

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه پیام نور

مرکز تهران

پایان نامه برای دریافت درجه کارشناسی ارشد  
در رشته مدیریت فن آوری اطلاعات

دانشکده فنی و مهندسی

گروه علمی مهندسی کامپیوتر و مدیریت فن آوری اطلاعات

عنوان پایان نامه:

ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و  
آموزش آگاهی از امنیت اطلاعات کاربران (مورد مطالعه):

پست بانک)

نگارش:

نرگس جهانگیری

استاد راهنما:

دکتر محمد حسن زاده

استاد مشاور:

دکتر داوود کریم زادگان مقدم

این پایان نامه مورد حمایت مالی سازمان پست بانک قرار گرفته است.

مهرماه ۱۳۹۰

تقدیم به:

پدر و مادر، همسر عزیز و فرزندانم

## تشکر و قدردانی

### دل هر ذره را که بشکافی      آفتابیش در میان بینی

اول از خداوند بزرگ سپاس گزارم که همواره بهترین‌ها را برایم خواسته است. بر خود واجب می‌دانم که از زحمات بی‌دریغ، تلاش بی‌وقفه و راهنمایی‌های راه‌گشای استاد ارجمند جناب آقای دکتر حسن زاده در طول این پروژه تشکر و قدردانی به عمل آورم. همچنین از زحمات استاد محترم جناب آقای دکتر کریم‌زادگان که با راهنمایی‌های خود راه‌گشای اینجانب بوده‌اند، تشکر می‌نمایم. از پدر و مادر عزیز و گرمی‌ام که همواره در طول تحصیل مشوق و پشتیبان من بوده‌اند تشکر نموده و سلامتی آن‌ها را از خداوند متعال خواستارم. از همسر عزیزم، به خاطر تمام سختی‌هایی که در طول این تحقیق ناگزیر بر ایشان گذشت و بدون هرگونه شکوه‌ای همواره یاور و حامی من بوده‌اند، قدردانی می‌نمایم. امیدوارم بتوانم قدردان زحمات ایشان باشم.

در پایان از کلیه عزیزانی که به هر شیوه ممکن در انجام این پروژه کمک و یاری رسانده‌اند، تشکر می‌نمایم.

### نرگس جهانگیری

## چکیده

با توجه ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است، مهم‌ترین سرمایه برای هر فرد و یا سازمان، اطلاعات است به همین جهت، امنیت اطلاعات جزء یکی از مهم‌ترین مسائل امروزی گشته است. بیشتر حوادث نقض امنیت اطلاعات، به دلیل عدم توجه به نیروی انسانی علیرغم راه‌حل‌های فنی است. تحقیقات گذشته نشان می‌دهد یکی از فاکتورهای موثر در عوامل انسانی موضوع آگاهی و اطلاع‌رسانی به کاربران از امنیت اطلاعات است. آموزش و آگاهی‌رسانی بایستی یکی از پایه‌ها و سرفصل‌های برنامه‌های امنیتی هر سازمان قرار گیرد. فقدان این مسئله در سازمان‌های دولتی به شدت مشهود است، همین‌طور در سطح اجتماع در حالی که نفوذ کامپیوتر به سرعت ادامه دارد، روند برنامه‌های آموزش و اطلاع‌رسانی به کندی پیش می‌رود. این امر باعث شده که کارکنان سازمان‌ها از حداقل آگاهی‌ها و تدابیر دفاعی لازم آگاه نباشند.

با توجه به اینکه در بیشتر تحقیقات گذشته، آگاهی از امنیت اطلاعات کاربران مورد توجه قرار نگرفته است. در این تحقیق، میزان سطح آگاهی از امنیت اطلاعات کاربران در سه سطح دانش، نگرش و رفتار مورد ارزیابی قرار گرفت و برای محاسبه سطح آگاهی از امنیت اطلاعات کارمندان، ۹ مؤلفه بررسی شد. عوامل متنوعی بر که بر میزان آگاهی کاربران از امنیت اطلاعات به عنوان متغیر وابسته این تحقیق، تأثیر گذار است، شناسایی شد که شامل ۷ متغیر مستقل جنسیت، میزان تحصیلات، میزان آشنایی با مهارت فن‌آوری اطلاعات، میزان سابقه شغلی، درجه سازمانی، رشته تحصیلی و رده شغلی کارمندان است. پرسشنامه نیز با کمک خبرگانی در زمینه امنیت اطلاعات تجدید نظر شده و مقیاس لیکرت ۵ امتیازی از ۱، به عنوان کاملاً مخالف تا ۵، به عنوان کاملاً موافق برای اندازه‌گیری منظور گردید و با استفاده از آزمون ضریب همبستگی اسپیرمن و کرامر و پیرسون ارتباط بین متغیرهای مستقل و متغیر وابسته در سطح معناداری ۰,۰۵، سنجیده شد. جامعه آماری، کارکنان ادارات ستادی پست بانک بودند و نمونه ۲۰۰ نفر انتخاب گردید. ضمن آنکه آلفای کرونباخ پرسشنامه نمونه اولیه به دست آمده، نشان از پایایی مناسب آن بود. نتایج آشکار کرد که از ۷ متغیر مستقل فقط متغیرهای درجه سازمانی، آشنایی با مهارت‌های فن‌آوری اطلاعات، رشته تحصیلی و رده شغلی در سطح معناداری با متغیر وابسته آگاهی از امنیت اطلاعات دارای همبستگی است.

