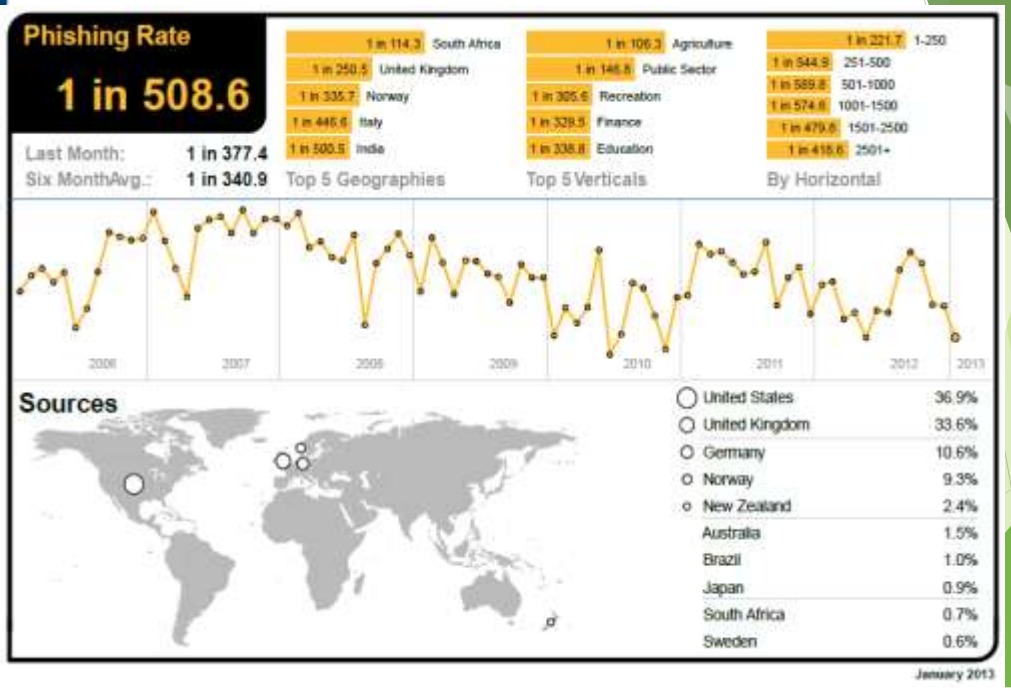
ارائه چارچوبی جهت ارتقاء استانداردهای امنیتی در سیستم بانکداری الکترونیک

عیسی جبارزاده

کارشناس بانک ملت،اداره کل فناوری اطلاعات (E.Jabbarzadeh@Bankmellat.ir)

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

conf.mbri.ac.ir/ebps3



ادبیات تحقیق

- بانکداری الکترونیک:

شامل ... جوه بین

یکپارچگی و صحت:کامل بودن و دقیق بودن اطلاعات و روشهای پردازش آن
دسترس پذیری:اطمینان از اینکه کاربران مجاز می توانند به اطلاعات دسترسی داشته باشند
محرمانگی:راز داری و امانت داری

داشته و تضمین کند که فقط افراد م

ادامه...

- اهداف ...

۱. پیشگیر...

۲.پیشگ...

۳.ح...

۴.ح...

