

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

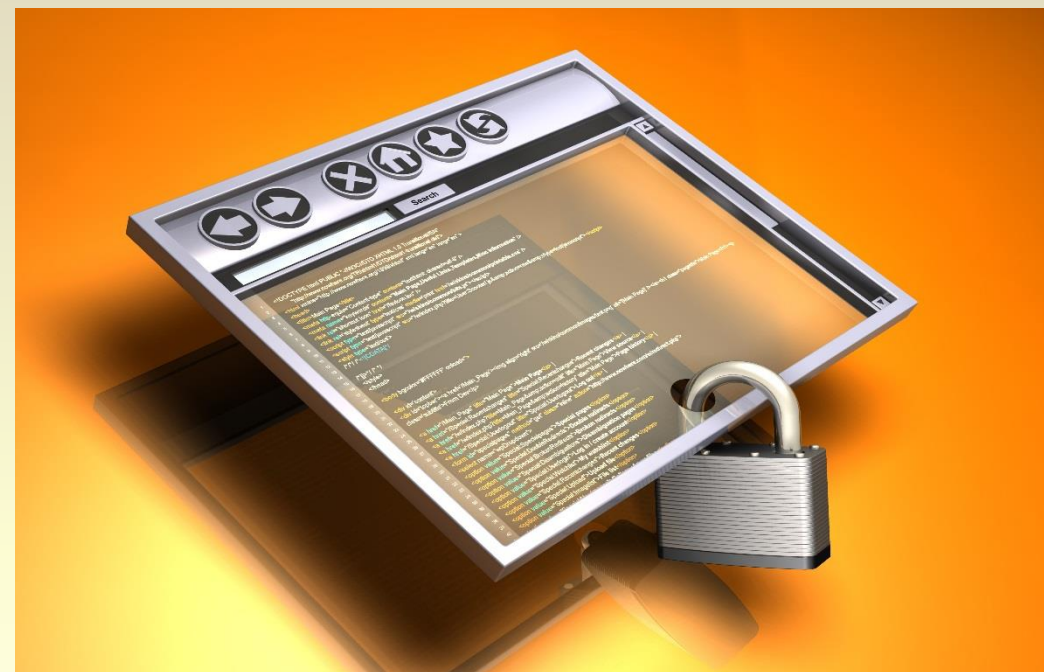


# امنیت فناوری اطلاعات و ارتباطات؛ ضرورت‌ها و روندها

احسان طیرانی راد

مدیر آموزش و روابط عمومی آزمایشگاه تخصصی آپا  
دانشگاه فردوسی مشهد

سمینار آموزشی مدیران و کارشناسان فناوری اطلاعات و ارتباطات استان آذربایجان غربی - ۲۶ مرداد ۱۳۹۵



امام صادق علیه السلام:

راز و اسرار تو به منزله‌ی خون توست، پس سعی کن که جز  
در شاهرگ‌هایت به جریان نیفتند.

# امنیت فناوری اطلاعات و ارتباطات

مفاهیم

# عصر اطلاعات

- نقش فزاینده اطلاعات در جهان امروز
- پیشرفت سریع فناوری‌ها، رشد و توسعه علوم به واسطه دسترسی همگانی به اطلاعات
- فناوری اطلاعات به عنوان عامل تغییر
- حیاتی بودن تولید اطلاعات، دانش و علم و اهمیت حفظ و نگهداری از آن‌ها در عصر اطلاعات

**اطلاعات و بهره‌گیری و تبدیل آن به دانش و خرد؛  
عامل مزیت رقابتی برای اشخاص، سازمان‌ها و ...**

# ویژگی‌های عصر اطلاعات

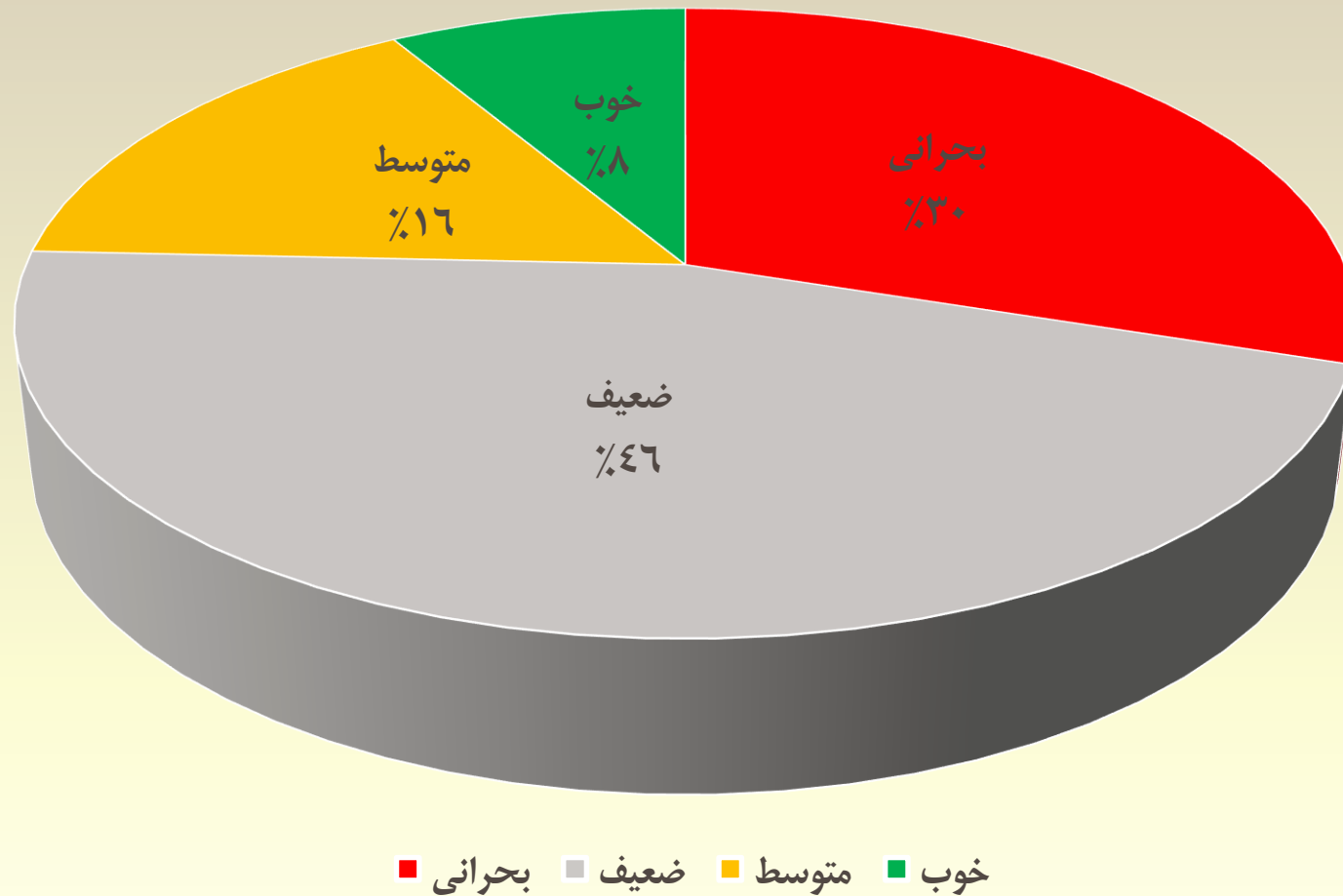
- اطلاعات، دارایی است
- سرمایه این عصر دارایی‌های نامشهود هستند (تحقیق و پژوهش، مهارت، دانش، فناوری و نوآوری)
- جامعه‌ای در این شرایط سرآمد است که بر اساس دانش و اطلاعات پایه‌ریزی شده باشد
- اکثر کسب‌وکارها بر اساس فناوری اطلاعات است و تاثیر بسیاری بر افزایش بهره‌وری فعالیت‌ها دارد

**بنابراین امنیت اطلاعات موضوعی حیاتی برای همگان است**

# برخی گزارش‌ها و تحلیل‌های امنیتی در سال‌های ۲۰۱۴ و ۲۰۱۵

وضع موجود

# نمونه گزارش آماری از وضعیت شبکه و زیرساخت در یک کره دیگر!!



# گزارش تحلیلی وضعیت همان شبکه همان کره دیگر!!

■ نقص در طراحی و عدم دانش فنی مناسب در پیکربندی

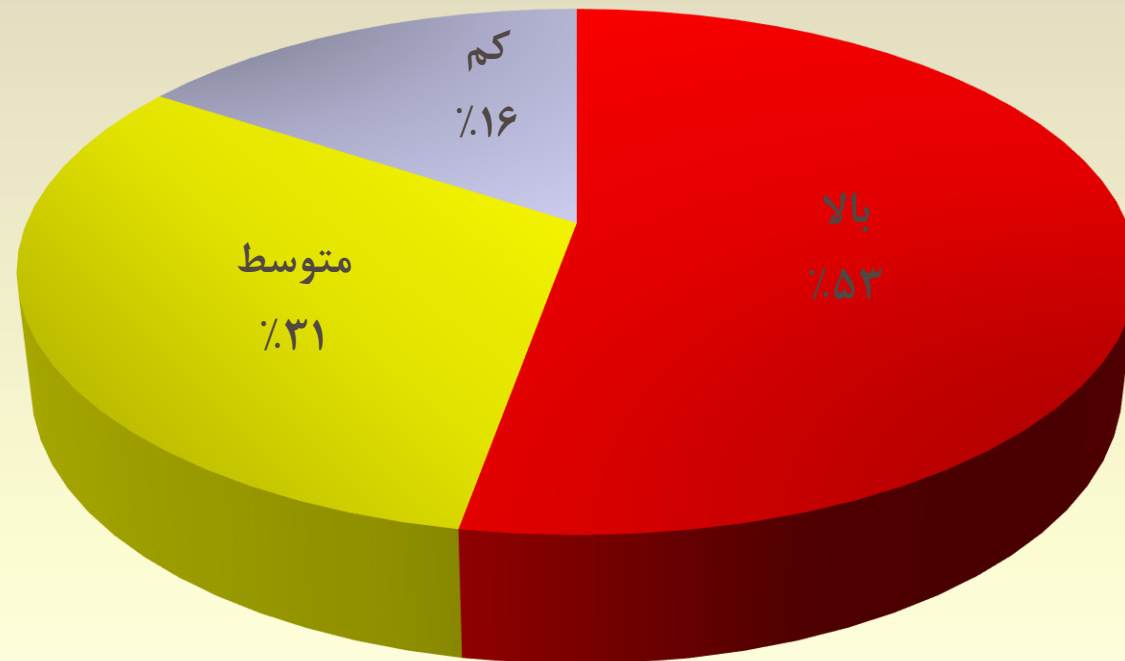
■ عدم استفاده بهینه از امکانات و تجهیزات