## کلمات کلیدی

چارچوب مفهومی، پرمایگی، امنیت اطلاعات، آگاهی از امنیت اطلاعات

## فهرست مطالب

### ۱- کلیات تحقیق

.....۲	.....
.....۲	..... ۱-۱ مقدمه
.....۳	..... ۲-۱ بیان مسئله
.....۴	..... ۳-۱ سوالات تحقیق
.....۴	..... ۴-۱ فرضیه‌ها
.....۵	..... ۵-۱ اهداف پژوهش
.....۵	..... ۱-۵-۱ اهداف آرمانی
.....۵	..... ۲-۵-۱ اهداف اصلی
.....۵	..... ۳-۵-۱ اهداف ویژه
.....۶	..... ۶-۱ نوآوری تحقیق
.....۶	..... ۷-۱ ضرورت و سابقه تحقیق
.....۸	..... ۸-۱ تعاریف کلمات کلیدی
.....۹	..... ۹-۱ تعاریف عملیاتی متغیرهای مستقل و وابسته مورد مطالعه
.....۱۰	..... ۱۰-۱ سیر تشکیل پست بانک ایران
.....۱۱	..... ۱۱-۱ ساختار پایان نامه

### ۲- ادبیات تحقیق

.....۱۳	.....
.....۱۳	..... ۱-۲ مقدمه
.....۱۳	..... ۲-۲ مفاهیم داده و اطلاعات
.....۱۳	..... ۱-۲-۲ داده
.....۱۳	..... ۲-۲-۲ اطلاعات
.....۱۴	..... ۳-۲-۲ اهمیت اطلاعات
.....۱۵	..... ۴-۲-۲ اهمیت و نقش اطلاعات در سازمان
.....۱۷	..... ۳-۲ مفاهیم امنیت
.....۱۷	..... ۱-۳-۲ امنیت چیست؟
.....۱۷	..... ۲-۳-۲ امنیت اطلاعات چیست؟
.....۱۹	..... ۳-۳-۲ تاریخچه امنیت اطلاعات
.....۱۹	..... ۴-۳-۲ امنیت اطلاعات در عصر کامپیوتر
.....۲۰	..... ۵-۳-۲ امنیت اطلاعات با ظهور اینترنت
.....۲۱	..... ۶-۳-۲ عناصر کلیدی در امنیت اطلاعات
.....۲۳	..... ۷-۳-۲ اصطلاحات امنیتی
.....۲۳	..... ۸-۳-۲ ضعف در بعد امنیت
.....۲۴	..... ۴-۲ حوادث امنیتی
.....۲۸	..... ۵-۲ رویکردهای متفاوت مدیریت خطرات امنیتی در پیاده‌سازی امنیت اطلاعات
.....۲۹	..... ۱-۵-۲ جزئیات مدل امنیتی دفاع در عمق
.....۳۱	..... ۱-۱-۵-۲ لایه‌ی سیاست‌ها، رویه‌ها و اطلاع‌رسانی
.....۳۱	..... ۶-۲ اهمیت امنیت اطلاعات در سازمان

..... ۳۳	۷-۲ مزایای سرمایه‌گذاری در امنیت اطلاعات
..... ۳۴	۸-۲ لایه‌های امنیت اطلاعات
..... ۳۵	۹-۲ جنبه‌های مختلف در امنیت اطلاعات
..... ۳۶	۱-۹-۲ تکنولوژی
..... ۳۷	۲-۹-۲ فرایندها و عملیات
..... ۳۷	۳-۹-۲ افراد
..... ۳۸	۱۰-۲ نقش عوامل غیر فنی در امنیت اطلاعات
..... ۴۰	۱۱-۲ نقش عوامل انسانی در امنیت اطلاعات
..... ۴۳	۱۲-۲ آگاهی و آموزش امنیت اطلاعات به کاربران
..... ۴۵	۱-۱۲-۲ طیف دانش امنیت اطلاعات به کاربران
..... ۴۵	۱۳-۲ سطوح یادگیری امنیت اطلاعات
..... ۴۵	۱-۱۳-۲ آگاهی
..... ۴۶	۲-۱۳-۲ تربیت
..... ۴۶	۳-۱۳-۲ تحصیلات و آموزش
..... ۴۶	۱۴-۲ تفاوت و مقایسه آگاهی، تربیت و آموزش
..... ۴۷	۱۵-۲ مدل‌های آگاهی، تربیت و آموزش امنیت اطلاعات
..... ۴۷	۱-۱۵-۲ طراحی
..... ۴۹	۲-۱۵-۲ توسعه
..... ۵۰	۳-۱۵-۲ پیاده‌سازی
..... ۵۱	۴-۱۵-۲ پشتیبانی و حمایت
..... ۵۲	۱۶-۲ آگاهی از امنیت اطلاعات کارمندان
..... ۵۳	۱۷-۲ سطوح آگاهی از امنیت اطلاعات
..... ۵۳	۱-۱۷-۲ سطح اول آگاهی امنیتی: دانش
..... ۵۳	۲-۱۷-۲ سطح دوم آگاهی امنیتی: نگرش
..... ۵۴	۳-۱۷-۲ سطح سوم آگاهی امنیتی: رفتار و بروندگی
..... ۵۴	۱۸-۲ استراتژی ارزیابی آگاهی از امنیت اطلاعات کارمندان
..... ۵۴	۱-۱۸-۲ ارزیابی
..... ۵۵	۲-۱۸-۲ طراحی
..... ۵۵	۳-۱۸-۲ پیاده‌سازی و اجرا
..... ۵۵	۴-۱۸-۲ ارزیابی و بازخورد
..... ۵۶	۵-۱۸-۲ پشتیبانی
..... ۵۶	۱۹-۲ آگاهی از امنیت اطلاعات چگونه حاصل می‌شود؟
..... ۵۶	۲۰-۲ آگاهی از امنیت اطلاعات در کاربران چه مؤلفه‌هایی را شامل می‌شود؟
..... ۵۶	۱-۲۰-۲ ایمیل، ضمیمه و اسپم (هرزنامه)
..... ۵۷	۲-۲۰-۲ پشتیبانی
..... ۵۷	۳-۲۰-۲ رمز عبور
..... ۵۷	۴-۲۰-۲ ایمنی در اینترنت
..... ۵۸	۵-۲۰-۲ بدافزارها (ویروس و کرم و تراجان‌ها و ...)
..... ۵۸	۶-۲۰-۲ انتقال ایمن اطلاعات