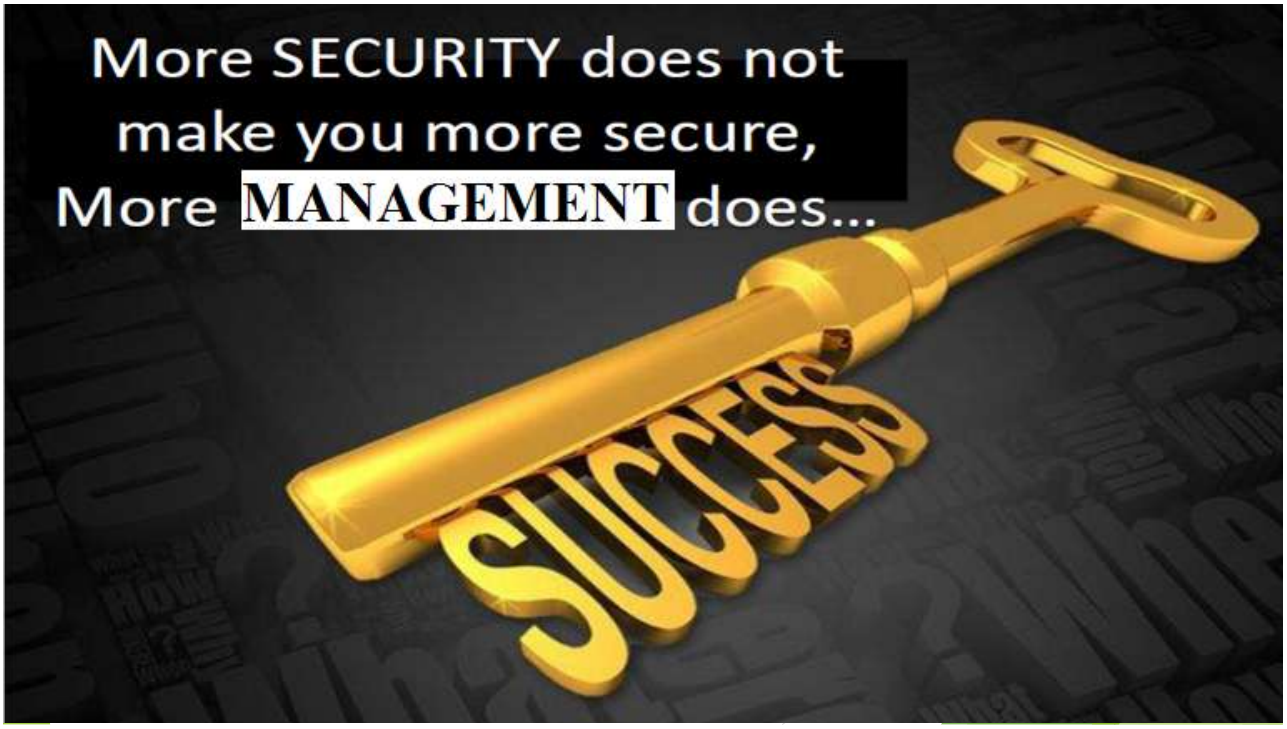
۵.عدم...

برای نیل به ...

(مشتری) طبق...

امنیت رسانه انتقال:
- پیشگیری ...

امنیت سمت کاربر:
- محافظت در برابر بدافزارهایی مانند Key logger، ویروس‌ها با استفاده از ضد بدافزارها
- مقابله با Phishing و حملات مبتنی بر مهندسی اجتماعی
- آگاهی‌رسانی و آموزش کاربر
- تصدیق اصالت چند عامله
- شاخص‌های امنیتی نرم‌افزار



تهدیدات و نفوذهای امنیتی

- **تهدیدات:(۱)**
  - ✓ تهدیدات ساختاریافته Structured Threats (فعال و غیر فعال)
  - ✓ تهدیدات غیر ساختاریافته Unstructured Threats(Virus, Worm, Trojan, Spyware, …)
- **تهدیدات: (۲)**
  - ✓ تهدیدات داخلی Internal Threats(پرسنل فرصت طلب،ناراضی و یا ناآگاه)
  - ✓ تهدیدات خارجی External Threats(رقبا، سارقین، جاسوسان و ...)
- **نفوذها:**
  - ✓ نفوذ به منظور شناسایی(نفوذ غیر فعال)
  - ✓ نفوذ به منظور دسترسی به اطلاعات(نفوذ فعال)
  - ✓ نفوذ به منظور از کار انداختن یک سرویس(نفوذ فعال) Denial of Service (DOS Attacks)

چالش های امنیتی

- بانکها علاوه بر مشکلاتی از قبیل تهدیدات امنیتی، عدم اعتماد مشتریان، هزینه ها و مشکلات نگهداری سایتها، موارد حقوقی و حفظ حریم شخصی مشتریان و ... در توسعه سیستم های بانکداری خود با چالش های دیگری نیز مواجه هستند که توجه به آنها موفقیت سیستم ها را پس از راه اندازی درپی خواهد داشت و عدم توجه به این چالشها منجر به تبدیل این چالشها به تهدید خواهد شد.