■ نبود امکانات، تجهیزات و زیرساخت‌های مناسب

■ عدم به کارگیری مشاوره‌ها و نظارت‌های فنی

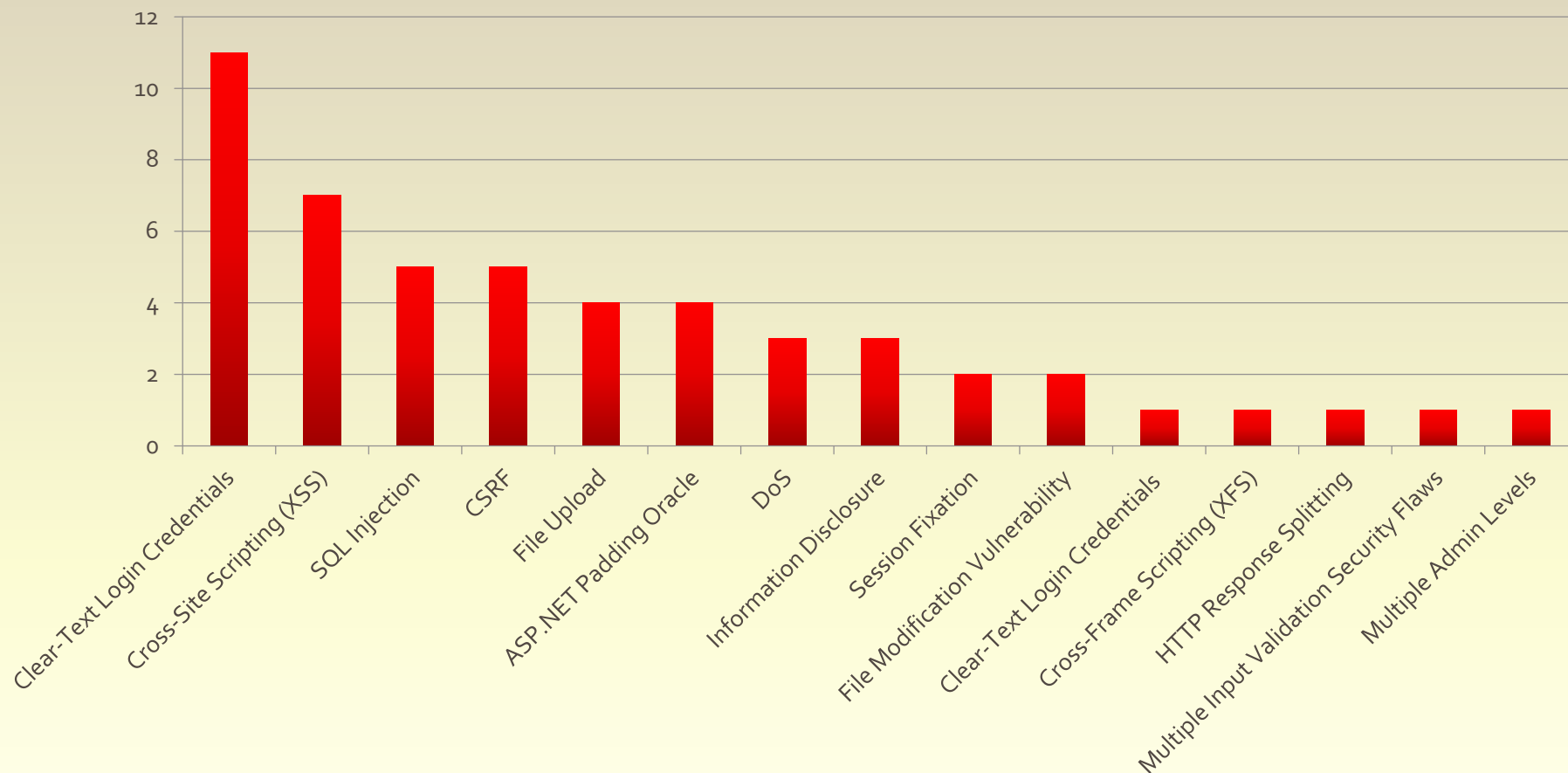
# نمونه گزارش وضعیت برنامه‌های کاربردی همان کره دیگر!!

سطح آسیب‌پذیری‌ها در پرتال‌ها و نرم‌افزارهای کاربردی



# گزارش تحلیلی وضعیت همان برنامه‌های کاربردی همان کره دیگر!!

پراکندگی آسیب پذیری‌های پرخطر کشف شده



# گزارش تحلیلی وضعیت همان برنامه‌های کاربردی همان کره دیگر!!

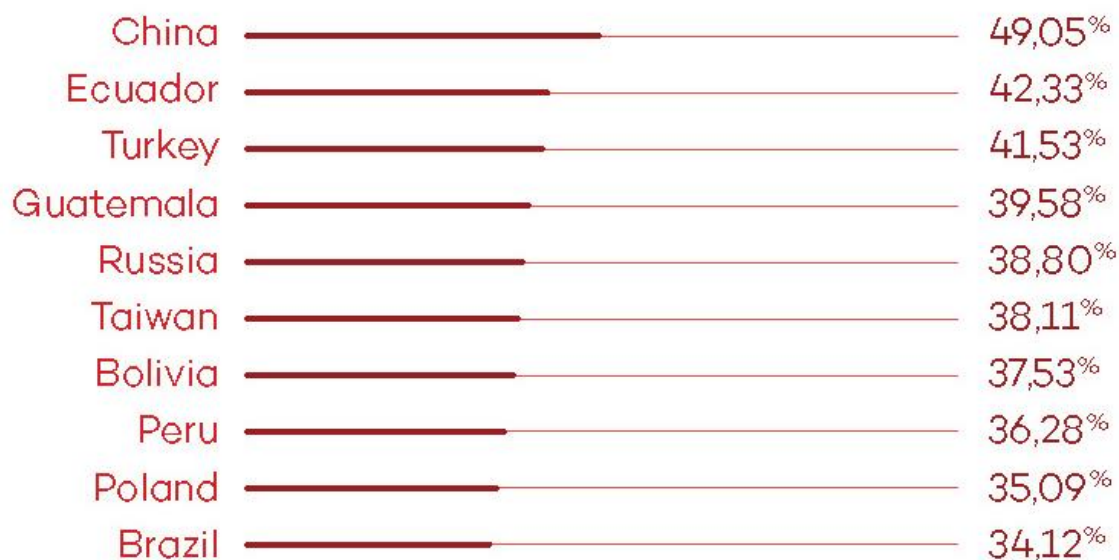
- عدم دانش امنیتی مناسب در تیم‌های برنامه‌نویسی
- صرف زمان طولانی در رفع مشکلات امنیتی از سوی شرکت‌ها



# گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

■ فهرست ۱۰ کشور با بیشترین نرخ آلودگی در سال ۲۰۱۴

COUNTRIES WITH THE HIGHEST INFECTION RATES IN 2014



COUNTRIES WITH THE LOWEST INFECTION RATES



■ بالاترین موقعیتها در این فهرست متعلق به کشورهای آسیایی و کشورهای آمریکای لاتین است. در مقابل، اروپا

منطقه‌ای با پایین ترین نرخ آلودگی است.

# گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

یکی از مهمترین حمله‌های سایبری در سال ۲۰۱۵ مربوط به باج‌افزار و به‌طور خاص کریپتولاگر می‌شود.

این نوع حملات روی تمامی کاربران تاثیرگذار است، البته تاثیر آن روی شرکت‌هایی که اطلاعات با ارزشی نگهداری می‌کنند و حاضرند برای آن باج بدهند بیشتر است.



# گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

■ در ماه فوریه شرکت آمریکایی Anthem اعلام کرد که قربانی حمله‌ای شده است که طی آن اطلاعات ۸۰ میلیون کاربر آن دزدیده شده است.



■ حمله‌کنندگان با استفاده از یک نام و گذرواژه دزدی توانسته بودند به پایگاه داده شرکت دسترسی پیدا کنند و حدود ۱۰۰ میلیون دلار به این شرکت خسارت وارد کنند.

# گزارش امنیتی شرکت پاندا در سال ۲۰۱۵

- هنگامی که ما در مورد حملات سایبری صحبت می‌کنیم، معمولاً به کامپیوترها، گوشی‌های هوشمند و تبلت‌ها فکر می‌کنیم. در حالی که سایر دستگاه‌های سخت‌افزاری نیز می‌توانند تحت تأثیر این حملات قرار گیرند.
- یک نقص امنیتی در روترهای Linksys به مهاجمین اجازه می‌داد که عملیاتی مانند تغییر تنظیمات DNS روتر را انجام دهند.

# گزارش امنیتی شرکت پاندا در سال ۲۰۱۴

■ مدت کوتاهی پس از انتشار خبر گم شدن هواپیمای مالزی، مجرمان سایبری شروع به انتشار لینکی روی فیس بوک کردند که ادعا می کردند ویدیویی از این هواپیما است. اما هنگامی که کاربر روی این لینک کلیک می کرد، کلمه عبور از وی درخواست می شد و به این ترتیب حساب وی مورد سرقت قرار می گرفت. اندکی بعد همین ترفند روی توئیتر هم اجرا شد.