..... ۵۸	۷-۲۰-۲ مهندسی اجتماع
..... ۵۹	۸-۲۰-۲ گزارش‌دهی حوادث امنیتی
..... ۵۹	۹-۲۰-۲ التزام و رعایت سیاست‌های امنیتی سازمان
..... ۵۹	۲۱-۲ بررسی تحقیقات عوامل تأثیر گذار در امنیت اطلاعات در سوابق داخلی
..... ۶۱	۲۲-۲ بررسی عوامل غیر فنی و انسانی تأثیرگذار در امنیت اطلاعات در سوابق خارجی
..... ۶۴	۲۳-۲ جمع‌بندی از مرور ادبیات

**۳- روش تحقیق**

..... ۶۸	۱-۳ مقدمه
..... ۶۸	۲-۳ شناخت کلی موضوع تحقیق و مطالعه ادبیات تحقیق
..... ۶۸	۳-۳ روش انجام تحقیق
..... ۶۹	۴-۳ تعیین متغیرهای تحقیق
..... ۶۹	۵-۳ جامعه آماری مورد مطالعه
..... ۶۹	۶-۳ روش نمونه‌گیری
..... ۷۰	۷-۳ ابزار سنجش و گردآوری داده‌ها
..... ۷۱	۸-۳ روایی ابزار
..... ۷۱	۹-۳ پایایی ابزار
..... ۷۱	۱۰-۳ ضریب آلفای کرونباخ پرسشنامه
..... ۷۲	۱۱-۳ روش‌های آمار بکارگرفته شده
..... ۷۲	۱-۱۱-۳ روش‌های آمار توصیفی
..... ۷۲	۲-۱۱-۳ روش‌های آمار استنباطی

**۴- گزارش یافته‌های تحقیق**

..... ۷۵	۱-۴ مقدمه
..... ۷۵	۲-۴ نتایج آمار توصیفی
..... ۷۵	۱-۲-۴ جنسیت پاسخ‌دهندگان
..... ۷۵	۲-۲-۴ گروه‌های سنی پاسخ‌دهندگان
..... ۷۶	۳-۲-۴ میزان تحصیلات پاسخ‌دهندگان
..... ۷۶	۴-۲-۴ رشته تحصیلی پاسخ‌دهندگان
..... ۷۷	۵-۲-۴ سابقه خدمت پاسخ‌دهندگان
..... ۷۸	۶-۲-۴ رده شغلی پاسخ‌دهندگان
..... ۷۸	۷-۲-۴ درجه سازمانی پاسخ‌دهندگان
..... ۷۹	۸-۲-۴ میزان آشنایی با مهارت‌های ICDL پاسخ‌دهندگان
..... ۸۰	۹-۲-۴ تعداد دفعات شرکت در کارگاه‌های آموزشی امنیت اطلاعات پاسخ‌دهندگان
..... ۸۰	۳-۴ آمار توصیفی میزان آگاهی از نه مؤلفه امنیت اطلاعات
..... ۸۰	۱-۳-۴ آمار توصیفی مؤلفه «ایمیل، ضمایم و اسپم»
..... ۸۱	۲-۳-۴ آمار توصیفی مؤلفه «پشتیبانی از اطلاعات»
..... ۸۳	۳-۳-۴ آمار توصیفی مؤلفه «رمز عبور»
..... ۸۴	۴-۳-۴ آمار توصیفی مؤلفه «مهندسی اجتماع»



..... ۸۴	۴-۳-۵ آمار توصیفی مؤلفه «انتقال ایمن اطلاعات»
..... ۸۵	۴-۳-۶ آمار توصیفی مؤلفه «بدافزارها و کدهای مخرب»
..... ۸۷	۴-۳-۷ آمار توصیفی مؤلفه «اینترنت»
..... ۸۸	۴-۳-۸ آمار توصیفی مؤلفه «گزارش‌دهی»
..... ۸۹	۴-۳-۹ آمار توصیفی مؤلفه «التزام به سیاست‌های امنیتی سازمان»
..... ۸۹	۴-۴ محاسبه امتیاز میزان آگاهی هر یک از مؤلفه‌های امنیت اطلاعات در سطوح مختلف
..... ۹۰	۴-۵ آزمون‌های نرمال بودن شاخص‌ها
..... ۹۰	۴-۵-۱ آزمون نرمال بودن برای شاخص آگاهی از مؤلفه‌های امنیت اطلاعات
..... ۹۱	۴-۵-۲ آزمون نرمال بودن برای شاخص آگاهی در سطح دانش از مؤلفه‌های امنیت اطلاعات
..... ۹۱	۴-۵-۳ آزمون نرمال بودن برای شاخص آگاهی در سطح نگرش از مؤلفه‌های امنیت اطلاعات
..... ۹۱	۴-۵-۴ آزمون نرمال بودن برای شاخص آگاهی در سطح رفتار از مؤلفه‌های امنیت اطلاعات

**۵- ارزیابی داده‌ها**

..... ۹۳	۵-۱ بررسی سوالات تحقیق و فرضیه‌های آن
..... ۹۳	۵-۱-۱ سوال اول تحقیق
..... ۹۳	۵-۱-۲ سوال دوم تحقیق و بررسی فرضیه‌های آن
..... ۹۳	۵-۱-۲-۱ بررسی فرضیه (۱)
..... ۹۴	۵-۱-۲-۲ بررسی فرضیه (۲)
..... ۹۴	۵-۱-۲-۳ بررسی فرضیه (۳)
..... ۹۵	۵-۱-۲-۴ بررسی فرضیه (۴)
..... ۹۶	۵-۱-۲-۵ بررسی فرضیه (۵)
..... ۹۶	۵-۱-۲-۶ بررسی فرضیه (۶)
..... ۹۷	۵-۱-۲-۷ بررسی فرضیه (۷)
..... ۹۷	۵-۱-۳ سوال سوم تحقیق و بررسی فرضیه آن
..... ۹۷	۵-۱-۳-۱ فرضیه (۱-۸)
..... ۹۸	۵-۱-۳-۲ فرضیه (۲-۸)
..... ۹۸	۵-۱-۳-۳ فرضیه (۳-۸)
..... ۹۹	۵-۲ نتایج کلی حاصل از آزمون فرضیه‌ها
..... ۱۰۰	۵-۳ امتیاز و اولویت هر یک از مؤلفه‌ها
..... ۱۰۲	۵-۴ جمع‌بندی
..... ۱۰۴	۵-۵ مقایسه نتایج تحقیق با تحقیقات گذشته

