ISSN:2821-1588 htpps://www.jadm.khadu.ir

فصلنامه علمی (( مدیریت دفاع هوایی ))
دوره ۲، شماره ۲ ،اسفند ۱۴۰۲

مقاله پژوهشی

# الگوی صیانت کارکنان در برابر حملات مهندسی اجتماعی

مهدی بصیری[۱]، حسین فتح آبادی[۲]

۱ -دکتری مدیریت فناوری اطلاعات و استادیار دانشگاه فرماندهی و ستاد آجا
۲- دکتری پژوهش عملیاتی و استادیار دانشگاه پدافند هوایی خاتم الانبیا (ص)

اطلاعات مقاله

تاریخ پذیرش: ۱۴۰۲/۱۱ /۱۰

تاریخ دریافت: ۱۴۰۲/۰۴/۰۹

کلمات کلیدی:

الگو، صیانت، مهندسی اجتماعی

نویسنده مسئول:

مهدی بصیری

ایمیل:

abbas.kheyrati@gmail.com

چکیده

امروزه فعالیت در فضای سایبر از آن جهت حائز اهمیت است که سازمان های متولی امر نیازمند سرعت و سهولت در جمع آوری و تحلیل داده ها و اطلاعات مربوط به سایر سازمان های متولی امر صیانت دفاعی در سطح کشور می باشند. هدف از این پژوهش ارائه الگوی صیانت از کارکنان در برابر حملات مهندسی اجتماعی و ارائه راهکارهای افزایش ضریب امنیت این نوع از سازمان ها در برابر حملات مهندسی اجتماعی به ویژه باج‌افزارها می باشد. در این پژوهش اطلاعات و داده‌ها به دو روش کتابخانه ای و میدانی گردآوری گردید. ابزار پژوهش حاضر نیز مصاحبه با کارشناسان و پرسشنامه حاوی تعدادی سؤال درباره‌ی متغیرهای مورد سنجش از جامعه‌ی مورد مطالعه است که روایی و پایایی آن نیز محاسبه و در حد مطلوبی ارزیابی گردید. جامعه آماری این پژوهش شامل کارشناسان فناوری اطلاعات یکی از یگانهای دفاعی مستقردر شهر تهران می‌باشد. تعداد نمونه آماری تحقیق بر اساس جدول ابداعی مورگان محاسبه و روش نمونه‌گیری تصادفی طبقه‌ای ساده می‌باشد. تجزیه و تحلیل داده ها نیز در دو بخش توصیفی و استنباطی انجام شده است که در پایان الگوی صیانت کارکنان در برابر حملات مبتنی بر مهندسی اجتماعی شامل ۶ بعد و ۱۸ مولفه احصاء گردید. این الگو ابزاری مناسب برای استانداردسازی و ارزیابی اقدامات سازمان برای ایمن سازی کارکنان و مقابله با حملات مهندسی اجتماعی ارائه می نماید.

**استناد به مقاله:** مهدی بصیری[۱]، حسین فتح آبادی[۲]. الگوی صیانت کارکنان در برابر حملات مهندسی اجتماعی فصلنامه علمی(مدیریت دفاع هوایی) دوره۲، شماره۴، اسفند ۱۴۰۲.

ISSN:2821-1588 htpps://www.jadm.khadu.ir

Journal of Air Defense Manegment
Vol. 2, No, 4, 1402

Research Paper

# Employee protection model against social engineering attacks

Mehdi Basiri[1], Hossein Fathabadi[2]

1- PhD in Information Technology Management and Assistant Professor at Command University and Aja Headquarters
2- PhD in Operational Research and Assistant Professor of Khatam Al Anbia Air Defense University (PBUH)