■ همین حملات به صورت ایمیلی نیز تکرار شدند. این ایمیل ادعا می کرد که حاوی آخرین مکالمات خلبان با برج مراقبت دقیقی پیش از قطع ارتباط برج با هواپیما است.



# گزارش امنیتی شرکت پاندا در سال ۲۰۱۴

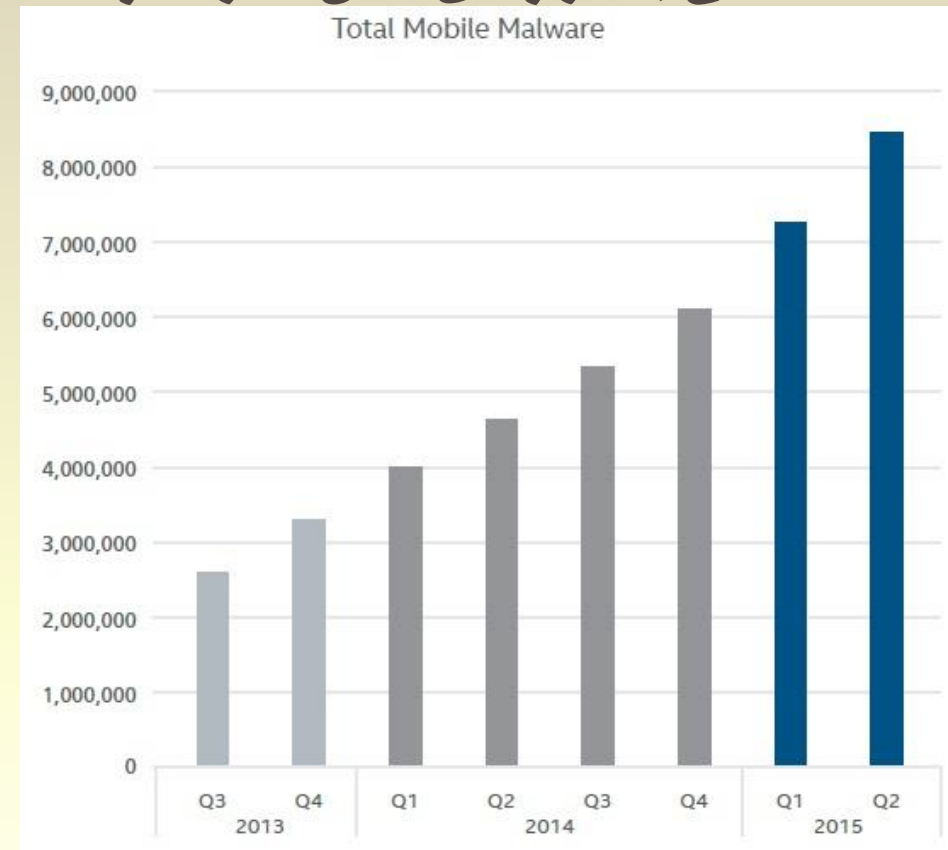
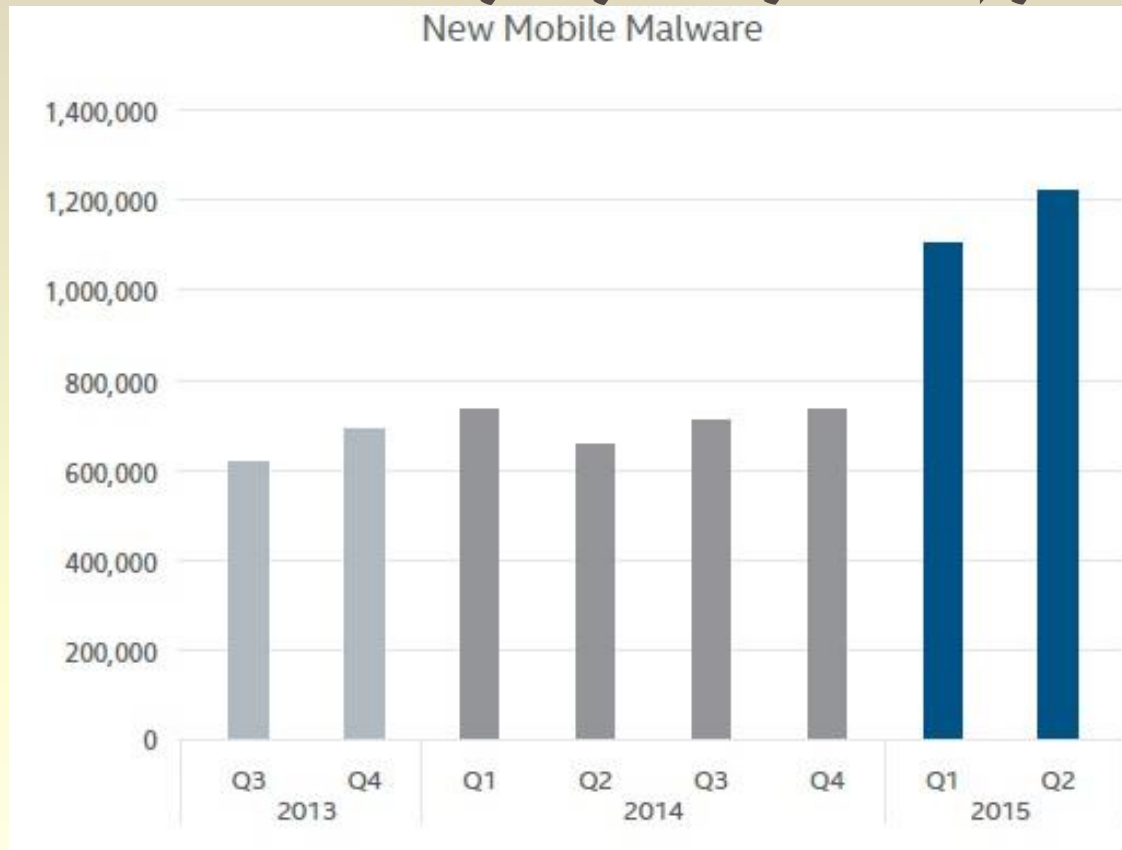
■ در حوزه بدافزارهای موبایل در سال ۲۰۱۴ و در ماه فوریه پاندا چهار برنامه بدافزار در گوگل پلی کشف کرد. این برنامه‌ها که موضوعاتی مانند رژیم غذایی و مدل مو داشتند، کاربر را در سرویس‌های پولی ثبت‌نام می‌کردند و حتی اس‌ام‌اس‌های دریافتی از این سرویس‌ها را نیز پنهان می‌کردند تا کاربر تا زمان دریافت صورتحساب تلفن خود، متوجه موضوع نگردد. این برنامه‌ها در طول مدت یک ماه بین ۳۰۰ هزار تا ۱ میلیون و ۲۰۰ هزار مورد دانلود داشتند.



■ در حمله مشابهی به جای گوگل پلی، مهاجمان صفحه‌ای مشابه آن طراحی کرده بودند و با تبلیغات در فیس بوک، کاربران را به آنجا می‌کشاندند.

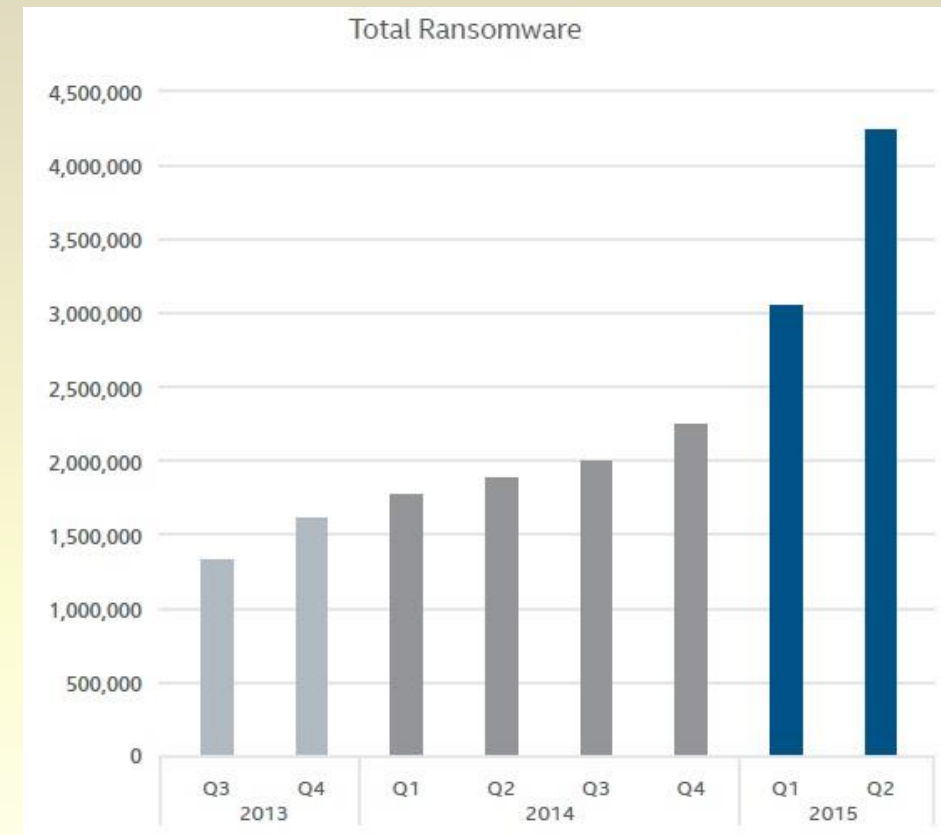
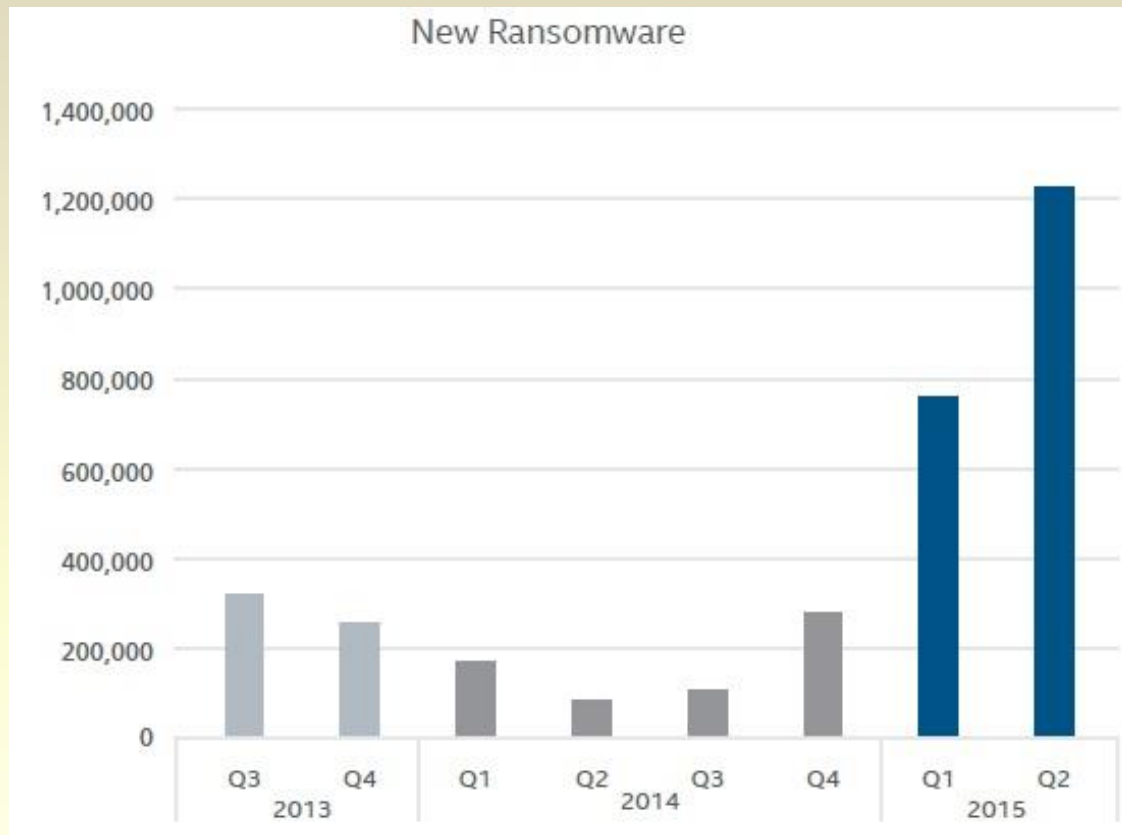
# گزارش امنیتی شرکت مک‌آفی در نیمه اول سال ۲۰۱۵