**۶- نتیجه‌گیری و پیشنهادها**

..... ۱۰۶	۶-۱ فعالیت‌های انجام شده در تحقیق
..... ۱۰۶	۶-۲ یافته‌های تحقیق
..... ۱۰۷	۶-۳ پیشنهادها برای تحقیقات آتی
..... ۱۰۸	۶-۴ پیشنهادهای اجرایی

**منابع**

..... ۱۱۴	واژه‌نامه انگلیسی به فارسی
-----------	----------------------------



## فهرست جداول

۲۵.....	جدول ۲ - ۱: حوادث امنیتی گزارش شده توسط CERT (۲۰۰۸)
۲۶.....	جدول ۲ - ۲: نتایج طبقه بندی MIS QUARTERLY از مسئله امنیت (KNAPP ET AL., 2005)
۴۲.....	جدول ۲ - ۳: نواحی کنترل امنیت اطلاعات (پاکدامن، ۱۳۸۸)
۴۳.....	جدول ۲ - ۴: عوامل انسانی موثر بر پیاده سازی سیستم امنیت اطلاعات (NOSWORTHY, 2000)
۴۴.....	جدول ۲ - ۵: طبقه بندی MIS QUARTERLY مباحث امنیتی (KNAPP ET AL., 2004)
۴۷.....	جدول ۲ - ۶: چارچوب مقایسه بین سطوح یادگیری امنیت اطلاعات (WILSON AND HASH, 2003)
۷۵.....	جدول ۴ - ۱: جدول جنسیت پاسخ دهندگان
۷۵.....	جدول ۴ - ۲: جدول فراوانی رده سنی پاسخ دهندگان
۷۶.....	جدول ۴ - ۳: جدول فراوانی میزان تحصیلات پاسخ دهندگان به پرسشنامه
۷۶.....	جدول ۴ - ۴: جدول فراوانی نوع مدرک تحصیلی پاسخ دهندگان به پرسشنامه
۷۷.....	جدول ۴ - ۵: جدول فراوانی سابقه خدمت پاسخ دهندگان به پرسشنامه
۷۸.....	جدول ۴ - ۶: جدول فراوانی رده شغلی پاسخ دهندگان به پرسشنامه
۷۸.....	جدول ۴ - ۷: جدول فراوانی درجه سازمانی پاسخ دهندگان به پرسشنامه
۷۹.....	جدول ۴ - ۸: جدول فراوانی میزان آشنایی با مهارت های ICDL پاسخ دهندگان به پرسشنامه
۸۰.....	جدول ۴ - ۹: جدول فراوانی دفعات شرکت در کارگاه های آموزشی امنیت اطلاعات پاسخ دهندگان
۸۰.....	جدول ۴ - ۱۰: پاسخ سوالات مربوط به مؤلفه «ایمیل، ضمایم و هرزنامه»
۸۱.....	جدول ۴ - ۱۱: پاسخ سوالات مربوط به مؤلفه «پشتیبانی از اطلاعات»
۸۳.....	جدول ۴ - ۱۲: پاسخ سوالات مربوط به مؤلفه «رمز عبور»
۸۴.....	جدول ۴ - ۱۳: پاسخ سوالات مربوط به مؤلفه «مهندسی اجتماع»
۸۴.....	جدول ۴ - ۱۴: پاسخ سوالات مربوط به مؤلفه «انتقال ایمن اطلاعات»
۸۵.....	جدول ۴ - ۱۵: پاسخ سوالات مربوط به مؤلفه «بدافزارها و کدهای مخرب»
۸۷.....	جدول ۴ - ۱۶: پاسخ سوالات مربوط به مؤلفه «اینترنت»
۸۸.....	جدول ۴ - ۱۷: پاسخ سوالات مربوط به مؤلفه «گزارش دهی»
۸۹.....	جدول ۴ - ۱۸: پاسخ سوالات مربوط به مؤلفه «التزام به سیاست های امنیتی سازمان»
۸۹.....	جدول ۴ - ۱۹: امتیاز میزان آگاهی هر یک از مؤلفه های امنیت اطلاعات در سطوح مختلف
۹۰.....	جدول ۴ - ۲۰: نرمال بودن متغیر آگاهی از مؤلفه های امنیت اطلاعات
۹۱.....	جدول ۴ - ۲۱: نرمال بودن برای شاخص آگاهی در سطح دانش از مؤلفه های امنیت اطلاعات
۹۱.....	جدول ۴ - ۲۲: نرمال بودن برای شاخص آگاهی در سطح نگرش از مؤلفه های امنیت اطلاعات
۹۱.....	جدول ۴ - ۲۳: نرمال بودن برای شاخص آگاهی در سطح رفتار از مؤلفه های امنیت اطلاعات
۹۳.....	جدول ۵ - ۱: ضریب همبستگی کرامر بین جنسیت کارکنان و آگاهی از مؤلفه های امنیت اطلاعات
۹۴.....	جدول ۵ - ۲: ضریب همبستگی کرامر بین میزان تحصیلات کارکنان و آگاهی از مؤلفه های امنیت اطلاعات

جدول ۵-۳: ضریب همبستگی اسپیرمن بین آشنایی با مهارت‌های آی‌سی‌دی‌ال کارکنان و آگاهی از مؤلفه‌های امنیت

اطلاعات

۹۴.....

جدول ۵-۴: ضریب همبستگی اسپیرمن بین تعداد دفعات شرکت در کارگاه‌های آموزشی امنیت اطلاعات کارکنان و

آگاهی از مؤلفه‌های امنیت اطلاعات

۹۵.....