- ✓ تحریم های سیاسی و اقتصادی و ...
- ✓ عدم وجود زیر ساختهای مناسب ارتباطی و مخابراتی، تکنولوژیکی، فنی، امنیتی و ...
- ✓ عدم وجود قوانین ومقررات و روش ها(زیر ساختهای حقوقی)
- ✓ عدم وجود تخصص کافی در بین کارکنان
- ✓ عدم وجود انسجام با سایر کانالهای ارتباطی(تعارض کانالها)
- ✓ هزینه های پیاده سازی و استراتژی های قیمت گذاری تکنولوژی بانکداری الکترونیک
- ✓ فشار ناشی از واسطه ها
- ✓ عدم پشتیبانی مدیران عالی (وجود شکاف بین بانکداری سنتی و بانکداری نوین ودخالتهای غیر اصولی افراد)

تمهیدات امنیتی

- **ضعف فناوری**

پروتکل، سیستم عامل

دلایل مقاومت در مقابل ایمن سازی

- •هرچی پیش بیاد اشکالی نداره (بی خیالی)!!!
- •برای ما چیزی پیش نمیاد(خوشبینی)!!!
- •مشکل ما نیست بقیه مشکل دارند!!!
- •اطلاعات ما بدرد کسی نمی خوره!
- •هزینه ایمن سازی زیاده!!!
- •چه بخواهیم چه نخواهیم اونا یه

چرا برای ایمن سازی ضعف های امنیتی خود

البته مهم است بدانیم:

✓دفاع لایه لایه فراموش نشود!!!

کنیم!

مقدمات دفاع:

- ❑ساختار شبکه را اصلاح کنیم.
- ❑از Firewall استفاده کنیم.(با دقت!!!)
- ❑ ترافیک شبکه را کنترل نماییم.
- ❑ نفوذگران را گمراه و شناسایی کنیم.
- ❑ از رمزنگاری استفاده نماییم.
- ❑سیستم های تشخیص هویت
- ❑سرویس های FTP
- ❑ و...

ت لازم است.

ست.

اقدامات امنیتی در شبکه بانکی

- **روشهای حفاظت امنیتی که توسط بانک ها پیشنهاد می شود و مشتریان نیز انتظار آنها را دارند عبارتند از:**
- ✓ واضح و مشخص بودن آدرس دقیق وب سایت تائید شده موسسه پولی و مالی در نشریات بانک
- ✓ تائید و تصدیق وب سایت از طریق گواهینامه های دیجیتالی
- ✓ نمایش شواهد حفاظتهای امنیتی در صفحه نمایش (مثل آیکون قفل)
- ✓ حفاظت PINو رمز عبور
- ✓ استفاده از صفحه کلیدهایی با محرک موس یا لمسی برای اطلاعات حساس
- ✓ محافظت در مقابل ویروس ها
- ✓ رمزگزاری حداقل ۱۲۸ بیتی(کوتاه نبودن طول رمز)
- ✓ پیاده سازی دیوار آتش
- ✓ قرار دادن محدودیت برای مشتریانی که در وب سایت شناسائی نشده اند و محدودیت در دسترسی به کدها
- ✓ و ...