تعداد کلی بدافزارهای تلفن همراه در سه ماهه دوم سال حدود ۱۷ درصد رشد داشته است.



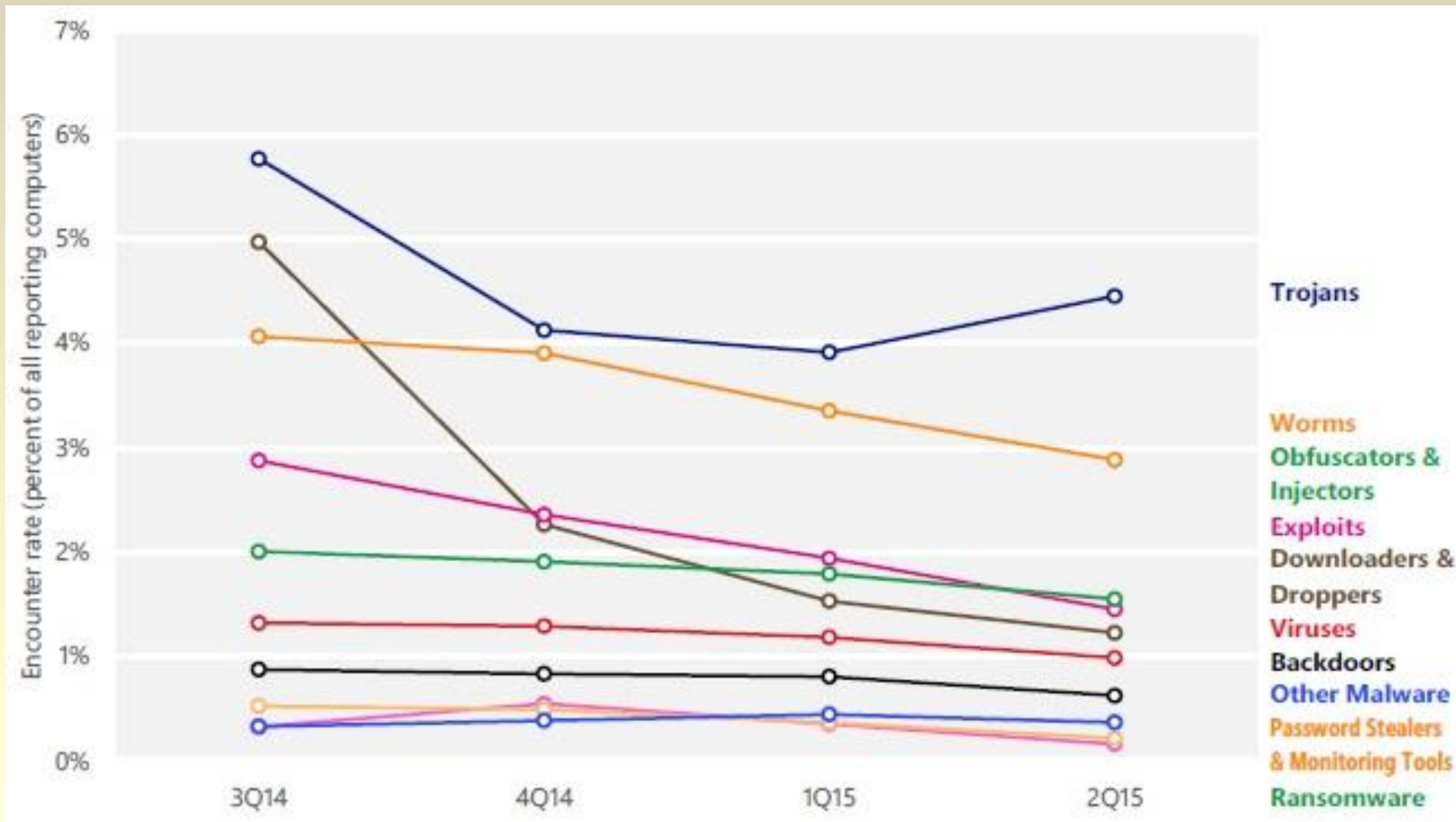
# گزارش امنیتی شرکت مک‌آفی در نیمه اول سال ۲۰۱۵

تعداد بدافزارهای گروهان‌گیر در سه ماهه دوم سال ۲۰۱۵، ۵۸ درصد افزایش یافته است.



# گزارش امنیتی شرکت مایکروسافت ۲۰۱۴-۲۰۱۵

## ■ طبقه‌بندی تهدیدات



# تهدیدهای امنیتی در گوشی‌های هوشمند و تبلت‌ها

■ شرکت Bit9 بیش از ۴۰۰ هزار اپلیکیشن را در گوگل پلی مورد ارزیابی قرار داده است:

■ ۷۲ درصد از تمام اپلیکیشن‌های اندروید یعنی حدود ۲۹۰ هزار برنامه، دست کم به یک اجازه نامه بسیار خطرناک دسترسی دارند.

■ ۲۱ درصد (بیش از ۸۶ هزار برنامه) به بیش از ۵ مورد پرمیشن خطرناک یا بیشتر دسترسی دارند.

■ ۲ درصد یعنی بیش از ۸ هزار اپلیکیشن به ۱۰ مورد اجازه نامه یا بیشتر دسترسی دارند که خطرناک

هستند

**تعداد نرم‌افزارهای موجود در گوگل پلی و دیگر ارائه‌دهندگان بسیار بیشتر از این عدد است**



# تهدیدهای امنیتی در گوشی‌های هوشمند و تبلت‌ها

## ■ طبق گزارش شرکت Bitg :

- بسیاری از اپلیکیشن‌ها سطح دسترسی‌هایی را تقاضا می‌کنند که به قابلیت‌های آن‌ها ارتباطی ندارد.
- تعداد قابل توجهی از برنامه‌ها عنوان «شناخته شده» دارند. به طور مثال، از ۱۱۵ اپلیکیشنی که دو کلمه Angry و Birds را در عنوان خود دارند، فقط ۴ اپلیکیشن هستند که به کمپانی Rovio Mobile تولیدکننده رسمی اپلیکیشن Angry Birds تعلق دارند. در میان آن‌ها، Angry Birds Live Wallpaper دو برابر بیشتر از برنامه اصلی بازی پرندگان خشمگین تقاضای دسترسی به سیستم کاربر را دارد. به طور مثال، این برنامه تقاضای دسترسی به اطلاعات جی‌پی‌اس را دارد که هیچ ارتباطی به کاربردش ندارد.

# گزارش سالانه امنیتی شرکت سیسکو - ۲۰۱۵

- کاربران فقط هدف نیستند بلکه همدستی توانا برای فراهم کردن ایجاد یک حمله به حساب می آیند.
- مهاجمین در استفاده از رخنه های امنیتی جهت پنهان سازی فعالیت های مخرب خود ماهرتر شده اند.
- حجم هرزنامه ها از ژانویه تا نوامبر ۲۰۱۴ میلادی، ۲۵۰ درصد افزایش داشته است.
- سازندگان بدافزارها از افزونه های مرورگرها به عنوان یک ابزار جهت توزیع بدافزارها و برنامه های ناخواسته استفاده می کنند.
- اکنون زمانی است که سازمان ها باید به طور متفاوتی به روند امنیت بنگرند تا بتوانند به صورت واقعی سازمان هایشان را بیشتر امن سازند.

