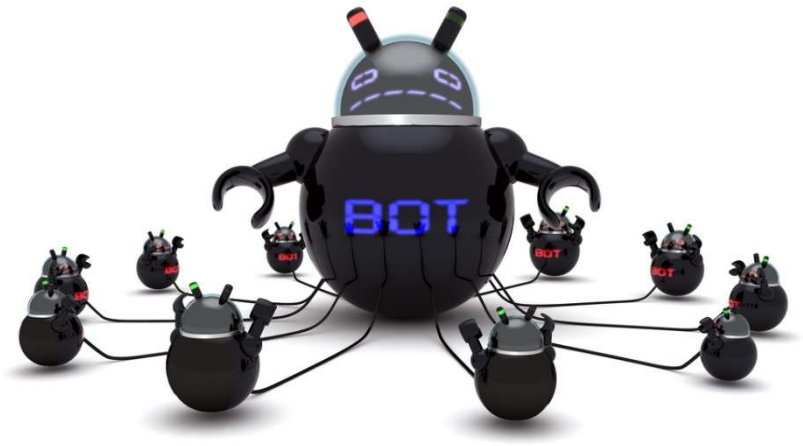
دشواری برقراری امنیت

- افزایش پیچیدگی و تهدید امنیت بدلیل تکامل پروتکلها
- امنیت: قربانی افزایش کارایی و مقیاس پذیری
- امنیت بالا: هزینه بر
- در اختیار بودن اطلاعات و ابزارهای دور زدن امنیت
- مبارزه و لذت بردن از دور زدن امنیت
- عدم در نظر گرفتن ملاحظات امنیتی در طراحی های اولیه سیستمها و شبکه ها
- امنیت معمولاً قربانی افزایش کارآیی و مقیاس پذیری می‌شود.
- بعنوان مانع در برابر انجام کار کاربران عادی عدم پیروی از سیاستهای امنیتی

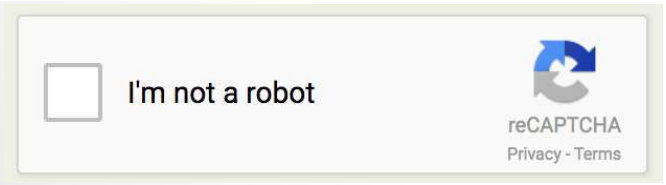
آگهی افزار

- به‌طور خودکار تبلیغات را ارائه‌می‌دهد.
- تبلیغات بالاپر pop-upبر روی وبسایت ها
- تبلیغات نمایش‌داده‌شده توسط نرم‌افزارها.
- اغلب اوقات نرم‌افزارها و برنامه‌های کاربردی که نسخه‌های رایگان عرضه‌می‌نمایند، همراه با آگهی‌افزارها می‌باشند.
- به عنوان ابزار تولید درآمد، توسط تبلیغات‌کننده‌ها، حمایت و یا نوشته‌می‌شوند.
- بسیاری از آن‌ها همراه با جاسوس افزارها برای ردیابی فعالیت‌های کاربران و سرقت اطلاعات همراه می‌شوند

رباتها



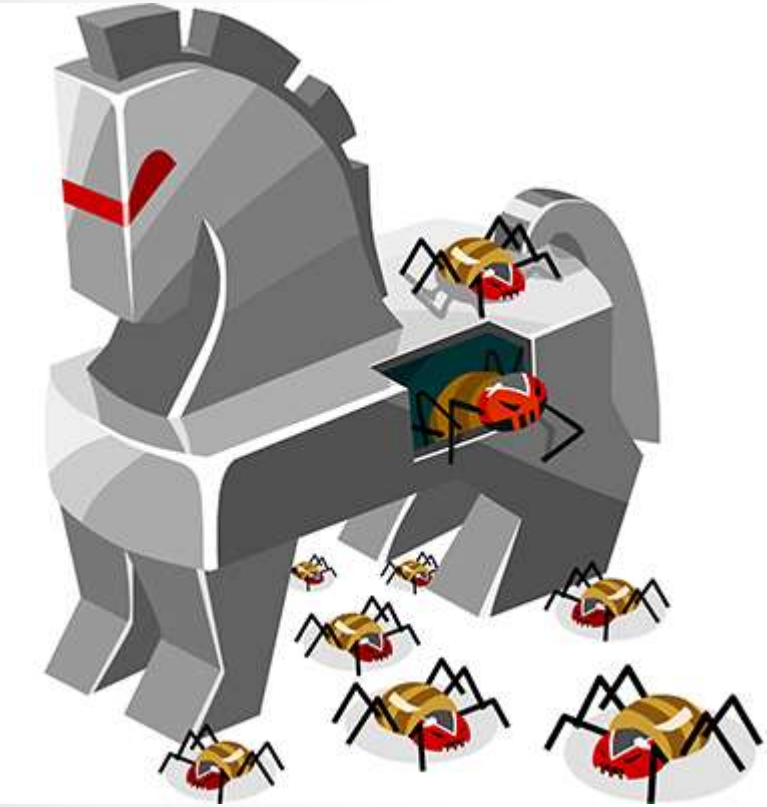
- برای انجام عملیات خاص به طور خودکار، ایجادشده‌اند
- برخی از ربات‌ها برای مقاصد بی‌ضرر ساخته‌شده‌اند (بازی‌های ویدئویی، مسابقات برخط، حراج‌های اینترنتی و...)
- می‌توان از ربات‌ها در باتنت‌ها (مجموعه‌ای از رایانه‌های متصل به‌هم که توسط شخص ثالث کنترل می‌شوند) برای حملات محروم‌سازی از خدمات (DDOS) استفاده نمود،
- به عنوان هرزنامه‌ها در ارائه‌ی تبلیغات در وب‌گاه‌ها، عنکبوت‌های وب که به داده‌های کارگزار آسیب‌می‌رسانند،
- برای توزیع بدافزارها که به عنوان اقلام جستجوی محبوب در وب‌گاه‌های بارگیری، تغییر چهره می‌دهند.
- وب‌گاه‌ها می‌توانند در برابر ربات‌ها، با استفاده از آزمون‌های کپچا (CAPTCHA)، در تأیید کاربران به عنوان انسان، از خود محافظت نمایند



باج افزار-RANSOM

- در اصل دسترسی به یک سامانه را محدود ساخته
- برای برداشتن این محدودیت، درخواست باج می‌نمایند
- از طریق رمزگذاری فایلها بر روی دیسک‌سخت
- معمولاً مانند یک کرم رایانه‌ای و از طریق یک فایل بارگیری‌شده و یا وجود یک آسیب‌پذیری در خدمات شبکه، خود را بر روی رایانه‌ها گسترش می‌دهند.