استانداردهای امنیت ISO/IEC 27001:2005

ISMS(Information Security Management System)

- ❖ موسسات SO بنام
- (ISM مبتنی

- براساس استاندارد ISO27001و درکنار سایر استانداردها از قبیل ISO9001 و تحت

استانداردISO27001 قالبی مطمئن برای داشتن یک سیستم مورد امنیتی قابل اعتماد می باشد.
تعدادی از فوائد پیاده سازی این استاندارد عبارتند از:

- •اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها
- •اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها
- •قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات
- •ایجاد اطمینان نزد مشتریان و شرکای تجاری
- •امکان رقابت بهتر با سایر شرکت ها
- •ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات
- •بخاطر مشکلات امنیتی اطلاعات و ایده های خود را در خارج سازمان پنهان نسازید
- •بومی سازی فرهنگ و دانش امنیت اطلاعات سازمان

ادامه

ISO27001

برنامه ریزی(Plan):
- ✓تعریف چشم انداز نظام مدیریتی و سیاست های امنیتی سازمان
- ✓تعیین و ارزیابی مخاطرات
- ✓انتخاب اهداف کنترل و آنچه برنامه ریزی مدیریت این

اجرا (Do):
- ✓تدوین و اجرای یک طرح برای تقلیل مخاطرات
- ✓اجرای طرح های کنترلی انتخابی برای تحقق اهداف کنترلی
- ✓اجرای برنامه های اموزش و آگاه سازی
- ✓مدیریت منابع و فعالیتها

باز انجام یا اقدام(Act):
- ✓اجرای توصیه های ارائه شده برای بهبود
- ✓نظام مدیریتی مذکور
- ✓انجام اقدامات اصلاحی و پیشگیرانه
- ✓ارزیابی اقدامات صورت پذیرفته در راستای بهبود

ارزیابی(Check):
- ✓استقرار روشهای نظارت و پایش
- ✓هدایت و بازنگری های ادواری به منظور ارزیابی اثربخشی
- ✓بازنگری در حد قابل قبول مخاطرات
- ✓پیشبرد و هدایت ممیزی های داخلی به منظور ارزیابی تحقق
- ✓فعالیتهای کنترلی متنوع

روش تحقیق

تفسیر
پایایی بالا
بالا

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k} S_i^2}{S_{sum}^2}\right)$$

k تعداد سؤالات S_i^2 واریانس سؤال iام و S_{sum}^2 واریانس کل سؤالات می باشد.

- روش تحقیق
- **از منظر** تحقیق حاضر پرسشنامه روایی محتوی صورت می باشد.
- **از منظر هدف:**

به علت آگاهی رساندن مدیران بانک به اجرایی کردن دستاوردهای پژوهش، **کاربردی** است.

- **از منظر کلی:**

نوع تحقیق **پیمایشی و توصیفی** است. چون براساس نحوه رفتار مشتریان در سیستم بانکداری الکترونیک و عناصر و متغیرهای مربوط به آن تعریف شده است.

جامعه و نمونه آماری

- داده های مورد نیاز این تحقیق از دو جامعه آماری جمع آوری شده است. جامعه اول کلیه مشتریان حقیقی و حقوقی بانک هستند که اطلاعات تراکنش های آنها در محیط بانکداری الکترونیک در سرور بانک ذخیره شده است که از روی اطلاعات ثبت شده، رفتار مشتریان مورد بررسی و تهدیدات وارد شده به سیستم از طریق آنان شناسایی می گردد. جامعه دوم تحقیق شامل مدیران ارشد و کارشناسان خبره در زمینه امنیت و تکنولوژی بانکداری الکترونیک در این بانک می باشد که نقطه نظرات آنها از طریق روشهای تحقیقی و میدانی که مشمول ارائه پرسشنامه و انجام مصاحبه است جمع آوری می گردد.
- نمونه آماری این تحقیق را ۲۰ نفر از متخصصان و کارشناسان حوزه امنیت الکترونیک در برمی گیرد. بعد از توزیع پرسشنامه بین آنها، تمامی این پرسشنامه ها برگشت داده شد. البته باید به این موضوع نیز اشاره داشت که این نوع نمونه گیری انتخابی غیر تصادفی (قضاوتی) می باشد چون باید کارشناسانی انتخاب می شدند که به موضوع و مبحث مورد نظر تسلط کامل را داشته باشند و نیز با استفاده از روش دلفی سعی بر آن شد که پاسخ های ارایه شده به رؤیت سایر کارشناسان قرار گرفته تا بهترین نتیجه ایفاد گردد.