**Article Information**

Accepted: 1402/11/10

Recceived:1402/04/09

Keywords:

pattern, conservation, social engineering

Corresponding anuthor:
Abbas Kheyrati
Email:
abbas.kheyrati@gmail.com

**Abstract**

Today, activity in the cyber space is important because the organizations in charge of the matter need speed and ease in collecting and analyzing data and information related to other organizations in charge of defense security at the level of the country. The purpose of this research is to provide a model of protecting employees against social engineering attacks and providing solutions to increase the security factor of this type of organization against social engineering attacks, especially ransom ware. In this research, information and data were collected by library and field methods. The tools of the present research are interviews with experts and a questionnaire containing a number of questions about the measured variables of the studied society, whose validity and reliability were also calculated and evaluated as optimal. The statistical population of this research includes information technology experts of one of the defense units located in Tehran. The number of statistical samples of the research is calculated based on Morgan's innovative table and simple stratified random sampling method. Data analysis has also been done in two parts, descriptive and inferential, and at the end, the model of employee protection against social engineering based attacks included 6 dimensions and 18 statistical components. This model provides a suitable tool for standardizing and evaluating the organization's actions to secure employees and deal with social engineering attacks.

**HOW TO CITE:** Mehdi Basiri[1], Hossein Fathabadi[2]. Employee protection model against social engineering attacks. Journal of Air Defense Manegment, Vol. 2, No, 4, 1402.

## ۱.مقدمه

امروزه استفاده از ابزارهای فناوری اطلاعات و ارتباطات برای تسهیل زندگی بشر در سراسر جهان به عنوان یک راهبرد مهم و پیشرفته مورد توجه قرار گرفته است. رایانه ها، تلفن های همراه هوشمند، اینترنت و شبکه های گسترده اجتماعی مجازی همگی زندگی انسان را تحت تأثیر قرار داده اند. این فضای جدید هم می تواند به عنوان یک فرصت بزرگ مورد استفاده قرار گیرد و هم می تواند تهدیدی جدی برای ادامه حیات باشد. مهندسی اجتماعی یکی از موضوعاتی است که در سالیان اخیر مورد توجه قرار گرفته است.(قوچانی و همکاران، ۱۳۹۴).

مهندسی اجتماعی اصطلاحی است که برای طیف گسترده ای از فعالیت های مخرب انجام می شود که از طریق تعامل انسان انجام می شود. این کار از دستکاری روانشناختی برای فریب کاربران در انجام اشتباهات امنیتی یا دادن اطلاعات حساس استفاده می کند.(وین جون فان و همکاران، ۲۰۱۷)

به منظور تدارک و یا برنامه ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص (روابط عمومی مناسب، ظاهری آراسته و ... ) سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند.

یک مهاجم ممکن است خود را به عنوان فردی موجه و قابل احترام نشان دهد . مثلا" وانمود نماید که یک کارمند جدید است، یک تعمیر کار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید. این امر بیانگر آن است که عامل انسانی بخش اصلی و مهم حملات مهندسی اجتماعی را شامل می گردد. چه اینکه این امکان وجود دارد که کارکنان و نیروی انسانی یک سازمان و یا شرکت بخشی از یک حمله مهندسی اجتماعی می باشند. (فرانکو موتون، ۲۰۱۸)

یک مهاجم، با طرح سوالات متعدد و برقراری یک ارتباط منطقی بین آنان، می تواند به بخش هائی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا نماید. در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نگردد، وی ممکن است با شخص دیگری از همان سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول، توانمندی خود را افزایش دهد.

حملات مهندسی اجتماعی در یک یا چند مرحله اتفاق می افتد. یک نفوذگر ابتدا برای قربانی در نظر گرفته شده برای جمع آوری اطلاعات لازم، از جمله نقاط احتمالی ورود و پروتکل های امنیتی ضعیف ، برای انجام حمله ، تحقیق می کند. سپس، مهاجم برای جلب اعتماد قربانی و ایجاد انگیزه برای اقدامات بعدی که باعث نقض اقدامات امنیتی می شود ، مانند افشای اطلاعات حساس یا دسترسی به منابع مهم، تلاش می کند(هانگی، ۲۰۱۱).