اسب تراوا-TROJAN



•خود را در قالب یک پرونده و یا برنامه‌ی معمولی، کاربر را برای بارگیری و نصب بدافزار فریب‌می‌دهند.

•امکان دسترسی از راه دور به رایانه‌ی آلوده را برای گروه مخرب فراهم‌می‌سازد

•زمانی که یک نفوذگر به رایانه‌ی آلوده دسترسی پیدا کرد، می‌تواند به سرقت اطلاعات (داده‌های مالی، داده‌های ورود، حتی پول الکترونیکی)، نصب بدافزارهای بیشتر، ویرایش پرونده‌ها، نظارت بر فعالیت‌های کاربر (تماشای صفحه‌نمایش، ثبت داده‌های واردشده از طریق صفحه‌کلید و ...)، به‌کارگیری رایانه در بات‌نت‌ها و فعالیت‌های اینترنتی ناشناس بپردازد.

ویروس کامپیوتری

توانایی کپی‌کردن خود و گسترش به رایانه‌های دیگر را دارا می‌باشد

اغلب از طریق اتصال خود به برنامه‌های مختلف و اجرای کد در زمان راه‌اندازی یکی از برنامه‌های آلوده، منتشر می‌شوند

همچنین می‌توانند از طریق پرونده‌های اسکریپت، اسناد، آسیب‌پذیری حملات تزریق کد در برنامه‌های تحت وب منتشرگردند

می‌توانند به منظور سرقت اطلاعات، آسیب‌رساندن به رایانه‌ی میزبان و شبکه، ایجاد بات‌نت‌ها، سرقت پول، نمایش تبلیغات، و... مورد استفاده قرارگیرند.

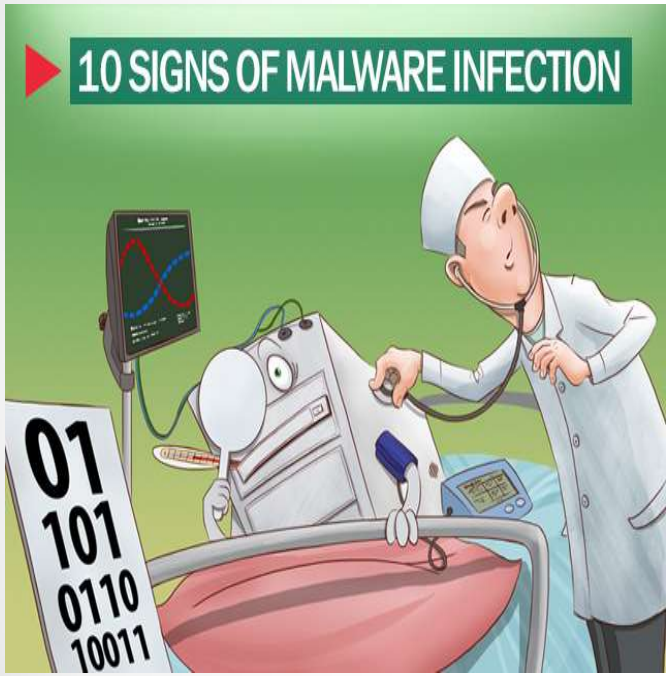
کرم رایانه ای-WORM

- برخلاف ویروس کرم‌ها خود را به برنامه‌های دیگر نمی‌چسباند.
- عموماً با اشغال پهنای باند به شبکه آسیب می‌رسانند
- که ویروس‌ها در بیشتر اوقات باعث خرابی برنامه‌های موجود در کامپیوتر آلوده و از دست رفتن اطلاعات موجود در آن می‌شوند.
- هدف کرم‌ها معمولاً استفاده از منابع می‌باشد و می‌تواند در دسترسی شما به منابع تأخیر بیاندازد.
- کرم در برخی از خصوصیات با ویروس مشترک است.
- مهمترین ویژگی مشترک آن‌ها این است که کرم‌ها نیز خود-همانندساز هستند،
- تولید مثل آن‌ها از دو جهت متفاوت است. اول اینکه، کرم‌ها مستقل و متکی به خود هستند، و محتاج به کد اجرایی دیگری نیستند.
- دوم، کرم‌ها از طریق شبکه‌ها، از ماشینی به ماشین دیگر منتقل و توزیع می‌شوند

هرزنامه-SPAM

- ارسال الکترونیکیِ پیام‌های ناخواسته می‌باشند
- رایج‌ترین رسانه برای هرزنامه‌ها، رایانامه می‌باشد
- غیرمعمول نیست که از پیام‌های فوری، نوشته‌ها، وب‌نوشت‌ها، انجمن‌های تحت وب، موتورهای جستجو و رسانه‌های اجتماعی برای ارسال هرزنامه استفاده نمایند.
- درست است که هرزنامه‌ها درواقع نوعی بدافزار نمی‌باشند، اما یکی از رایج‌ترین روش‌ها برای گسترش بدافزارها می‌باشند
- و این موضوع زمانی اتفاق می‌افتد که رایانه‌هایی که با ویروس‌ها، کرم‌های رایانه‌ای یا انواع دیگر بدافزار، آلوده شده‌اند، برای توزیع پیام‌های هرزنامه شامل بدافزارهای بیشتر، مورد استفاده قرارگیرند.
- کاربران می‌توانند با اجتناب از بازکردن رایانامه‌های ناشناس و خصوصی نگه‌داشتن آدرس رایانامه، خود را در برابر هرزنامه‌ها ایمن نگه‌دارند.