روش تحلیل داده ها

- دراین تحقیق پیشگیری از آن در جهت ارتـ
- حال در این ای) سعی داریم اولویت های رم جهت افزایش امنیت سیست بستگی پیرسون و ضریب تع گی اقدام شد.
- میزان اهمیـ تدا ماتریسی که سطرهای آ ت زیر تشکیل می شود.(ما

خبره پاسخ دهنده / معیار ها	خبره ۱	خبره۲	.....	خبره زام
معیار ۱	Xij			
معیار۲				
.....				
معیار iام				

- در گام بعدی پس از نرمالیزه کردن ماتریس تصمیم گیری ، ایده ال های مثبت و منفی و فاصله اقلیدسی بین این ایده ال ها که اعدادی فازی هستند بدست می آید. و پس از تعیین نز

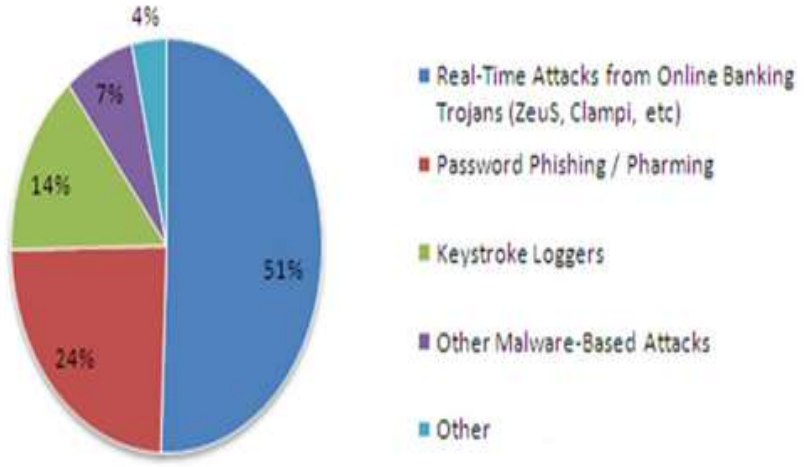
میزان اهمیت معیار i ام از نظر خبره jام

شامل:خیلی‌کم، کم، کم تا متوسط، متوسط، متوسط تا زیاد،زیاد،خیلی زیاد

یافته های تحقیق_ تهدیدات امنیتی

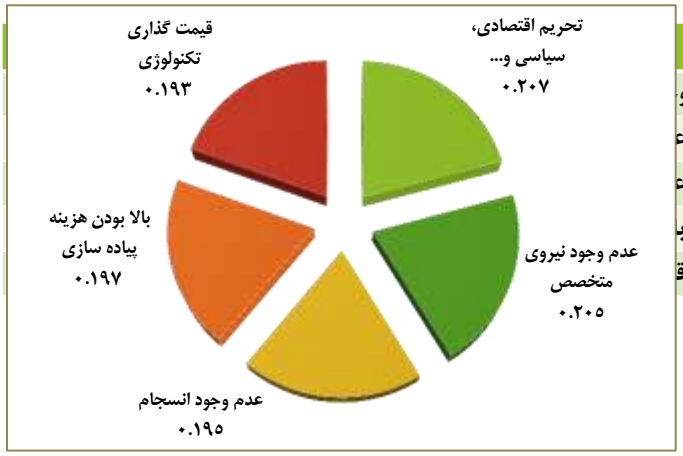
وزن
0.03
0.03
0.03
0.04
0.03
0.03
0.03
0.03
0.03
0.03
0.03
0.03

بیشترین تهدیدات بانکداری آنلاین(منبع: سایت بانک جهانی و مؤسسه CSI)



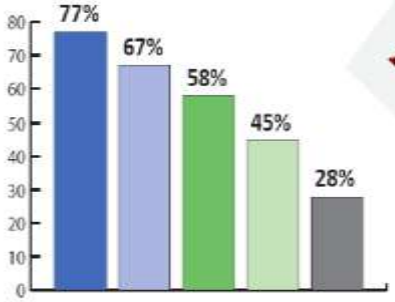
یافته های تحقیق_چالش های امنیتی

ردیف	
C1	و
C2	ع
C3	ع
C4	با
C5	قا



یافته های تحقیق_ تمهیدات امنیتی

What have you found to be the most effective ways to prevent fraud?