نیروی پدافند هوایی آجا به جهت نوع ماموریت و فعالیت های تخصصی همواره با اطلاعات حساس و طبقه بندی شده سرو کار دارند. و این امر موجب می‌گردد تا همواره سیستم ها و کارکنان این سازمان در معرض تهدید حملات رایانه ای از نوع مهندسی اجتماعی قرار گیرند. لذا آگاهی کارکنان از چگونگی تشخیص و مقابله با این نوع حملات ضرورتی اجتناب ناپذیر خواهد بود. به ویژه که ماهیت اطلاعاتی که کارکنان این نوع از سازمان ها با آن سرو کار دارند همواره برای کشور حیاتی و مهم بوده و سرقت و یا دسترسی غیر مجاز به این نوع از اطلاعات می تواند صدمات و آسیب های جبران ناپذیری را برای امنیت ملی کشور فراهم سازد. بر این اساس مقاله پیش رو به دنبال پاسخ به این مساله اساسی است که الگوی صیانت کارکنان در مقابل حملات مبتنی بر مهندسی اجتماعی کدام می باشد؟

## مبانی نظری و پیشینه:

مهندسی اجتماعی بیشتر هنر بهره‌گیری از روانشناسی رفتار افراد است تا مجموعه‌ای از تکنیک‌های فنی هک کردن. مجرمان از این هنر برای دسترسی به ساختمان‌ها، سیستم‌ها یا داده‌ها استفاده می‌کنند. با تمرین می‌توان نشانه‌های به‌کارگیری مهندسی اجتماعی را تشخیص داد. در ادامه‌ی این مطلب متداول‌ترین تکنیک‌های مهندسی اجتماعی، شناخته شده‌ترین حملات مبتنی بر مهندسی اجتماعی و راهکارهای مقابله با این تکنیک‌ها را بیان خواهیم کرد.

ایده مهندسی اجتماعی و بسیاری از تکنیک‌های موجود در این زمینه قدمتی برابر با وجود کلاهبرداران و کلاهبرداری دارد، اما اصطلاح **مهندسی اجتماعی** در دهه آخر قرن بیستم میلادی عمومیت یافته که هکر مشهورکوین مینتیک (Kevin Mitnick) نقشی اساسی در این موضوع داشته است.

حتی به‌کارگیری تمام تجهیزات امنیتی مورد نیاز برای تامین امنیت مراکز داده، فضای ابری و محیط فیزیکی ساختمان شرکت، سرمایه‌گذاری بر روی فناوری‌های دفاعی، استفاده از سیاست‌ها و

فرایندهای امنیتی مناسب و بررسی و بهبود مداوم اثرگذاری این سیاست‌ها و فرایندها نیز ممکن است برای جلوگیری از ورود یک مهندس اجتماعی ماهر کافی نباشد.(ساندوکا، ۲۰۰۹)

## تعریف مهندسی اجتماعی:

مهندسی اجتماعی، هنر متقاعد کردن کاربران برای نفوذ به سیستم‌های اطلاعاتی است. مهندسین اجتماعی به جای استفاده از حملات فنی علیه سیستم‌ها، انسان‌هایی را که به اطلاعاتی خاص دسترسی دارند، مورد هدف قرار داده و آنها را تشویق به افشای اطلاعات حساس می‌کنند و یا حتی حملات مخربشان را از طریق نفوذ به افراد و متقاعد کردن آنها اجرا می‌کنند. در حالی که مردم تصور می‌کنند که در شناسایی چنین حملاتی مهارت دارند، تحقیقات نشان می‌دهند که مردم در شناسایی دروغ و فریب عملکرد ضعیفی دارند(کرامبلز و همکاران، ۲۰۱۵)

## انواع حملات مهندسی اجتماعی:

حملات مهندسی اجتماعی به اشکال مختلفی رخ می دهد و می‌تواند در هر جایی که تعامل انسان در آن دخیل باشد، انجام شود. در ادامه به معرفی انواع مرسوم از حملات مهندسی اجتماعی می پردازیم:

**گذاشتن طعمه (Baiting):** مهاجم یک دستگاه فیزیکی آلوده به بدافزار مانند فلش مموری Universal Serial Bus را در مکانی که مطمئن است پیدا می شود ، رها می کند. سپس هدف دستگاه را برداشته و آن را در کامپیوتر خود قرار می دهد و بدافزار را ناخواسته نصب می کند.