علائم بدافزار



1.اشکالات غیر-منتظره Unexpected Crashes

2.کاهش سرعت-Slow System

3.فعالیت بیش از حد هارد درایو-Excessive Hard Drive Activity

4.پنجره های ناشناس-Strange Windows

5.پیامهای عجیب و غریب-Peculiar Messages

6.فعالیت های بد برنامه-Bad Program Activity

7.فعالیت شبکه بصورت تصادفی-Random Network Activity

8.ایمیل ناخواسته-Erratic Email

9.آدرس های آی درون لیست سیاه-Blacklisted IP Address

10.غیرفعالی غیر منتظره آنتی ویروس-Unexpected Antivirus Disabling

قانون جرایم رایانه ای

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	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	

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.

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

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.**

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.

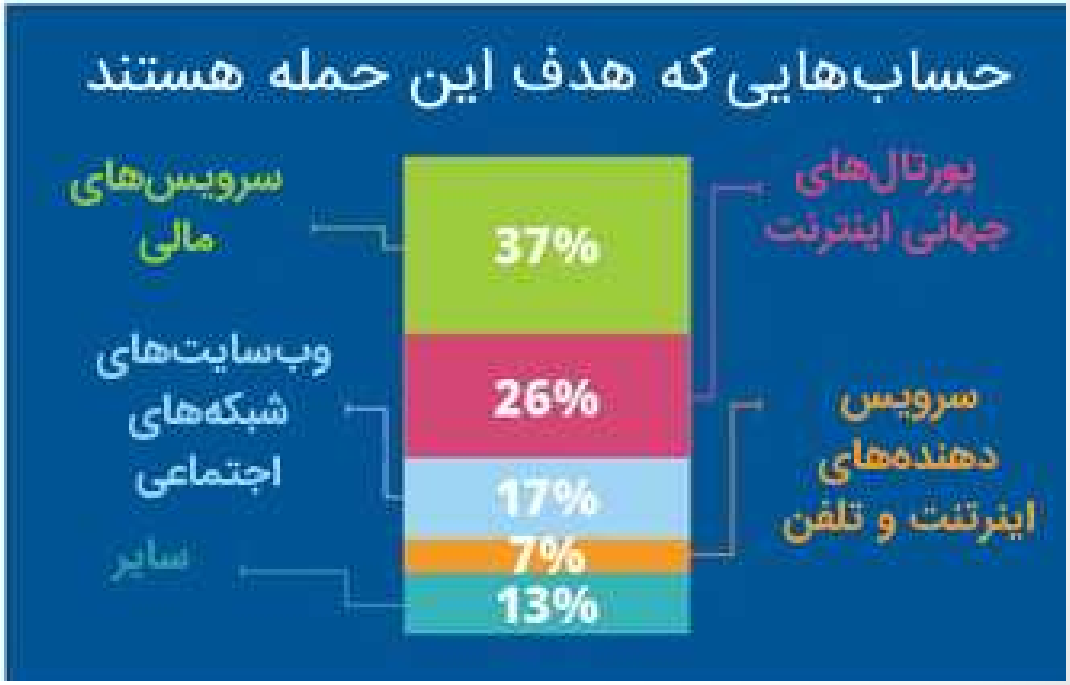
راه های امنیتی جهت کنترل و کم کردن خطرات احتمالی سوءاستفاده از گوشی تلفن همراه:

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.