جدول ۵-۵: ضریب همبستگی اسپیرمن بین سابقه کاری کارکنان و آگاهی از مؤلفه‌های امنیت اطلاعات

۹۵.....

جدول ۵-۶: ضریب همبستگی اسپیرمن بین درجه سازمانی کارکنان و آگاهی از مؤلفه‌های امنیت اطلاعات

۹۶.....

جدول ۵-۷: ضریب همبستگی کرامر بین رشته تحصیلی کارمندان و آگاهی از مؤلفه‌های امنیت اطلاعات

۹۶.....

جدول ۵-۸: ضریب همبستگی کرامر بین رده شغلی کارکنان و آگاهی از مؤلفه‌های امنیت اطلاعات

۹۷.....

جدول ۵-۹: ضریب همبستگی پیرسون بین سطح دانش و سطح نگرش آگاهی از مؤلفه‌های امنیت اطلاعات

۹۸.....

جدول ۵-۱۰: ضریب همبستگی پیرسون بین سطح دانش و سطح رفتار آگاهی از مؤلفه‌های امنیت اطلاعات

۹۸.....

جدول ۵-۱۱: ضریب همبستگی پیرسون بین سطح نگرش و سطح رفتار آگاهی از مؤلفه‌های امنیت اطلاعات

۹۹.....

جدول ۵-۱۲: نتایج حاصل از آزمون فرضیه‌ها

۹۹.....

جدول ۵-۱۳: نتایج ارزیابی پرمایگی آگاهی از امنیت اطلاعات کارمندان

۱۰۰.....

## فهرست شکل‌ها

.....۲۵	شکل ۲-۱: نمودار آسیب‌پذیری‌ها در سال‌های ۲۰۰۰ تا ۲۰۰۸ (جاویدفومنی مقدم، ۱۳۸۸)
.....۲۷	شکل ۲-۲: میزان حملات PHISHING طبق گزارشات RSA در سال ۲۰۰۷ (طاهری، ۱۳۸۶)
.....۳	شکل ۲-۳: مدل امنیتی دفاع در عمق (سزاروش، ۱۳۹۰)
.....۳۴	شکل ۲-۴: لایه‌های امنیت اطلاعات (داگلاس و مکدائل، ۱۹۸۴)
.....۳۵	شکل ۲-۵: مدل کوه یخ پولانی دانش امنیت اطلاعات در سال ۱۹۹۴ (طاهری، ۱۳۸۶)
.....۳۵	شکل ۲-۶: جنبه‌های مختلف در امنیت اطلاعات (طاهری، ۱۳۸۶)
.....۳۹	شکل ۲-۷: فاکتورهای غیر فنی اثر گذار بر به‌کارگیری خط‌مشی‌های امنیتی IS (KARYDA ET AL., 2004)
.....۴۲	شکل ۲-۸: ارتباط بین میزان کنترل و هزینه‌ها (HINSON., 2003)
.....۴۵	شکل ۲-۹: مراحل ارتقاء دانش امنیت اطلاعات (NIST, SP800-50)
.....۴۷	شکل ۲-۱۰: متدولوژی ارائه شده برای برنامه آگاهی، تربیت و آموزش امنیت اطلاعات (NIST, SP800-50)
.....۴۸	شکل ۲-۱۱: برآورد نیازهای آموزشی (NIST, SP800-50)
.....۵۱	شکل ۲-۱۲: بازنگری برنامه آگاهی‌رسانی و آموزشی (NIST SP800-50)
.....۵۴	شکل ۲-۱۳: استراتژی کلی در ارتقاء آگاهی از امنیت اطلاعات در سازمان‌های مالی (SANTA, 2008)
.....۶۰	شکل ۲-۱۴: مدل عوامل انسانی اثر گذار بر اثربخشی امنیت سیستم‌های اطلاعاتی (طاهری، ۱۳۸۶)
.....۶۱	شکل ۲-۱۵: مدل ارزیابی آگاهی از امنیت اطلاعات کاربران (KRUGER AND KEARNEY, 2006)
.....۶۲	شکل ۲-۱۶: نقشه ارزیابی از آگاهی امنیت اطلاعات در استرالیا و (B) آگاهی در صورت کلی
.....۶۳	شکل ۲-۱۷: تأثیر مستقیم آگاهی از امنیت اطلاعات بر عملکرد سازمان (CHIO ET AL., 2008)
.....۶۵	شکل ۲-۱۸: چارچوب کلی ارتقاء آگاهی از امنیت اطلاعات کاربران
.....۶۶	شکل ۲-۱۹: چارچوب مفهومی اولیه برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران
.....۷۳	شکل ۳-۱: ساختار شماتیک روش تحقیق
.....۷۵	شکل ۴-۱: نمودار دایره‌ای جنسیت پاسخ‌دهندگان
.....۷۶	شکل ۴-۲: نمودار دایره‌ای رده سنی پاسخ‌دهندگان
.....۷۶	شکل ۴-۳: نمودار دایره‌ای میزان تحصیلات پاسخ‌دهندگان
.....۷۷	شکل ۴-۴: نمودار دایره‌ای رشته تحصیلی پاسخ‌دهندگان
.....۷۷	شکل ۴-۵: نمودار دایره‌ای سابقه خدمت پاسخ‌دهندگان
.....۷۸	شکل ۴-۶: نمودار دایره‌ای رده شغلی پاسخ‌دهندگان
.....۷۹	شکل ۴-۷: نمودار دایره‌ای درجه سازمانی پاسخ‌دهندگان
.....۷۹	شکل ۴-۸: نمودار دایره‌ای میزان آشنایی با مهارت‌های ICDL پاسخ‌دهندگان
.....۸۰	شکل ۴-۹: نمودار دایره‌ای دفعات شرکت در کارگاه‌های آموزشی امنیت اطلاعات پاسخ‌دهندگان
.....۱:۰	شکل ۵-۱: میزان آگاهی کارمندان از مؤلفه‌های امنیت اطلاعات
.....۱:۰	شکل ۵-۲: چارچوب کلی ارتقاء آگاهی از امنیت اطلاعات کاربران
.....۱:۰	شکل ۵-۳: چارچوب مفهومی ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کارمندان