**فیشینگ (Phishing)** : هنگامی که هکر یک ایمیل تقلبی به عنوان یک ایمیل مجاز ارسال می کند، که اغلب ادعا می شود از یک منبع قابل اعتماد است. این پیام به منظور فریب گیرنده است تا اطلاعات مالی یا شخصی را به اشتراک بگذارد یا روی لینکی که بدافزار یا ویروس را نصب می کند کلیک کند.

**فیشینگ هدف دار (Spear phishing):** این مانند فیشینگ است ، اما حمله برای فرد یا سازمان خاصی طراحی شده است.

**ویشینگ (Vishing) :** که به عنوان فیشینگ صوتی نیز شناخته می شود، شامل استفاده از مهندسی اجتماعی از طریق تلفن برای جمع آوری اطلاعات مالی یا شخصی از هدف است.

**حمله Whaling** : نوع خاصی از حملات فیشینگ ، حمله نهنگ ، کارکنان برجسته را هدف قرار می دهد مانند مدیر مالی یا مدیر اجرایی، تا کارمند هدف را فریب داده و اطلاعات حساس را فاش کند.این سه نوع حملات فیشینگ زیر چتر وسیع مهندسی اجتماعی قرار دارند.

**بهانه گیری (Pretexting)** : یکی از طرفین برای دسترسی به داده های ممتاز به دیگری دروغ می گوید. به عنوان مثال ، یک کلاهبردار به بهانه ای می تواند تظاهر کند برای تأیید هویت گیرنده به داده های مالی یا شخصی نیاز دارد.

**ترس افزار (Scareware)** : این شامل فریب قربانی می شود تا فکر کند رایانه اش آلوده به بدافزار است یا سهواً محتوای غیرقانونی دانلود کرده است. سپس مهاجم به قربانی راه حلی ارائه می دهد که مشکل ساختگی را برطرف می کند. در واقع ، قربانی به سادگی فریب داده می شود که بدافزار مهاجم را دانلود و نصب کند.

**گودال آب (Watering hole)** : مهاجم سعی می کند گروه خاصی از افراد را با آلوده کردن وب سایت هایی که شناخته شده اند و با هدف دسترسی به شبکه مورد اعتماد قرار می دهند ، به خطر اندازد .

**سرقت انحرافی (Diversion theft)** : در این نوع حملات ، مهندسان اجتماعی یک شرکت حمل و نقل یا پیک را فریب می دهند تا به محل تحویل یا خروج اشتباه برود ، بنابراین معامله را قطع می کند.

**طعمه گذاری Quid pro quo** : این یک حمله است که در آن مهندس اجتماعی وانمود می کند که در ازای اطلاعات یا کمک هدف چیزی ارائه می دهد. به عنوان مثال ، یک هکر با مجموعه ای از شماره های تصادفی در یک سازمان تماس می گیرد و وانمود می کند که یک متخصص پشتیبانی فنی است در نهایت ، هکر شخصی را پیدا می کند که دارای مشکل فنی قانونی است و سپس تظاهر می کند که به او کمک می کند. از طریق این تعامل ، هکر می تواند نوع مورد نظر در دستورات راه اندازی بدافزار را داشته باشد یا می تواند اطلاعات رمز عبور را جمع آوری کند.