انواع حمله های مهندسی اجتماعی

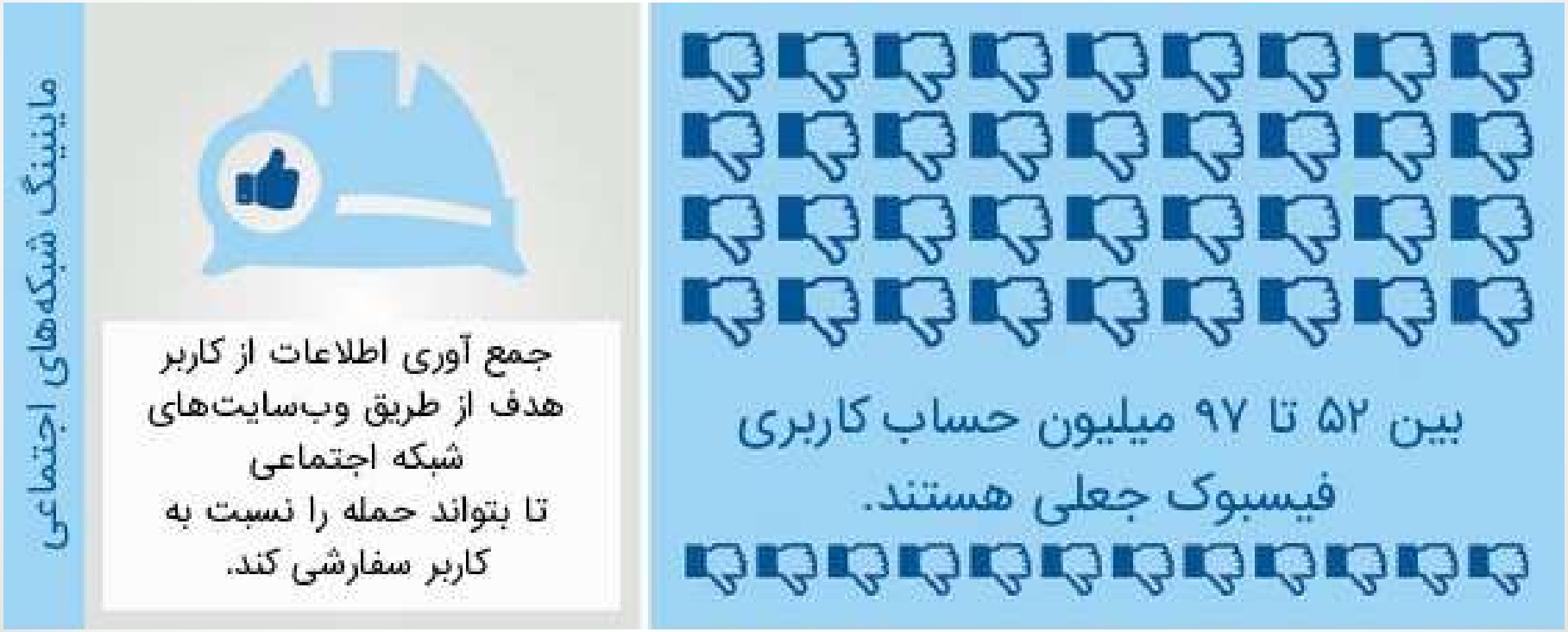
فیشینگ

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

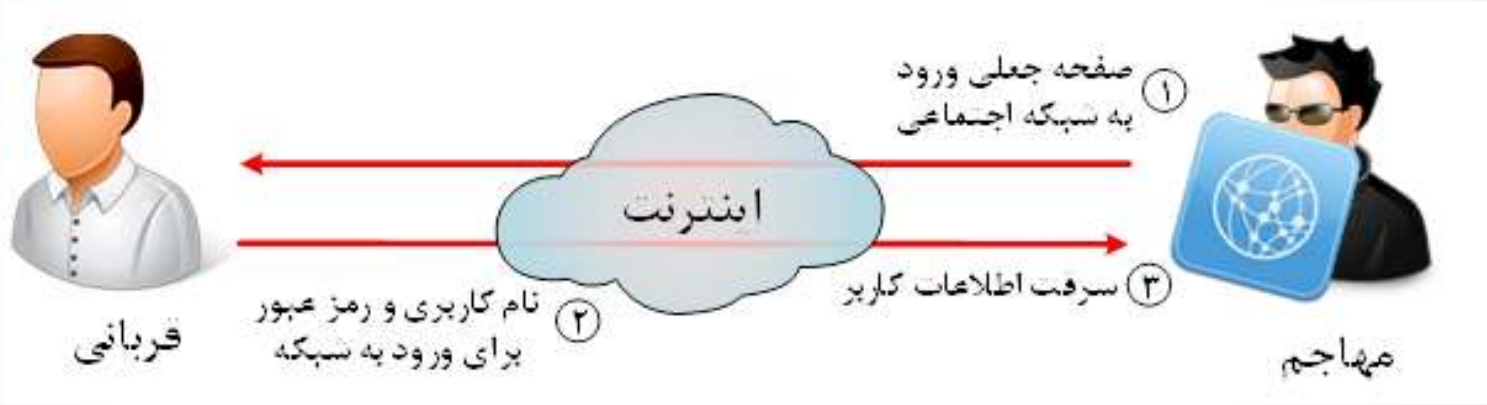


انواع حمله های مهندسی اجتماعی

انواع حمله های مهندسی اجتماعی



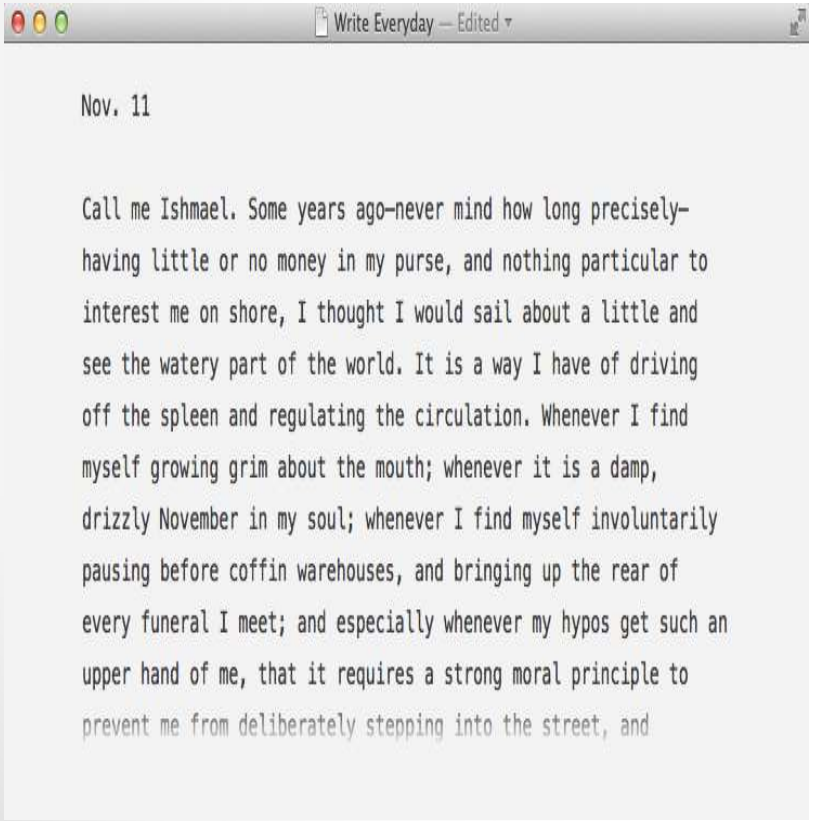
مهندسی اجتماعی
روش صیادی(Phishing)



مهندسی اجتماعی
روش دستاویزسازی (Pretexting)