## فصل اول

کلیات تحقیق

## ۱ + مقدمه

در سال‌های اخیر با پیشرفت تکنولوژی اطلاعات<sup>۱</sup> و ارتباطات<sup>۲</sup> شاهد به کارگیری تجهیزات الکترونیک و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های روزمره همچون ارائه خدمات مدیریت و نظارت و اطلاع‌رسانی هستیم. فضایی که چنین فعالیت‌هایی در آن صورت می‌پذیرد با عنوان فضای تبادل اطلاعات شناخته می‌شود. فضای مذکور همواره در معرض تهدیدهای الکترونیکی یا آسیب‌های فیزیکی از قبیل جرایم سازمان یافته به منظور ایجاد تغییر در محتوا یا جریان انتقال اطلاعات، تخریب بانک‌های اطلاعاتی<sup>۳</sup>، اختلال در ارائه خدمات اطلاع‌رسانی یا نظارتی و نقض حقوق مالکیت معنوی است.

از طرف دیگر با رشد و توسعه فزاینده فن‌آوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری<sup>۴</sup> فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یاد شده، گسترده‌تر و پیچیده‌تر می‌شود. از این رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهم‌ترین اهداف توسعه فن‌آوری اطلاعاتی و ارتباطی محسوب می‌شود (Wilson and Hash, 2003; Kruger and Kearmey, 2006; Veiga and Eloff, 2010).

بررسی‌های موسسه‌های expo storage حاکی از آن است که ۸۳ درصد شرکت‌های تجاری برای حفظ امنیت اطلاعات ذخیره شده خود برنامه خاصی ندارند و در صورت از بین رفتن این اطلاعات در اثر خراب‌کاری یا نفوذ هکرها و کلاه برداران به سیستم‌های رایانه‌ای به سختی می‌توانند این اطلاعات را بازیافت کنند. همچنین در گزارشی دیگر عدم توجه و سهل‌انگاری کاربران را خطرناک‌تر از حملات هکرها اعلام کردند (Santa, 2008).

به طور کلی امنیت اطلاعات، به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیر مجاز اشاره دارد (Von Solms, 2000). همچنین مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری (خالقی، ۱۳۸۳) و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است (Wilson and Hash, 2003). با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیر مجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود.

یکی از جنبه‌ها و راه‌های غیر فنی<sup>۵</sup> برای حفاظت و مدیریت امنیت اطلاعات ارتقاء آگاهی<sup>۶</sup> کاربران از امنیت اطلاعات است در این صورت افراد، آگاه به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود هستند. آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و

---

1 Information Technology  
2 Communication  
3 Data Base  
4 Vulnerability  
5 Non Technical  
6 Awareness

تقویت فعالیت‌های خوب امنیتی<sup>۱</sup> می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فن‌آوری اطلاعات نگران و پاسخگو باشند (Wilson and Hash, 2003) و به تدریج به فرهنگ<sup>۲</sup> در سازمان‌ها تبدیل خواهد شد (Kruger and Kearney, 2006; Nikerk and Solms, 2009).

لذا بایستی به موازات تمهیدات فنی<sup>۳</sup> اعمال شده جهت امنیت اطلاعات، در قوانین و سیاست‌های جاری متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شده و فرهنگ و آموزش‌های صحیح به‌کارگیری اطلاعات و تأمین امنیت آن‌ها در اولویتی بالاتر نیز در سطح جامعه ترویج شود.

## ۴-۱ بیان مسئله

با افزایش وسعت شبکه‌ها و دسترسی آسان به اینترنت، خطرات امنیتی نیز به سرعت بیشتر و بیشتر می‌شوند. طی تحقیقی پیرامون موضوع آگاهی از امنیت اطلاعاتی کاربران معلوم شد که در سال‌های بین ۲۰۰۴ تا ۲۰۰۶ میزان متوسط زیان و تعداد قانون شکنی‌های امنیتی به حد چشمگیری کاهش پیدا کردند (Shaw et al., 2009). یکی از دلایل اصلی این ارتقاء در مشکل امنیتی، سرمایه‌گذاری‌های مستمر شرکت‌های کوچک و متوسط در فن‌آوری امنیت اطلاعات و برنامه‌های آگاهی از امنیت اطلاعات است (Shaw et al., 2009). کارمندان فن‌آوری اطلاعات به تنهایی در متوقف سازی رخداد قانون شکنی‌های امنیتی نمی‌توانند موثر باشند (Shaw and Charlie, 2002) لذا آگاهی امنیتی کاربران نهایی باید ارتقاء داده شود و یک توازن بین راه‌حل‌های فنی و غیر فنی در سازمان وجود داشته باشد (Kruger and Kearney, 2006).

بدیهی است که توجه نکردن به مقوله امنیت اطلاعات و افزایش ندادن آگاهی‌های لازم برای امنیت اطلاعات متناسب با سطوح مختلف افراد مانع از گسترش فضای اطلاعاتی در میان آحاد جامعه و جلب اعتماد مدیران در به‌کارگیری روش‌های نوین نظارتی و اطلاع‌رسانی خواهد شد. ایجاد یک چارچوب کلی در سطح کلان با لحاظ کردن ویژگی‌های خاص فضای تبادل اطلاعات و مقوله امنیت در این فضا یک ضرورت است.