67% say customer education is the best way to prevent fraud.

77% - Employee education emphasizing identification and response to fraudulent activities

67% - Customer awareness emphasizing the techniques used by fraudsters, such as phishing, vishing, etc.

58% - Fraud detection tools & technologies

45% - Real-time decision tools

28% - Manual account monitoring

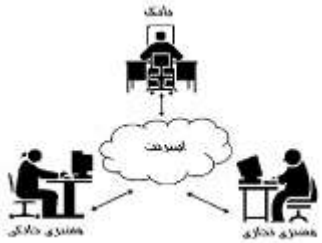
یافته های تحقیق...

- بطور کلی بحث امنیت درسیستم های بانکداری الکترونیک در ۳ حوزه و شاخه اصلی باید مورد بررسی قرار گیرد.

۱)مشتری و یا کاربر و یا کسی که از خدمات بانکداری الکترونیک استفاده می کند.(شخص حقیقی و یا حقوقی)

۲) بانک یا سازمان و یا موسسه مالی خدمات دهنده.

۳) رابط، که شامل کلیه سخت افزارها و نرم افزارهای ارتباطی با مشتریان و بانک جهت ارائه خدمات بانکداری الکترونیکی است.(مانند محیط اینترنت)



ادامه...

- پس می توا
  - سیاس
  - آموز
  - کنترل
  - امنیت

	محافظت	تأیید	تصدیق	رد انکار
آسیب پذیری	نفوذ به مقصد و یا منابع(مثلHacking)	تغییر شکل وب سایت (مثل Phishing)	جا زدن خود به عنوان فرد اصلی(مثل Synthetic Identity) یا Spoofing	برخورد با گروهی که بعداً به دروغ منکرتراکنش انجام شده باشند.
روش مقابله	افشاء خط مشی ها با توجه به روش محافظت و جمع آوری اطلاعات	پورتال مانند(www.yahoo.com) برای تعیین نام دقیق دامنه وب سایت	وجود شخص ثالث بیطرف مثل VeriSign (www.Verisign.com) برای صحه گذاشتن به افرادی که وارد وب سایت می شوند.	مکانیزهایی برای اطمینان کلاینت(مشتری) از اتصال به سرور بانک (سرور اصلی) و یا بالعکس
فناوری پیاده سازی	تکنولوژی Firewall	ورود اطلاعات صحیح	مبادله نمودن گواهینامه های دیجیتال با رمز گزاری	امضاهای دیجیتال

در نهایت می توان گفت...

با پیاده سازی چارچوب فوق بانک ها، موسسات پولی و تجاری از مزایای ذیل بهره مند خواهند شد:

- افزایش مشتریان بانکی و بالتبع بانکداری الکترونیک با افزایش میزان اطمینان و اعتماد آنان به سیستم های بانکداری الکترونیک
- سودآوری بیشتر موسسات پولی و مالی با جذب سرمایه های مشتریان افزوده شده
- کاهش احتمال غیرفعال شدن سیستم ها و برنامه ها(از دست دادن فرصت ها)
- استفاده مؤثر از منابع انسانی و غیر انسانی در یک موسسه پولی و مالی(افزاش بهره وری)
- کاهش هزینه از دست دادن داده توسط ویروس های مخرب و یا حفره های امنیتی (حفاظت از داده های ارزشمند سخت افزاری، نرم افزاری و سرویسهای IT)
- افزایش حفاظت از مالکیت معنوی
- دارا بودن یک استراتژی برای مدیریت مخاطرات در مواقع لازم