چند تعریف در رمزنگاری

متن آشکارPlaintext

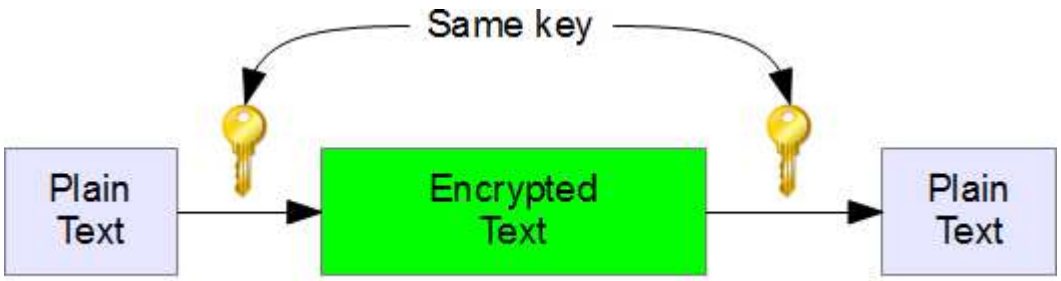


متن رمز Ciphertext

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUtl1lXyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```

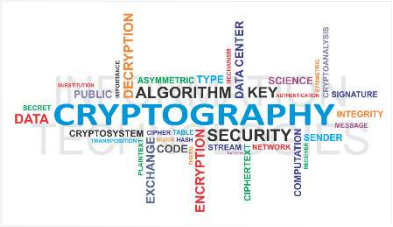
چند تعریف در رمزنگاری

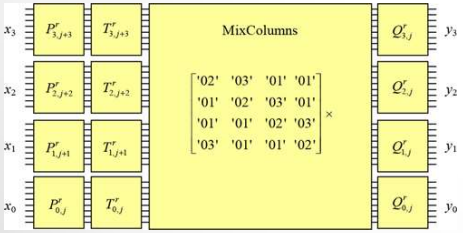
کلید key



اطلاعاتی که در Cipher استفاده میشود و فقط فرستنده و یا گیرنده آن را میدانند

چند تعریف در رمزنگاری





- رمز گذاری(**Encipher,Encrypt**)

  تبدیل Plaintextبه Ciphertext

- رمز گشایی(**Decipher,Decrypt**)

  استخراج Plaintextاز Ciphertext

- رمز نویسی(**Cryptography**)

  علم اصول روش های encryption

- تحلیل رمز(**Cryptanalysis**)

  علم اصول و روش های Decryptionبدون اطلاع از Keyکه به آن به اصطلاح codebreakingهم گفته میشود

- رمز نگاری(**Cryptology**)

  و بالاخره رمز نگاری یعنی علم حاصل از ترکیب Cryptographyو Cryptanalysis

رمزنگاری متقارن-Symmetric

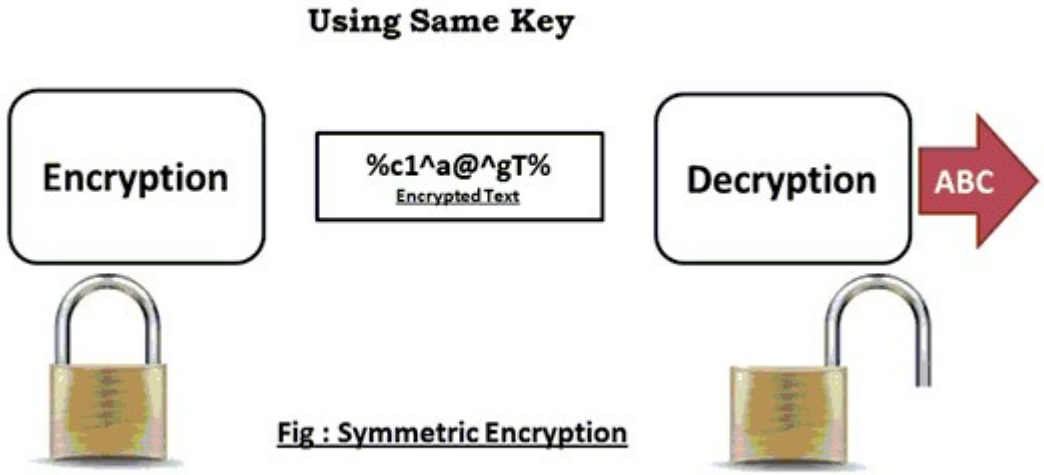


Fig : Symmetric Encryption

در این روش از کلید مشترک برای Encryptو Decryptاستفاده میشود از الگوریتم های معروف آن

- AES
- DES
- 3DES
- Blowfish
- RC4
- ..

رمزنگاری نا متقارن-Asymmetric

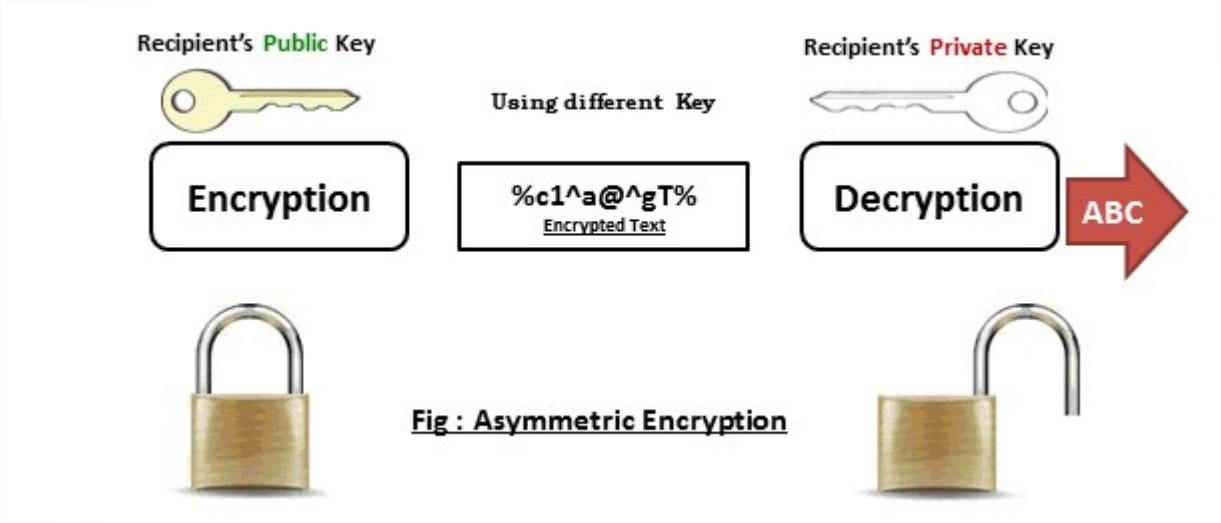


Fig : Asymmetric Encryption

در این روش به جای استفاده از یک کلید مشترک از یک جفت کلید به نام های عمومی(public)و خصوصی(private)استفاده میشود به این صورت که با public key اطلاعات encryptشده و با private key اطلاعات decryptمیشودز الگوریتم های معروف این روش:

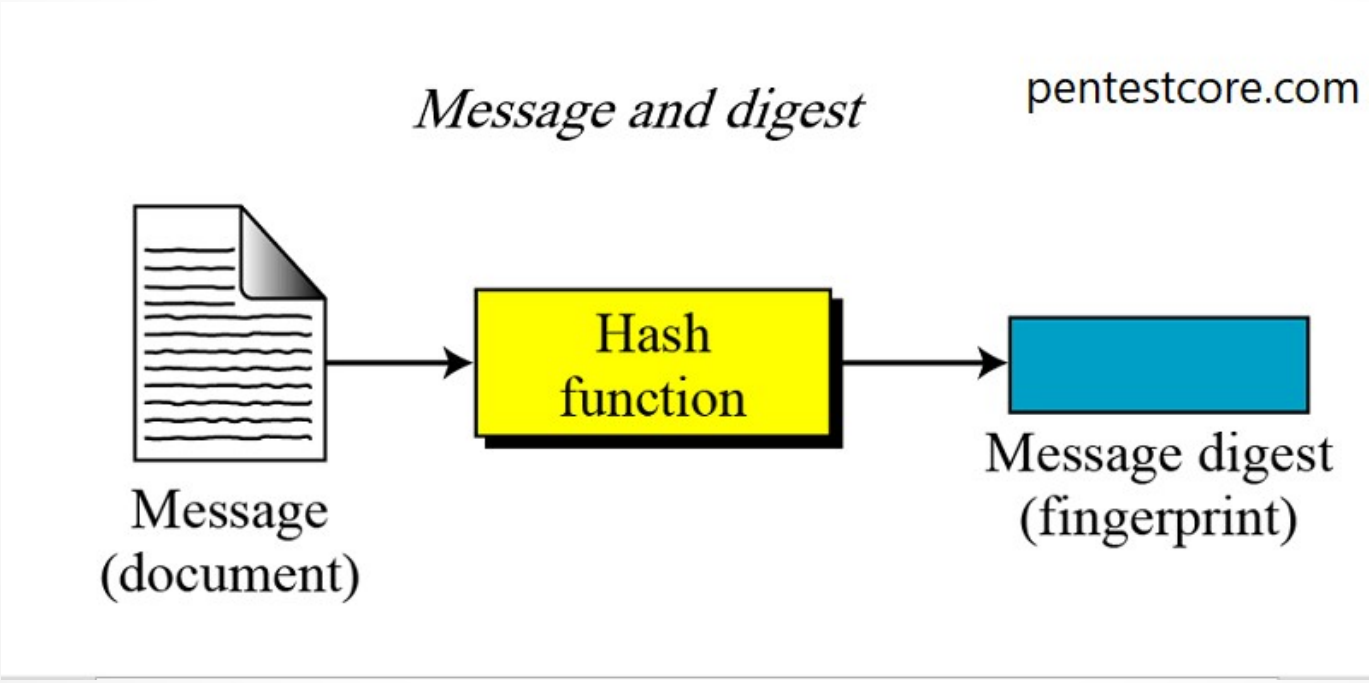
RSA

ElGamal

...

هش -hash

الگوریتم هش اطلاعات را در هر اندازه ای(عدد، حروف، فایل های رسانه ای) دریافت کرده و آنها را به یک رشته از اعداد و حروف ثابت تبدیل می کند. این اندازه بیت ثابت می تواند متفاوت باشد(مثل ۶۴ بیت یا ۱۲۸ بیت یا ۲۵۶ بیت). این اندازه بستگی به تابع هش مورد استفاده دارد.



هش -hash

ویژگی ها:

- قطعی بودن
- محاسبه سریع
- غیر قابل بازگشت بودن

INPUT	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

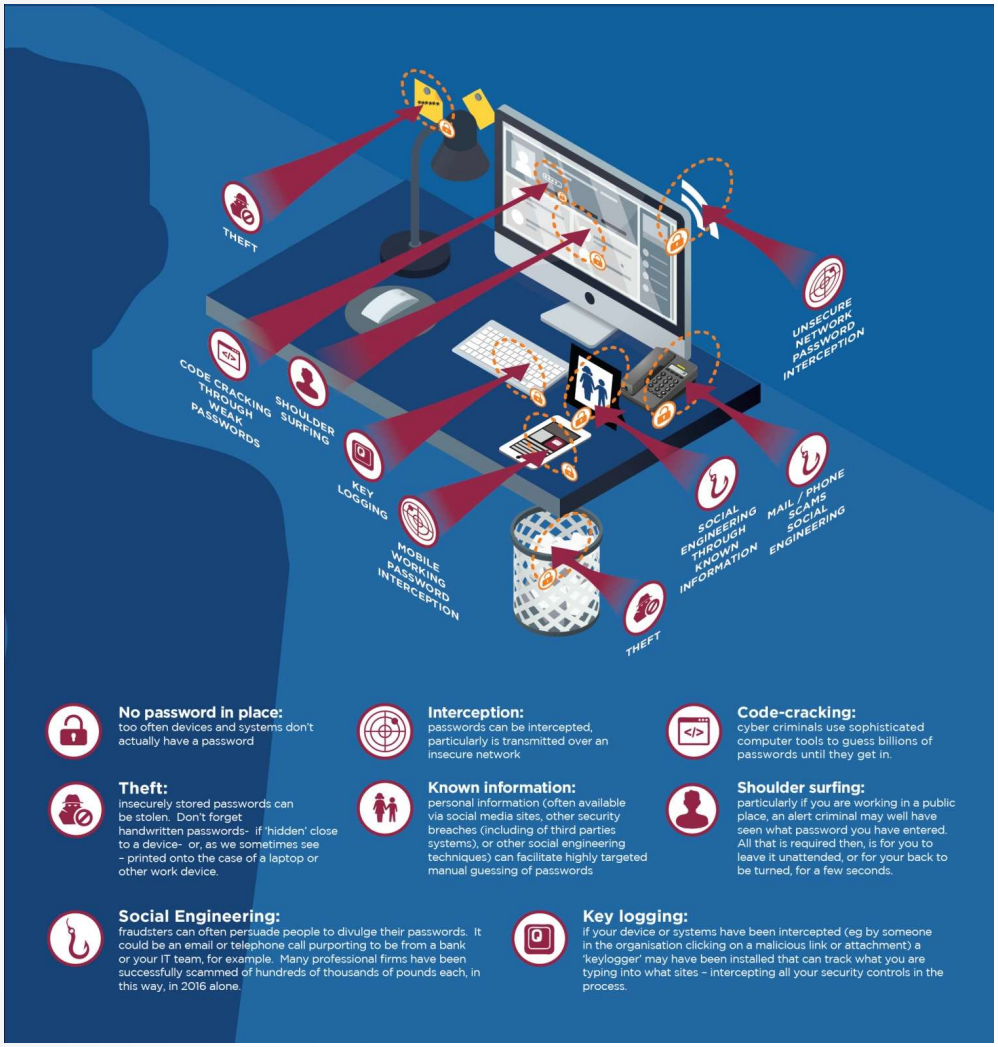
- تغییر کوچک در ورودی، هش را تغییر می دهد

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

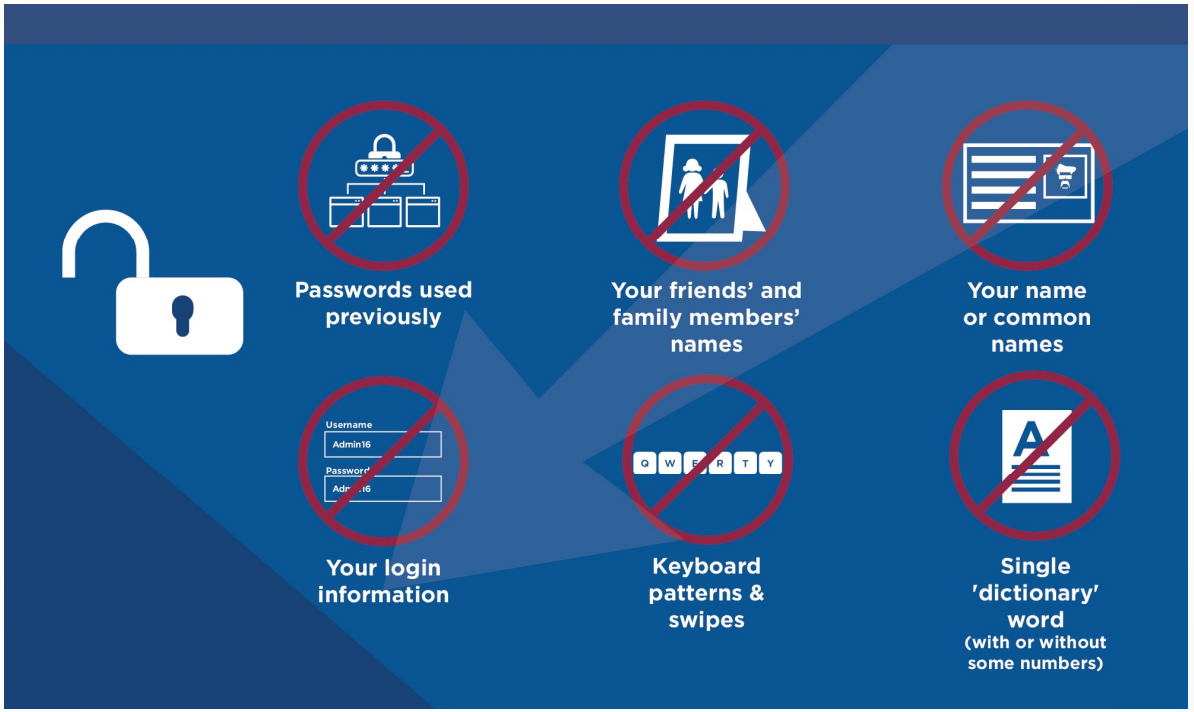
امنیت اطلاعات برای کارکنان سازمان

- ✓ استفاده از کلمات عبــور قــوی و حفاظــت ازآن ها؛
- ✓ قوانین مربوط به دسترسی ایمن از راه دور به شبکه شرکت(ریموت به شبکه شرکت)؛
- ✓ دانلود کردن برای استفاده شخصی (با توجه به بحث هزینه و پهنای باند)؛
- ✓ عدم ارسال مطالب محرمانه یا ایمیل. ارسال مطالب حساس و مهم باید به‌صورت رمزنگاری‌شده باشد؛
- ✓ سهواً یا عمداً دانلود کردن نرم‌افزارهای مخرب؛
- ✓ نشت دسترسی غیرمجاز به اطلاعات مهم و حساس؛
- ✓ استفاده ایمن و مسئولانه از ایمیل؛
- ✓ حفظ اطلاعات محرمانه سازمان؛
- ✓ دسترسی غیرمجاز به اطلاعات مهم و حساس؛