هرچند در بیشتر سازمان‌ها در سطوح مختلف کاری اعم از وزارتخانه‌ها، سازمان‌های دولتی، نهادهای آموزشی و دیگر ارگان‌ها تدابیر و فرایندها، سیاست‌ها و استانداردهای مختلفی را پذیرفته و اجرا کرده‌اند ولی همچنان شاهد نقض امنیت اطلاعاتی در اکثر سازمان‌ها و نهادها می‌باشیم؛ و به نظر می‌رسد توجه لازم به تمام ابعاد مدیریت امنیت از جمله بخش عوامل انسانی نشده است

در این تحقیق پژوهشگر مؤلفه‌های موثر در ارزیابی<sup>۴</sup> پرمایگی<sup>۵</sup> و آموزش آگاهی از امنیت کاربران را شناسایی کرده و پس از بررسی اعتبار، یک چارچوب کلی برای ارزیابی پرمایگی آگاهی از امنیت

---

1 Good security activities  
2 Culture  
3 Technical  
4 Assess  
5 Richness



اطلاعات را ارائه می‌دهد. در این چارچوب سه سطح از آگاهی امنیتی که عبارتند از: دانش<sup>۱</sup>، نگرش<sup>۲</sup> و رفتار<sup>۳</sup>، مورد توجه قرار می‌گیرد (Kruger and Kearney, 2006).

با افزایش دانش و آگاهی‌های کارمندان یک سازمان از امنیت اطلاعات در راستای این سه سطح، میزان پرمایگی دانش امنیت اطلاعات از جانب افراد بالاتر می‌رود. رعایت اصول امنیتی در افراد به تدریج به صورت نهادینه و رفتاری تبدیل می‌شود؛ و این امر به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کرده و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود. اگرچه روشی واحد که با تمامی موقعیت‌ها منطبق باشد در سطح سازمانی و انسانی در عملکردهای مختلف برنامه‌های مربوط به ارزیابی و ارتقاء آگاهی امنیتی یکسانی جود ندارد، داشتن یک رویه مشخص برای برقراری برنامه‌های ارزیابی و ارتقاء بر اساس سطوح آگاهی امنیتی بسیار ضروری است.

### ۳-۱ سوالات تحقیق

۱. مؤلفه‌های آگاهی از امنیت اطلاعات کارکنان کدام است؟
۲. چه عواملی بر سطح آگاهی از مؤلفه‌های امنیت اطلاعات کارمندان در یک سازمان عینی تأثیرگذار است؟
۳. آیا بین سطوح آگاهی از امنیت اطلاعات (دانش، نگرش و رفتار) ارتباط وجود دارد؟

### ۴-۱ فرضیه‌ها

- هفت فرضیه اول مربوط به سوال دوم است و فرضیه ۸ مربوط به سوال سوم می‌باشد.
- فرضیه (۱): بین جنسیت کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
  - فرضیه (۲): بین میزان تحصیلات کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
  - فرضیه (۳): بین مهارت‌های فن‌آوری اطلاعات کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
  - فرضیه (۴): بین سابقه خدمت کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
  - فرضیه (۵): بین درجه سازمانی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.

---

1 knowledge  
2 Attitude  
3 Behavior

- فرضیه (۶) : بین رشته تحصیلی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۷) : بین رده شغلی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۸) : بین سطوح آگاهی از امنیت اطلاعات (دانش، نگرش و رفتار) همبستگی وجود دارد.

## ۱ ۵ اهداف پژوهش

### ۱ ۵ ۱ اهداف آرمانی

- رسیدن به یک جامعه اطلاعاتی ایمن و مطمئن.
- تقویت بنیه‌ی دولت الکترونیکی و کاهش جرایم اینترنتی.
- مقابله با سوءاستفاده‌های ناشی از ناآگاهی کاربران از مسائل امنیت اطلاعات.

### ۱ ۵ ۲ اهداف اصلی

- ارائه یک چارچوب برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران در سازمان‌ها.
- کمک به رسیدن به سطح قابل قبولی از امنیت به موازات پذیرش راه‌حل‌های فنی در حفظ اطلاعات به عنوان بارزترین سرمایه سازمان.

### ۱ ۵ ۳ اهداف ویژه

- تعیین همبستگی جنسیت با میزان آگاهی از مؤلفه‌های امنیت اطلاعات کارمندان.
- تعیین همبستگی سطح با نوع تحصیلات کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی مهارت فن‌آوری اطلاعات کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی سابقه خدمت کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی درجه سازمانی کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی رده شغلی کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.

- تعیین اولویت‌بندی مؤلفه‌های امنیت اطلاعات در یک محیط سازمانی (عینی).
- شناخت ارتباط بین سطوح آگاهی از امنیت اطلاعات کارمندان.

## ۱ ۶ نوآوری تحقیق

بیشتر تحقیقات در زمینه امنیت اطلاعات بر روی عوامل فنی تاکید دارند و کمتر به عوامل غیر فنی پرداخته می‌شود. طبق تحقیقات انجام شده آگاهی و آموزش کاربران از امنیت اطلاعات یکی از فاکتورهای شناخته شده از عوامل غیر فنی تاثیرگذار بر امنیت اطلاعات سازمان است. تاکید این تحقیق بر ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کارمندان در سازمان‌ها، نوآوری آن محسوب می‌شود که در صورت ارائه می‌تواند به عنوان نقشه راهی برای همه سازمان‌ها جهت ارزیابی و ارتقاء دانش کارمندان از امنیت اطلاعات تلقی شود.

## ۱ ۷ ضرورت و سابقه تحقیق

امروزه امنیت از اطلاعات به عنوان مهم‌ترین چالش سازمان‌هایی که در تلاش هستند از فرصت‌های فن‌آوری اطلاعات بهره‌مند شوند، مطرح است و برای بهره‌مندی از فرصت‌های فاوا باید به امنیت اطلاعات فراتر از فن‌آوری و در قالب یک فرهنگ نگریست (طاهری، ۱۳۸۶). در واقع امنیت باید در یک سازمان تبدیل به یک فعالیت و فرآیند دائمی جهت مدیریت مخاطرات شود که پوشش دهنده مجموعه منابع اطلاعاتی، فن‌آوری‌ها، انسان‌ها و فرآیندهایی است که به این منابع مرتبط می‌باشند. یکی از راه‌های کم هزینه و موثر در رسیدن به این آرمان افزایش سطح آگاهی کاربران از امنیت اطلاعات و مخاطرات آن است. موضوعی که معمولاً به سادگی از کنار آن می‌گذرند در صورتی که باید در کنار راه‌حل‌های فنی و سیاست‌ها در جهت رسیدن به سطح قابل قبولی از امنیت، مورد توجه ویژه قرار گیرد (Kruger and Kearney, 2006).