**هانی پات (Honey trap)** : در این حمله، مهندس اجتماعی وانمود می‌کند که فردی جذاب برای تعامل با یک فرد آنلاین ، جعل یک رابطه آنلاین و جمع آوری اطلاعات حساس از طریق آن رابطه است.

**Tailgating** : گاهی اوقات به نام Piggybacking از ، فاصله با اتومبیل جلویی است. در این حمله فرض می کند که شخصی که به ساختمان دسترسی قانونی دارد به اندازه کافی مودب است و می تواند درب را برای شخصی که پشت سرش است باز نگه دارد ، با این فرض که اجازه دارد در آنجا باشد. ورود به ساختمانی بدون کارت ورود.

**نرم افزار امنیتی سرکش (Rogue security software)** : این یک نوع بدافزار است که هدف آن پرداخت هزینه، برای حذف جعلی بدافزار است.

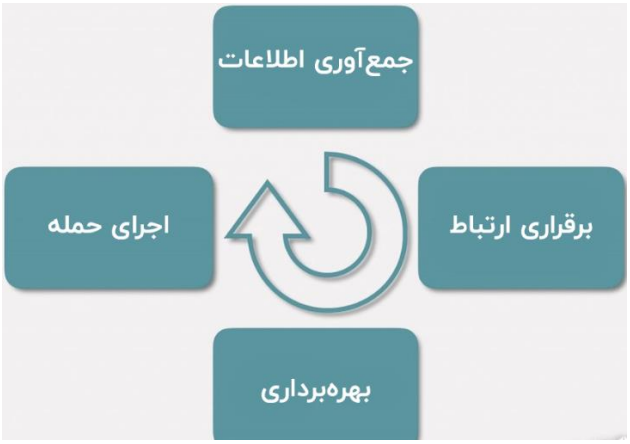
**شیرجه در زباله (Dumpster diving)** : این یک حمله مهندسی اجتماعی است که به موجب آن شخصی برای یافتن اطلاعاتی مانند گذرواژه ها یا کدهای دسترسی نوشته شده روی یادداشت های چسبنده یا کاغذ ، که می تواند برای نفوذ به شبکه سازمان مورد استفاده قرار گیرد ، سطل زباله شرکت را جستجو می کند.

**فارمینگ (Pharming)** : با این نوع کلاهبرداری آنلاین ، یک مجرم سایبری کد مخرب را روی رایانه یا سرور نصب می کند که به طور خودکار کاربر را به یک وب سایت جعلی هدایت می کند، جایی که ممکن است کاربر در ارائه اطلاعات شخصی فریب بخورد.

## چرخه مهندسی اجتماعی

گارتنر در مقاله‌ای راجع به روش‌های دفاع در مقابل حملات مهندسی اجتماعی، اذعان کرد هر جرمی دارای الگوی متداولی می‌باشد. برای مهندسی اجتماعی نیز الگویی وجود دارد، که قابل تشخیص و قابل جلوگیری می‌باشد. این الگو به صورت چرخه‌ای در شکل نشان داده شده‌است. این چرخه شامل چهار مرحله، جمع‌آوری اطلاعات، برقراری ارتباطات بهره‌کشی و عمل و اجرا است، که مانند تکه‌های پازل به هم مرتبط و وابسته‌اند.

- جمع‌آوری اطلاعات
- برقراری ارتباطات
- بهره‌کشی
- عمل و اجرا (گارتنر، ۲۰۰۲)




**شکل ۱:** چرخه مهندسی اجتماعی

## شناسایی انواع حملات مهندسی اجتماعی

ریشه بسیاری از حملات باج‌افزارها، حمله مهندسی اجتماعی است که شامل دستکاری شخص یا اشخاصی برای دسترسی به سیستم‌های کاربران، شرکت و اطلاعات آنهاست. وظیفه مهم مهندسی اجتماعی جلب اعتماد قربانی است. برای نمونه، مهاجم با استفاده از حمله مهندسی اجتماعی، به جای صرف کلی وقت برای پیدا کردن رمزعبور، کاری می‌کند که خود قربانی آن را تحویل وی بدهد.. (تورنتون، ۲۰۱۷)