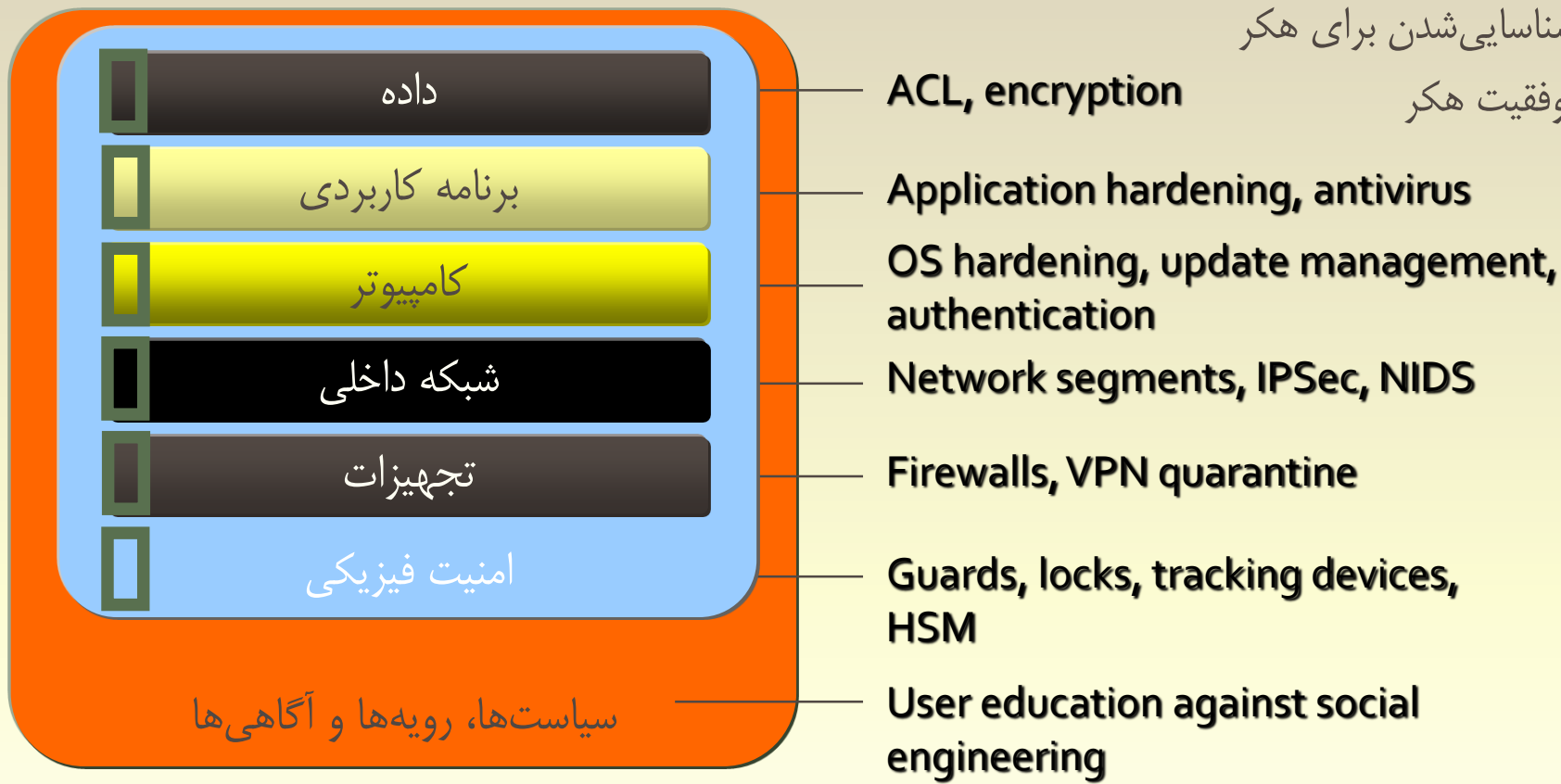
# امنیت در فضای مجازی

تهدیدها، اهداف حملات، لایه‌های امنیت، ابزارها و سیاست‌ها

# دفاع در عمق

## ■ استفاده از رویکرد لایه‌ای

- افزایش ریسک شناسایی شدن برای هکر
- کاهش احتمال موفقیت هکر



# تهدیدهای کلی فضای مجازی



■ تخریب و انهدام

■ تحریف و انحراف

■ ربایش و ازاله

■ افشا

■ قطع و وقفه

# اهداف حملات سایبری

## ■ اهداف سیاسی

- تضعیف دولت‌ها (با حمله سایبری به زیرساخت‌های حساس و حیاتی)

## ■ اهداف اقتصادی

- ضربه زدن به رقبا
- کسب اطلاعات رقبا
- کسب درآمد از طرق نامشروع

## ■ اهداف شخصی

- انتقام‌جویی (خصومت‌های شخصی یا نارضایتی کاری)
- اثبات و بروز توانمندی‌ها

# لایه‌های امنیت فضای تبادل اطلاعات

- امنیت شخصی
- امنیت فیزیکی
- امنیت اطلاعات
- امنیت عملیات
- امنیت شبکه
- امنیت ارتباطات