بسیاری از سازمان‌ها به اهمیت برقراری یک برنامه برای ارزیابی و آگاهی رسانی پیرامون امنیت اطلاعاتی در سازمان‌هایشان پی برده‌اند. بالا رفتن آگاهی امنیتی افراد می‌تواند به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کرده و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود و سازمان، بیشترین منفعت را از به‌کارگیری فن‌آوری اطلاعات و ارتباطات را در جهت رشد و ترقی خواهد داشت. اگرچه روشی واحد که با تمامی موقعیت‌ها منطبق با سطح سازمانی و انسانی در عملکردهای مختلف برنامه‌های مربوط به آگاهی امنیتی وجود ندارد. داشتن یک روش مشخص برای برقراری یک برنامه برای ارزیابی و ارتقاء دانش کاربران از امنیت اطلاعات امنیتی بر اساس این سطوح بسیار ضروری است. مفهوم و اهمیت ایمنی و امنیت از همان آغاز زندگی بشر وجود داشت، بشر همیشه برای بقا و ادامه زندگی سعی نموده است که آگاهی‌ها و دانش خود را نسبت به محیط و خطرات اطراف خود افزایش دهد. ایمنی و امنیت یک مفهوم ذاتی است که با حفاظت از چیزهای ارزشمند ارتباط پیدا می‌کند؛ و به طور خلاصه ایمنی به راه‌های ممکن که در آن سلامت یک سیستم بایستی تأمین و دفع نقایصی که در راه حصول به اهداف وجود دارد تعریف می‌شود (سادوسکای، ۱۳۸۴).

امروزه در هر لحظه با سر زدن به هر یک از سایت‌های خبر گزارى شاهد نقض امنیت و جرایم اینترنتی، کلاه برداری از حساب‌های شخصی و دولتی و هک شدن تعداد بی‌شماری از سایت‌های حقیقی و حقوقی و غیره می‌باشیم، می‌توان با توجه به این اخبار و ارقام به این نتیجه رسید که امنیت اطلاعات هنوز جایگاه خود را نیافته است هر چند در انتهای دهه ۱۹۸۰ استانداردهای مختلفی برای امنیت اطلاعات همچون، BS7799, ISO/IEC TR13335, ISO/IEC 27001 ایجاد شد و خیلی از سازمان‌ها با پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات (ISMS) برای ارزیابی امنیت سیستم‌های اطلاعاتی تا حدودی امنیت اطلاعات را برای خود تأمین کردند (پاکدامن، ۱۳۸۸). از سال ۲۰۰۰ تا به این زمان، تحقیقات متعددی در ارتباط با ارزیابی و آگاهی از امنیت اطلاعات انجام شده است که در ادامه ارائه شده است.

ماکوناچی<sup>۱</sup> و همکارانش در سال ۲۰۰۱ ابعاد مهم در امنیت اطلاعات را مورد توجه قرار داده‌اند. توجه به مشخصات اصلی امنیت اطلاعات (در دسترس بودن، صحت، قابلیت اعتماد) و اقدامات امنیتی (تکنولوژی، سیاست‌ها، رویه‌ها و آموزش و آگاهی) و وضعیت‌های اطلاعات (وضعیت انتقال و حافظه‌ها و پردازش) در رسیدن به امنیت اطلاعات مورد بررسی قرار گرفت. کراگر و کرنی<sup>۲</sup> در تحقیق، به عمل آمده در سال ۲۰۰۶ در زمینه ارزیابی میزان آگاهی از امنیت اطلاعات در شرکت‌های بین‌المللی معادن، نتایج به دست آوردند. آن‌ها سطوح آگاهی از امنیت اطلاعات را در سه سطح دانش، نگرش و رفتار تقسیم کردند و به این نتیجه رسیدند که در کل، سطح آگاهی کارمندان در حد متوسطی قرار دارد که نیاز به آموزش و توجه بیشتری دارد. پژوهش دیگری که در سال ۲۰۰۷ توسط چانگ<sup>۳</sup> انجام شد نیز ثابت شد فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. یکی از تحقیقات مهم در این زمینه در سال 2008 توسط چو<sup>۴</sup> و همکارانش انجام شد، این بود که افزایش میزان مدیریت آگاهی و دانش کاربران از امنیت اطلاعات تأثیری مستقیم بر نحوه مدیریت عمل و رفتار امنیتی کارکنان خواهد گذاشت و در نتیجه و عملکرد سازمان بهبود خواهد یافت.

در تحقیق دیگری با عنوان مدلی برای آگاهی و ارزیابی امنیت اطلاعات توسط اسمیت و کریتزینگر<sup>۵</sup> در سال 2008 انجام شد، بدنه کلی برای مدیریت امنیت مستخرج شده از اسناد امنیت اطلاعات (همچون استانداردها، گزارش‌ها و NIST و غیره) به دو قسمت موضوعات فنی و غیر فنی تقسیم شد، که از جمله موضوعات غیر فنی تأثیرگذار برای مدیریت امنیت اطلاعات، موضوع عوامل انسانی بود. یکی دیگر از تحقیقاتی که مستقیماً به موضوع آگاهی از امنیت اطلاعات می‌پردازد توسط شو<sup>۶</sup> و همکارانش در سال ۲۰۰۹ با عنوان بررسی ارزیابی غنای اطلاعاتی بر آگاهی از امنیت اطلاعات کاربران در محیط آن‌لاین است. وی آگاهی از امنیت اطلاعات را به سه سطح دریافت<sup>۷</sup>، درک<sup>۸</sup> و برون

---

1 Maconachy

2 Kruger & Kearney

3 Chang Ernest

4 Choi Namjoo

5 E. kritzinger and E Smith

6 Shaw

7 Perception

8 Comprehension