## فیشینگ

رایج‌ترین حمله مهندسی اجتماعی ، فیشینگ[1] است. در فیشینگ، حمله از طریق ایمیل، چت، وب‌سایت یا آگهی‌های تبلیغاتی انجام می‌شود، و مهاجم سعی می‌کند از طریق جعل هویت سازمان یا شرکت، اعتماد قربانی را جلب کند. پیغام‌های فیشینگ می‌تواند از طرف بانک، شرکت‌های بزرگ و حتی دولت باشد. رفتارهای فیشینگ بسیار متنوع هستند. برخی از آنها ازکاربر نهایی درخواست می‌کنند که اطلاعات ورود حساب کاربری‌اش را تائید کند، و برای این منظور فرم ورودی با لگو و ظاهر وب‌سایت مورد نظر آماده می‌کنند. برخی از آنها کاربر را برنده یک مسابقه یا قرعه کشی اعلام

[1] Phishing

می‌کنند و برای پرداخت جایزه، درخواست اجازه دسترسی به حساب بانکی یا کاربری آنان را دارند. برخی از آنها با سو استفاده از حوادث طبیعی مانند سیل، زلزله و یا تاریخ‌های خاص شروع به جمع‌آوری کمک‌های مردمی می‌کنند.

### طعمه گذاری

طعمه گذاری[۲] هم شبیه فیشینگ است. در این نوع از حمله با ارائه چیز قابل توجه و جذابی به کاربر، از وی درخواست اطلاعات شخصی یا اطلاعات ورود به حساب‌های کاربری‌اش را می‌کنند. طعمه به شکل‌های مختلفی ارائه می‌شود. از طریق دنیای دیجیتال، مانند دانلود فیلم یا موزیک در سایتpeer-to-peer ، یا به صورت فیزیکی در دنیای واقعی، مانند جا گذاشتن حافظه USB با برچسب قابل توجه مانند اطلاعات حقوق سه ماه اول، روی میز کارمندان. به محض اینکه موزیک دانلود شد یا حافظه USB به دستگاه کاربر متصل شد، نرم‌افزارهای مخرب وارد دستگاه کاربر می‌شوند و خرابکار کار خودش را شروع می‌کند.

## دفاع در برابر مهندسی اجتماعی

دفاع در مقابل حملات مهندسی اجتماعی سخت‌تر از دفاع در برابر سایر مخاطرات امنیتی بوده و جزء سخت‌ترین نوع دفاع‌ها خواهد بود. زیرا انسان‌ها، رفتارها و عکس العمل‌های آنها بسیار پیچیده و غیرقابل پیش بینی می‌باشد؛ بنابراین برای دفاع در مقابل حملات مهندسی اجتماعی، ابتدا نیاز به شناسایی محرک‌های روانشناسی متقاعدسازی و سپس تکنیک‌های مورد استفاده در حملات داریم. با توجه به اینکه هیچ استاندارد خاصی برای دفاع و پیش گیری از حملات مهندسی اجتماعی وجود ندارد، بهترین راه برای دفاع، شناسایی سطوح مختلف دفاع و ایجاد سیاست‌های امنیتی دقیق و آموزش کارکنان در راستای دنبال کردن این سیاست‌ها می‌باشد. به طور کلی گام‌های کلیدی برای ایجاد دفاعی مؤثر در سازمان عبارتند از:

- شناسایی محرک‌های روانشناسی متقاعدسازی
- آشنایی با تکنیک‌های حمله مهندسی اجتماعی
- شناسایی سطوح مختلف دفاع
- استراتژی‌ها ی دفاع

[12] ***Baiting***

## استراتژی‌های رویارویی با حملات مهندسی اجتماعی

استراتژیهای مستند شده پاسخگویی، این اطمینان را به وجود می‌آورند که کارمند درشرایط ای که تحت فشار است، دقیقاً بداند که باید از چه رویه‌هایی پیروی کند. بعنوان مثال، اگر کارمند درخواستی را دریافت کرد، صحت آن را قبل از عمل به آن دستورالعمل، برررسی کند و اگر قبلاً به آن درخواست عمل کرده بود، باید رئیس را از این موضوع مطلع کند. از این به بعد، این مسئولیت رئیس است که مطمئن شود هیچ کارمند دیگری به درخواست‌های مشکوک پاسخ نمی‌گوید.