# ابزارهای تحقق امنیت فناوری اطلاعات

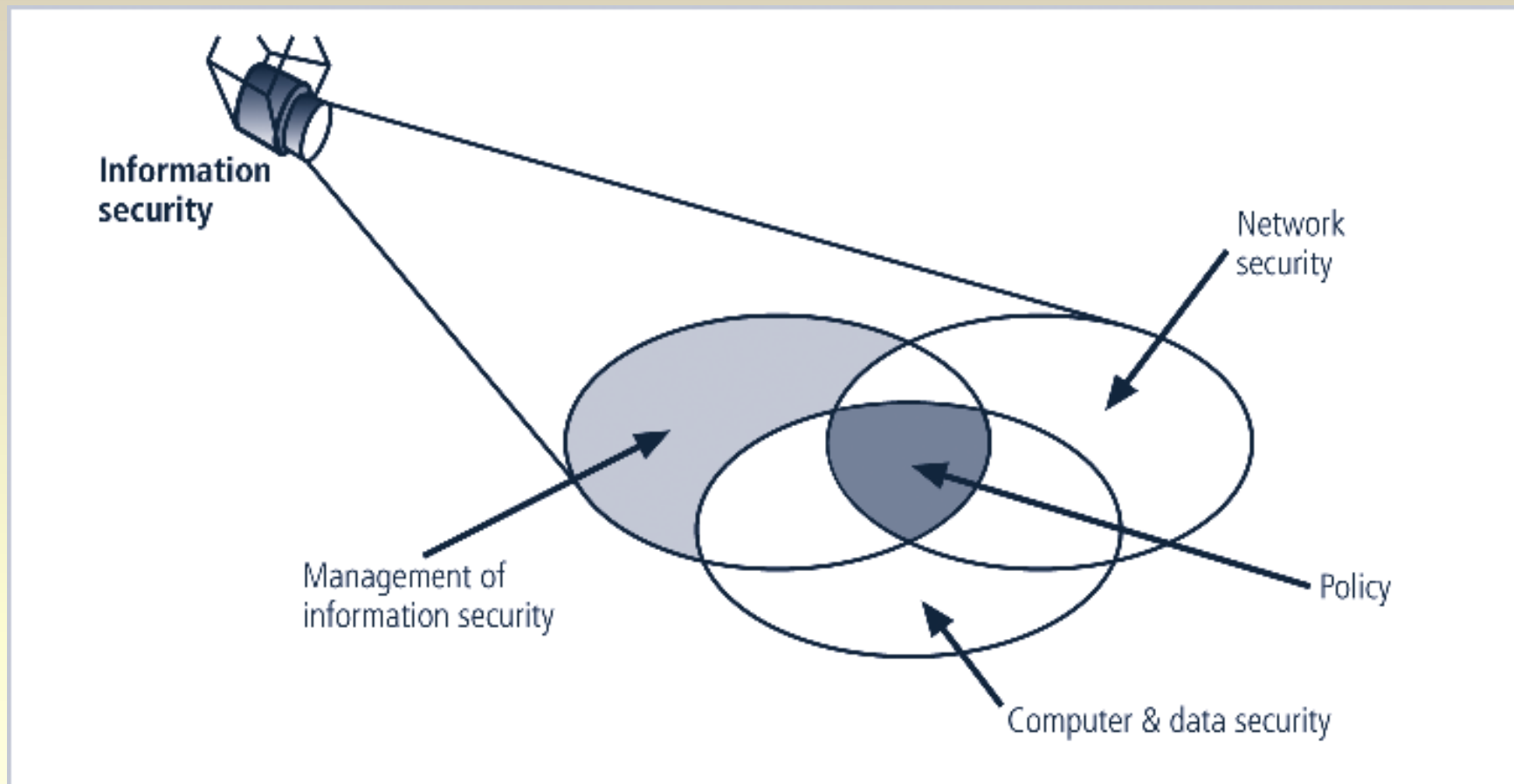


- سیاست
- آگاهی
- آموزش
- فناوری

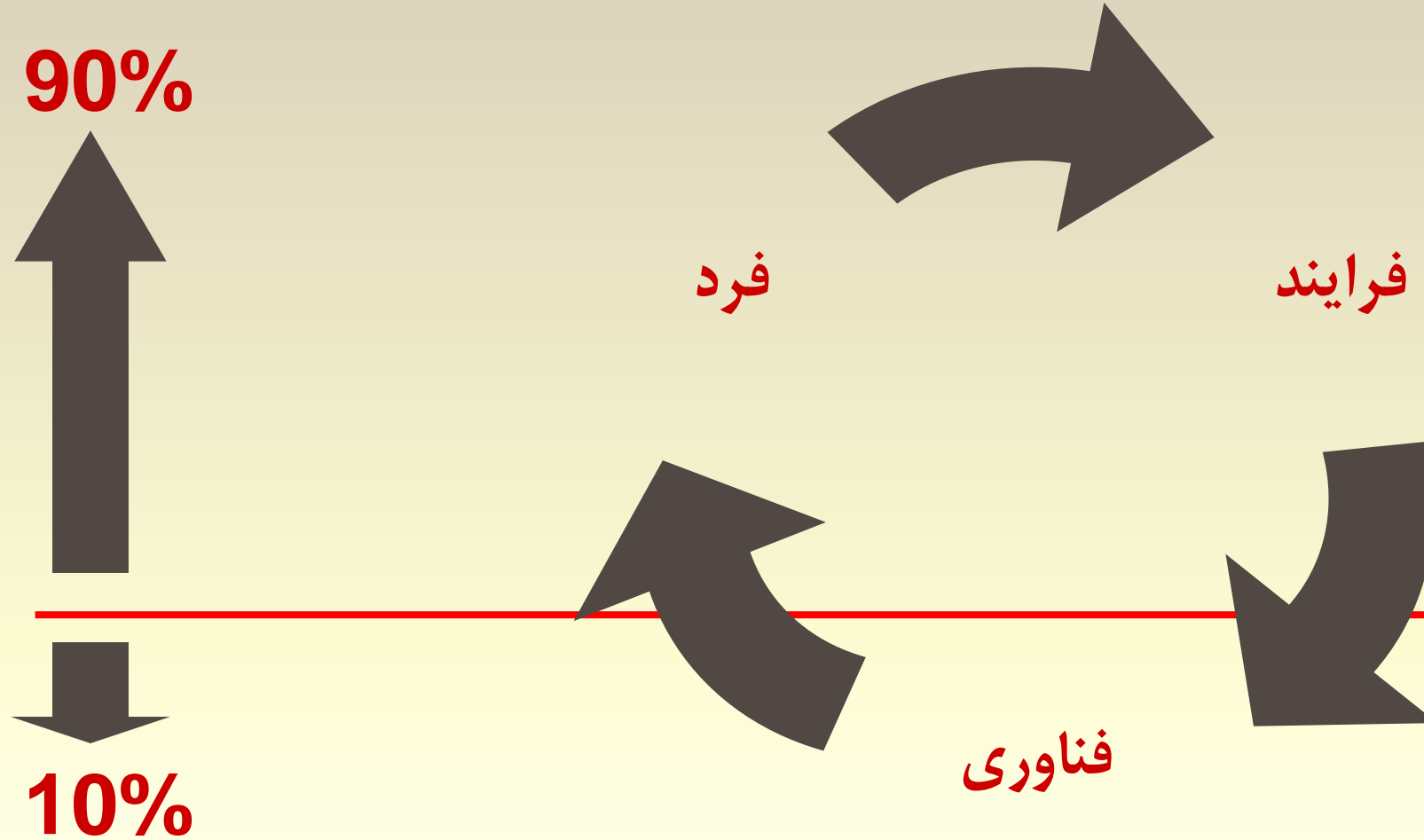
# توازن در برقراری امنیت فضای تبادل اطلاعات

- توازن امنیت اطلاعات و دسترسی
- دست یافتن به سطح کامل امنیت در فناوری اطلاعات و ارتباطات ممکن نیست.
- برای برقراری سطح مطلوب امنیت اطلاعات باید تعادل مناسب بین حفاظت و دسترسی‌ها ایجاد شود.

# امنیت فضای تبادل اطلاعات



# امنیت فضای تبادل اطلاعات



# نقش کاربران در امنیت فضای تبادل اطلاعات

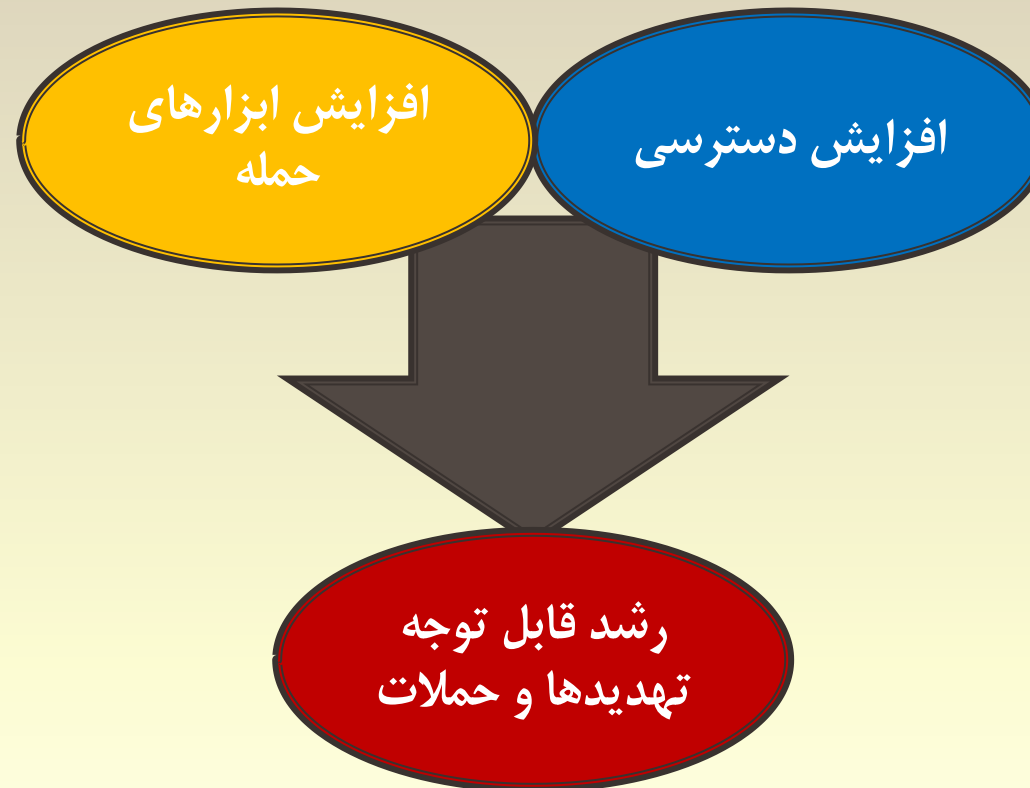
- در امنیت اطلاعات؛ بزرگ‌ترین دارایی افراد هستند و بزرگ‌ترین تهدید نیز افراد می‌باشند.



# روندهای امنیت فناوری اطلاعات و ارتباطات













روندهای تهدیدها و حملات

# رشد تهدیدها و حملات در فضای مجازی



# تهدیدهای فضای تبادل اطلاعات

## Highway of Threats

 UNAUTHORIZED ACCESS	 MOBILE DEVICE ATTACK	 SYSTEM COMPROMISE
 CYBER ESPIONAGE	 SOCIAL ENGINEERING	 SPAM
 MALWARE	 INSIDERS	 DENIAL OF SERVICE
 DATA LEAKAGE	 PHISHING	 IDENTITY THEFT

### Are you Vulnerable?

Copyright 2009 MindfulSecurity.com The Awareness Resource All Rights Reserved.

# منشا خطاهای احتمالی در کاربری

- خطاهای ناشی از نبود دانش
- خطاهای ناشی از نبود تجربه
- خطاهای ناشی از آموزش نادرست
- خطاهای ناشی از پیش فرض‌های نادرست

# در فضای مجازی، آن چه می بینید، تمام واقعیت نیست

## A WOLF IN SHEEP'S CLOTHING



# ساده‌شدن حملات



**SO EASY A BABY  
CAN HACK IT.**

Protect Your Computer. Get **FREE**  
password tips and antivirus software  
[oit.wvu.edu](http://oit.wvu.edu)

The advertisement shows a baby in a blue onesie crawling on a white surface and interacting with a black laptop. The laptop has the 'West Virginia University' logo on the lid. The scene is set against a grey brick wall with two black light fixtures.

# شبکه‌های اجتماعی؛ فرصت و تهدید



# روندهای امنیت فناوری اطلاعات و ارتباطات



■ اینترنت اشیا (IoT)؛ ملاحظات امنیتی، حقوقی و غیره

■ تدوین مقررات حفاظت از اطلاعات در اروپا

■ افزایش حملات هدفمند به سازمان‌ها و شرکت‌ها به منظور سرقت اطلاعات

■ با اعمال این مقررات از سال ۲۰۱۷، مسوولیت سازمان‌ها و شرکت‌ها در قبال امنیت اطلاعات افزایش می‌یابد.



# روندهای امنیت فناوری اطلاعات و ارتباطات



■ تمرکز نفوذگران به تلفن‌های هوشمند، رایانه‌های همراه و ...

■ با توجه به مخاطرات این حوزه، سازمان‌ها و شرکت‌ها، رویکرد کارمندمحوری را در زمینه امنیت اطلاعات برگزیده‌اند.

■ شکاف عمیق در دانش و مهارت جهانی در حوزه امنیت

# روندهای امنیت فناوری اطلاعات و ارتباطات



■ امنیت در سامانه‌های کنترل صنعتی

■ تمرکز بر سیاست‌های پاسخ به حملات در کنار

سیاست‌های پیش‌گیرانه

# روندهای امنیت فناوری اطلاعات و ارتباطات

■ امنیت سامانه‌های پردازش ابری



■ داده‌های بزرگ؛ الزامات امنیتی در نرم‌افزارها و کاربردها

■ نگرانی از امنیت داده‌ها در سال ۲۰۱۵ تاثیر منفی در نوآوری برخی سازمان‌ها و شرکت‌ها داشته است.

# روندهای امنیت فناوری اطلاعات و ارتباطات



■ تغییرات و ارتقای شبکه‌های اجتماعی

■ نرم‌افزارهای پیام‌رسان، نسل جدید شبکه‌های اجتماعی

# روندهای امنیت فناوری اطلاعات و ارتباطات



■ ادامه افزایش حملات بدافزارهای گروگان گیر



■ ادامه تلاش دولت‌ها در انجام حملات سایبری و

...

# روندهای امنیت فناوری اطلاعات و ارتباطات

## ■ افزایش روند BYOD ها و نگرانی از امنیت آنها



■ بر اساس آمارگیری از ۱۱۵۰۰ کارمند در ۲۳ کشور مشخص شده است که ۸۷ درصد آنها گمان می‌کردند بخش فناوری اطلاعات و ارتباطات از آنها در برابر تهدیدات محافظت می‌کنند.