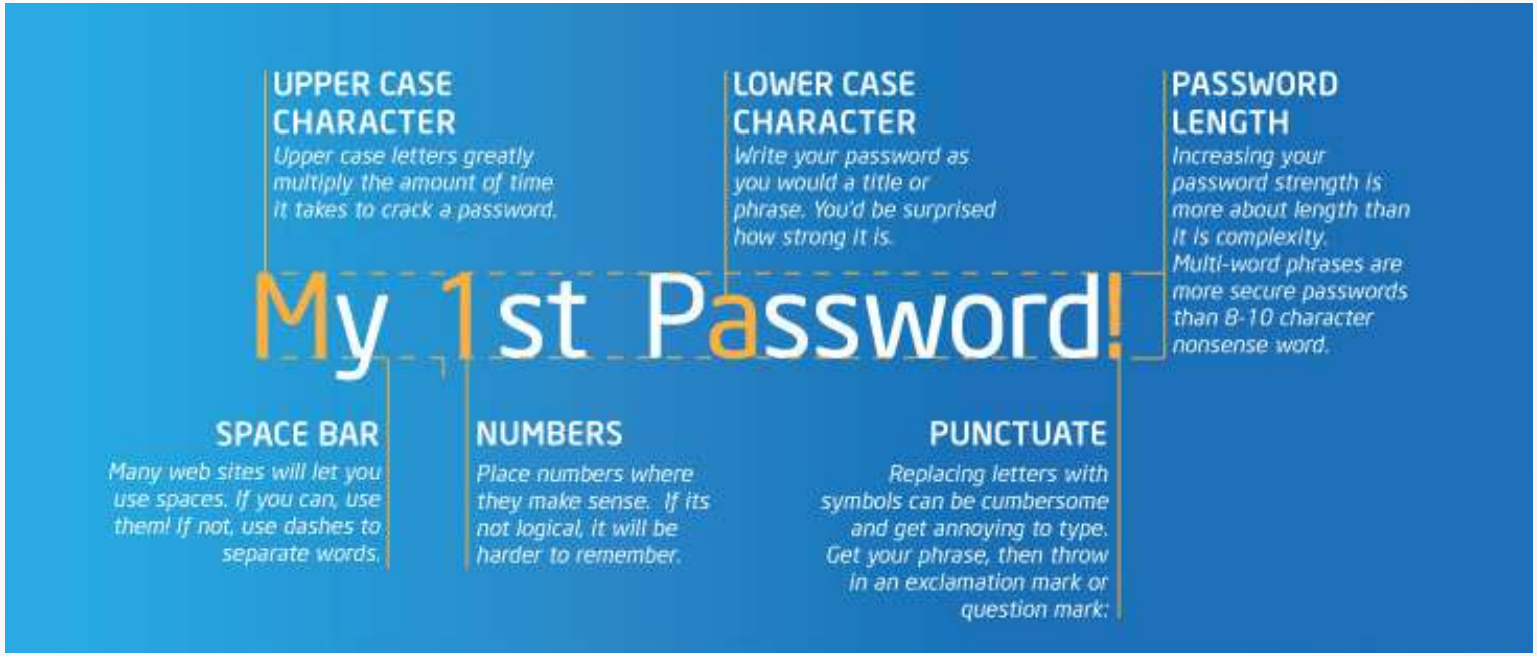
نکات پر مخاطره در استفاده از پسورد



ویژگی های یک پسورد ضعیف



ویژگی های یک پسورد قوی




مرکز ملی
امنیت سایبری
۱۰ قدم تا
امنیت سایبری
سازمان ملی امنیت سایبری ۱۰ قدم زیر را
برای افزایش امنیت سایبری شما و
شرکتتان پیشنهاد می‌دهد.
مدیریت دسترسی‌های کاربر
دسترسی‌های کامل را محدود کنید.
فعالیت‌های کاربران را مانیتور کنید.
برای کاربران مختلف دسترسی‌های
متفاوت و محدود ایجاد کنید.
مدیریت حادثه
برای بعد از وقوع رخداد
یا حادثه برنامه و سیاست
داشته باشید. برنامه خود
را تست کنید.
جرایم را به مراجع قانونی
اطلاع دهید.
مانیتورینگ
یک روش مانیتورینگ و
سیاست پشتیبانی برای
خودتان داشته باشید.
به صورت مرتب تمام شبکه و سیستم‌ها را
مانیتور کنید. لاگ‌ها و فعالیت‌های غیر
معمول را بررسی کنید.
آزاد کاری
سیاست کار از راه دور داشته
باشید. کارمندانتان را آموزش
دهید که به آن پایبند باشند.
از داده‌ها در ارسال و دریافت
محافظت کنید.
امنیت شبکه
شبکه را نسبت به حمله‌ها امن
کنید. شبکه را مانیتور کنید و
تست‌های امنیتی را انجام دهید.
بالا بردن دانش و آگاهی کاربران
حتما یک سیاست برای کارمندانتان
داشته باشید تا سیستمشان را امن
نگاه دارند. مطمئن شوید که ایشان
را نسبت به تهدیدهای سایبری
آموزش دهید.
جلوگیری از بدافزار
سیاست‌های امنیتی
مربوطه را وضع کنید و
آنتی بدافزار نصب کنید.
کنترل حافظه‌های خارجی
حتما سیاستی برای کنترل و دسترسی
های حافظه‌های خارجی وضع کنید.
قبل ار اتصال این حافظه‌ها به کامپیوتر
حتما آنها را با آنتی ویروس بررسی
کنید.
تنظیمات امنیتی
باگ‌های امنیتی را پچ کنید و
تنظیمات امنیتی کل سیستم را
ست کنید
مدیریت ریسک
سیاست‌های مدیریت ریسک داشته باشید
امنیت سایبری را در الویت قرار دهید
ریسک را ارزیابی کنید
For more information go to www.ncsc.gov.uk @ncsc
ترجمه توسط تیم فنی کنش‌تک - https://koneshtech.academy