■ ۳۱ درصد اذعان کرده‌اند که داده‌های آنها در تلفن همراهشان را از دست داده‌اند.

# روندهای امنیت فناوری اطلاعات و ارتباطات

- چالش های امنیتی در شبکه های نظارت تصویری
- یک شبکه کاملاً امنیتی با اهداف خاص
- گزارش ها و بازدیدهای فنی نشان داده است که این نوع شبکه ها از دانش فنی و نگرش امنیتی مناسبی در فرآیندهای زیر برخوردار نیستند:
  - طراحی شبکه و زیرساخت
  - پیکربندی و مدیریت
- القاء حس کاذب امنیت در این شبکه ها به دلیل:
  - جداسازی از شبکه مرسوم سازمانی!!
  - غفلت از سایر مولفه های امنیتی
  - عدم کارایی و قابلیت اطمینان در این نوع شبکه ها

# ضرورت‌های امنیت فناوری اطلاعات و ارتباطات

راهکارها

# نقاط ضعف در کاربری امنیت فناوری اطلاعات و ارتباطات

## ■ ضعف فناوری

- پروتکل، سیستم عامل، تجهیزات

## ■ ضعف تنظیمات

- رها کردن تنظیمات پیش فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه اندازی سرویس‌های اینترنت بدون اعمال تنظیمات لازم، ...

## ■ ضعف سیاست گذاری

- عدم وجود سیاست امنیتی
- عدم وجود طرحی برای مقابله و بازیابی مخاطرات
- نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

## ■ ضعف دانش و آگاهی

- عدم اطلاع از تنظیمات حریم خصوصی، نبود دانش کافی برای استفاده امن از شبکه‌های اجتماعی

# امنیت فناوری اطلاعات و ارتباطات؛ بایدها و نبایدها

- نگرش جامع به مسأله امنیت لازم است و نه فقط نگرش فنی و مقطعی.
- امن سازی به مراتب سخت تر از ناامن سازی است.
- امن سازی یک فرایند است (نه یک محصول و وظیفه خاص و مقطعی).
- امن سازی سیستم مستلزم سرمایه گذاری های جدی و زمان بر است.
- مادام که انسان ها امن فکر نکنند نمی توان سیستم امن داشت.

# اصول اولیه امنیت (بیانیه امنیتی سیسکو)

- امنیت باید موتور رشد شرکت در نظر گرفته شود.
  - امنیت هیچ‌گاه نباید مانع بازده و نوآوری شرکت شود.
- امنیت باید با معماری موجود کار کند و قابل استفاده باشد.
  - سازمان‌های برای اینکه با فناوری امنیت خود را سازگار کنند، نباید روش‌های کسب و کار خود را تغییر دهند.
- امنیت باید شفاف و آموزنده باشد.
  - کاربران باید اطلاعاتی در اختیارشان قرار داده شود که بفهمند چرا مسائل امنیتی مانع از انجام برخی اعمال می‌شود.
- امنیت باید قابلیت رؤیت باشد و انجام عمل مناسب را ممکن کند.
  - راه‌حل‌های امنیتی که دارای معماری امنیتی باز هستند تیم‌های امنیتی را قادر می‌سازند که بفهمند آیا این راه‌حل‌ها واقعاً مؤثر هستند.
- امنیت باید به عنوان راه حلی برای مردم در نظر گرفته شود.
  - هنگام مواجه شدن با مسائل امنیتی اتخاذ روشی که تمرکزش بر روی فناوری است امنیت را بهبود نمی‌بخشد؛ بلکه آن را بدتر می‌کند.

# چرخه ایجاد امنیت



# سرویس‌های امن سازی



# آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

معرفی خدمات و فعالیتها

# حوزه فعالیتها

- رسیدگی به حوادث: دریافت، تحلیل و پاسخ به حوادث رایانه‌ای و رخداد‌های امنیتی
- رسیدگی به آسیب پذیری‌ها: دریافت اطلاعات لازم در مورد وجود آسیب پذیری‌ها در شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، تحلیل ماهیت و اثرات آن‌ها
- اطلاع‌رسانی: گزارش آسیب پذیری‌ها و ارائه هشدارهای امنیتی
- آموزش: گسترش دانش در زمینه امنیت فناوری اطلاعات و ارتباطات
- مشاوره امنیتی: ارائه توصیه‌ها، راهنمایی‌ها و مشاوره‌های امنیتی به متقاضیان
- آزمون نفوذپذیری: ارزیابی امنیت شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری برای کشف آسیب پذیری‌های بالقوه و ارائه راهکارهای رفع آن‌ها

# خدمات

## ❑ آزمون نفوذپذیری

- ❑ شبکه‌های رایانه‌ای
- ❑ برنامه‌های کاربردی تحت وب
- ❑ پورتال‌ها
- ❑ سامانه‌های نظارت تصویری

## ❑ تدوین طرح امنیت جامع شبکه‌های رایانه‌ای

## ❑ صدور گواهینامه امنیتی برای نرم‌افزارهای کاربردی تحت وب

❑ OWASP ASVS 1A certificate

## ❑ برگزاری دوره‌های آموزشی تخصصی به صورت حضوری و مجازی

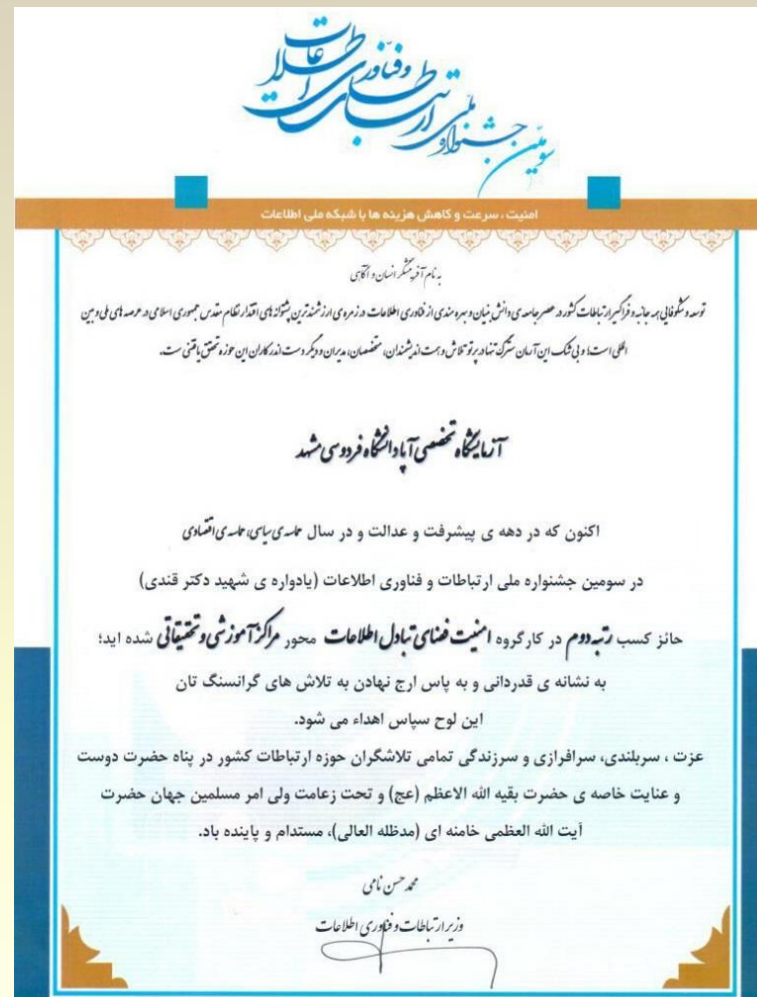
## ❑ فعالیتهای پژوهشی و تحقیقاتی

## ❑ انتشار دانش

# دستاوردها

- نهادینه‌سازی افتا و نظام آفا در مدیریت کلان استان خراسان رضوی
- آشنایی مدیران کلان و مدیران فناوری اطلاعات سازمان‌های اجرایی استان خراسان رضوی با اهمیت افتا و کارکرد آفا
- افزایش اهمیت امنیت اطلاعات در بین شرکتهای ارائه‌دهنده خدمات سخت‌افزاری و نرم‌افزاری و خدمات آفا به این شرکتهای
- آگاه‌نمودن بخشی از کارشناسان سازمان‌های اجرایی با اهمیت افتا
- ایجاد انگیزه برای دانشجویان مهندسی کامپیوتر برای انتخاب گرایش‌های مرتبط با امنیت و ادامه تحصیل در این گرایش
- دعوت از آزمایشگاه تخصصی آفا دانشگاه فردوسی مشهد برای حضور در نمایشگاه‌های تخصصی فاوا و ارائه سمینارهای آموزشی مرتبط در آنها

# کسب رتبه از سومین جشنواره فناوری اطلاعات و ارتباطات



# برخی سازمان‌ها و دستگاه‌های که تاکنون با آنها قرارداد منعقد شده است

- استانداری خراسان رضوی
- استانداری خراسان شمالی
- سازمان فناوری اطلاعات ایران – مرکز ماهر
- اداره اطلاعات خراسان رضوی
- شهرداری تهران
- مرکز پدافند سایبری کشور
- اداره کل گمرکات استان خراسان رضوی
- اداره کل نوسازی، توسعه و تجهیز مدارس خراسان رضوی
- اداره کل تنظیم مقررات و ارتباطات رادیویی شمال شرق
- شرکت آب و فاضلاب شهری خراسان شمالی
- اداره کل هواشناسی خراسان رضوی
- شرکت توزیع نیروی برق خراسان رضوی
- شرکت توزیع نیروی برق مشهد
- آستان قدس رضوی
- موسسه فرهنگی هنری خراسان
- سازمان صنعت، معدن و تجارت استان خراسان رضوی
- و بیش از ۲۰ شرکت و سازمان خصوصی

# گزارش آماری عملکرد

- ارزیابی امنیتی و آزمون نفوذپذیری برنامه های کاربردی تحت وب  
■ بیش از ۱۵۰ مورد
- ارزیابی امنیتی و آزمون نفوذپذیری شبکه ها و زیرساخت  
■ بیش از ۵۰ مورد
- ارائه گواهی های امنیتی برنامه کاربردی تحت وب  
■ ۱۲ مورد
- ارائه مشاوره های تخصصی، ارائه طرح جامع شبکه و امنیت و استقرار  
■ بیش از ۱۰ مورد
- برگزاری دوره های آموزشی و تخصصی مرتبط  
■ بیش از ۵۰ دوره - بیش از ۱۵۰۰ ساعت

# گواهی نامه امنیتی برنامه‌های کاربردی تحت وب



## گواهی نامه

### CERTIFICATE

#### گواهی نامه امنیت برنامه‌های کاربردی تحت وب

گواهی می‌شود برنامه کاربردی تحت وب [Redacted] با مشخصات فنی پیوست، پس از نصب بر روی سرور و دانشجویان آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد و بر اساس تنظیمات انجام شده مورد ارزیابی امنیتی قرار گرفت و در تاریخ ۱۳۹۴/۴/۱۵ موفق به دریافت گواهی نامه امنیت برنامه‌های کاربردی تحت وب آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد شد.

این گواهی نامه بنا به درخواست [Redacted] و برای نسخه موجود در آزمایشگاه تخصصی آپا صادر شده است. بدیهی است اعمال هرگونه تغییر در کد برنامه و تنظیمات انجام شده نیازمند دریافت گواهی نامه جدید است. اشخاص حقیقی و حقوقی متقاضی استفاده از این برنامه کاربردی به منظور کنترل صحت گواهی نامه می‌توانند کد درج شده ذیل را در وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد به نشانی <http://cert.um.ac.ir/certificate> جستجو نمایند.

کد گواهی نامه : [Redacted]

دکتر محسن کاهانی  
مدیر آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد



این گواهی نامه با شماره ۶۹ در تاریخ ۱۳۹۴/۴/۲۴ در دبیرخانه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد ثبت شده است و با امضا و مهر برجسته آزمایشگاه معتبر می‌باشد.

## طراحی و پیاده‌سازی برنامه کاربردی آزمون کشف آسیب‌پذیری در برنامه کاربردی تحت وب

# وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

صفحه اصلی درباره ما تماس با ما ورود نسخه RSS

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

آزمایشگاه تخصصی آپا در زمینه امنیت فناوری، اطلاعات و ارتباطات. در آپا، فردوسی، فعالیت‌هایی از قبیل شناسایی تهدیدات رایانه‌ای، کشف آسیب‌پذیری‌ها، کمک به سازمان‌ها در هنگام بروز حملات و رخدادهای امنیتی، ارزیابی امنیتی و انجام آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای، ارائه طرح امنیت برای امن‌سازی شبکه‌ها، و خدمات آگاهی‌رسانی و آموزش عمومی و تخصصی مرتبط ارائه می‌شود.

دوره‌های آموزشی  
درخواست همکاری  
عضویت در سایت

اطلاعاتی‌ها  
گواهی‌نامه‌های صادره  
ثبت نام دوره‌های آموزشی

عنوان‌های برگزیده:  
کسب افتخار آزمایشگاه در سومین جشنواره ملی فاوا  
بررسی معماری سیستم عامل ویندوز (توابع API بومی ویندوز)  
جرم‌پایی شبکه

فهرست اصلی  
اخبار و رویدادها  
مقاله‌های علمی و آموزشی  
آسیب‌پذیری‌ها  
سوال‌های متداول  
ارسال نظر  
دریافت فایل  
گالری تصاویر

جستجو  
بگرد

پیوندهای مفید  
دانش‌آموختگان دانشگاه فردوسی مشهد  
مرکز اطلاعات آمار و امور رایانه‌ای  
دانشگاه فردوسی مشهد

اخبار و رویدادها  
انتشار دوباره به‌روزرسانی امنیتی Exchange 2010 تاریخ ارسال خبر: 24-09-1393  
Salesforce هم به پشتیبانی از مرورگر IEB پایان داد. تاریخ ارسال خبر: 22-09-1393  
ضرورت توجه کسب و کارها به تهدیدات سایبری تاریخ ارسال خبر: 20-09-1393  
اصلاحیه‌های مایکروسافت منتشر می‌شود. تاریخ ارسال خبر: 16-09-1393  
چگونه طعمه حملات Phishing بشویم؟ تاریخ ارسال خبر: 13-09-1393  
اقدامات پیشگیرانه برای جلوگیری از هک شدن تلفن همراه تاریخ ارسال خبر: 11-09-1393  
"مضاحبه" ای که در دسترس‌ساز شد. تاریخ ارسال خبر: 10-09-1393  
حمله‌ی هکرک موفق به رایانه‌های سنوپی تاریخ ارسال خبر: 08-09-1393  
جزئیات دیگری از فعالیت بدافزار Regin تاریخ ارسال خبر: 07-09-1393

اطلاعی‌ها  
کسب افتخار آزمایشگاه در سومین جشنواره ملی فاوا

سامانه ویکی  
آزمایشگاه تخصصی آپا  
دانشگاه فردوسی مشهد

# سامانه ويكي آزمائشگاه تخصصي آيا دانشگاه فردوسي مشهد

صفحه اصلی

امنیت شبکه های کامپیوتری و سامانه های نرم افزاری، موضوع جدیدی در حوزه فناوری اطلاعات و ارتباطات نیست؛ اما دغدغه تازه ای برای کاربران این حوزه به حساب می آید. امروزه همگام با پیشرفت فناوری های ارتباطی و گسترش شبکه های رایانه ای، امنیت فضای تبادل اطلاعات به یکی از دغدغه های اصلی مدیران، کارشناسان، دانش پژوهان و کاربران حوزه فناوری اطلاعات و ارتباطات تبدیل شده است. در پاسخ به این دغدغه گروه هایی به نام CERT1 یا CSIRT2 در دنیا تشکیل شده که آزمائشگاه آيا دانشگاه فردوسي مشهد نمونه ای از آن ها است.

گفتن

- صفحه اصلی
- تغییرات اخیر
- صفحه تصادفی
- همه صفحه ها

جمعه آزار

پیوندها به این صفحه

تغییرات مرتبط

صفحه های ویژه

نسخه قابل چاپ

پیوند یابید

آشنایی با پروتکل ها

- تحلیل بدافزارها
- تحلیل یویا
- تحلیل ایستا

- یزشکی قانونی شبکه
- معرفی روتس ها
- معرفی ابزارها

- امنیت سرویس های شبکه
- معرفی ابزارهای شبکه
- معرفی سرویس های شبکه
- دیواره آتش
- مایکروسافت
- لینوکس
- یزاکسی

# سامانه SOC آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

The screenshot shows a web browser window with the URL `https://cert.um.ac.ir/soc/index.php?f=users/YumAuth/login`. The page header features the university logo and the text "آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد". Navigation links include "ورود", "تماس با ما", "درباره ما", and "صفحه اصلی". A secondary navigation bar contains "سامانه مدیریت رویدادهای رایتهای" and "صفحه اصلی".

The main content area includes a "فهرست اصلی" sidebar with options: "ارسال رویداد", "ثبت نام", and "ارسال پیشنهادات". The central text reads: "ورود به سامانه", "آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد هماهنگ با فعالیتها و خدمات خود نسبت به طراحی و پیادهسازی سامانه مدیریت رویدادهای رایتهای اقدام نموده است. این سامانه با هدف آگاهی و پایش مستمر رخدادها و رویدادهای امنیتی فضای تبادل اطلاعات راهاندازی شده است و در آن فرایندهای عضویت کارشناسان آپا سازمانی (کارشناسان امنیت سازمانها و شرکتهای عضو) و اعلام رویدادها و رخدادها امنیتی فناوری اطلاعات و ارتباطات، و همچنین پیگیری و پاسخ به این رویدادها و رخدادها طراحی و پیادهسازی شده است. به منظور استفاده از امکانات سیستم ثبت نام کنید".

Below the text is a login form with two input fields: "نام کاربری\*" and "کلمه عبور\*", and a "ورود" button.

The footer contains the text "صفحه اصلی | تماس با ما | درباره ما | ورود" and "©2014 Ferdowsi University Of Mashhad".

# دوره آموزش مجازی آگاهی‌های امنیتی شبکه‌های رایانه‌ای

The screenshot shows a web browser window with the URL `http://cert.um.ac.ir/e-learning/content.php?cid=14`. The page title is "سامانه آموزش الکترونیکی آزمایشی AT". The course is titled "course1". Navigation buttons include "صفحه اصلی", "جستجو", "راهنما", "برو", "گالری عکس‌ها", "نقشه سایت", "شبکه اجتماعی", "ذخیره سازی فایل", "فرهنگ لغت", and "انجمن‌ها". The user is logged in as "apaiser student". The main content area displays a slide titled "دوره آموزشی آگاهی‌های امنیتی شبکه‌های رایانه‌ای" with a logo of a quill pen and the text "دانشگاه فردوسی مشهد" and "آزمایشگاه تخصصی آبا". The slide content includes:

- مسئولیت‌ها من در رابطه با امنیت اطلاعات
- برای حفاظت از اطلاعات چه باید کرد؟
- راهکارهای ایجاد محیط امن در سازمان

There is an illustration of a red puzzle piece forming a head profile with a lightbulb icon next to it. A sidebar on the right shows a table of contents with 7 items, where "اسلاید 5" is highlighted. Below the table of contents are sections for "کاربران متصل" (showing "apaiser student" and "میهن‌ان در لیست نیامده اند") and "انجمنی" (with a search box and radio buttons for "تمام کلمات" and "هر کلمه‌ای").

# از بذل توجهتان متشکرم

<http://cert.um.ac.ir>

[tayarani@um.ac.ir](mailto:tayarani@um.ac.ir)