## استراتژی‌های محافظت از پسورد و روش‌های صحه گذاری

متداول‌ترین اطلاعاتی که مهاجم مهندسی اجتماعی سعی در آگاهی از آن دارد، دانستن رویه‌های اعتبار سنجی می‌باشد. به محض اینکه پسورد کارمندی لو برود، هکر کنترل اوضاع را در دست خواهد گرفت و به سازمان ضرر خواهد رساند. سیاست پسورد بسیار ساده‌است. درباره پسورد هرگز، نه تنها در تلفن بلکه هر زمان دیگر صحبت نکنید. کاربران باید بطور کامل از اهمیت پسوردشان آگاه باشند و اگر به آنها آموزش لازم داده نشود آن را بدون هیچ فکر و واهمه‌ای در اختیار دیگران قرار می‌دهند. پسوردها باید در زمانهای متوالی تعویض شوند و قوانین پسورد توسط مدیران ارشد به کارمندان القاء شود. البته راه حل‌های تکمیلی دیگری چون PIN و ID کارت‌ها نیز برای حفظ دسترسی به سیستم‌های مهم وجود دارد. البته باید توجه کرد که اولین اقدام هر هکر آن خواهد بود که در اولین فرصت PINها را عوض کند.

## استفاده از رویه‌های احسن برای کاهش ریسک

- برای سنجش وضعیت کارمندان و پیمانکاران، رویه‌های صحه گذاری باید مد نظر قرار گیرد.
- سیستم‌های طبقه‌بندی داده با چارچوب‌هایی برای آزادسازی اطلاعات در هر سطح، تدوین شود.
- برای پیامدهای امنیتی تمامی کارمندان، برنامه آموزشی گذاشته شود.
- پرسنل کلیدی باید آموزش‌هایی برای مقاومت در برابر حملات مهندسی اجتماعی ببینند.
- تست‌های نفوذ پذیری و اطمینان از اطلاعات بطور مستمر، برای توسعه آگاهی و بازخورد سریع از کارمندان گرفته شود.
- بطور مستمر و اتفاقی، مانورهای مهندسی اجتماعی در سازمان انجام شود.
- به کارمندان آموزش داده شود که قسمت حیاتی از سیستم امنیتی را تشکیل می‌دهند و در برابر آن مسئول هستند.

- تمام کارمندان باید از حملات مهندسی اجتماعی آگاه باشند. تا خود قاضی خود باشند و مثلاً اگر فکر می‌کنند نامه‌ای مشکوک است، آن را باز نکنند.
- باید به تمام کارمندان فنی مفاهیم اسب تراوا و نامه‌های زنجیره‌ای توضیح داده شود.
- به تمام کاربران سیستم اطلاعاتی باید آموزش داده شود که چگونه از نرم‌افزارهای ضد ویروس استفاده کنند و آن را بروز رسانی کنند. نیز آگاه باشند که پیوست نامه‌های الکترونیکی و لینک‌های ناشناخته را باز نکنند.
- به کارمندان آموزش داده شود که چگونه مودبانه با افرادی که دارای قدرت بالاتری هستند ولی درخواست‌های نا معقول دارند، برخورد کنند.
- آگاهی باید همواره در سطح بالایی قرار گیرد. به همین دلیل باید دوره‌های بروزرسانی وجود داشته باشد و بعنوان مثال در آن‌ها نمونه‌های جدید حملات مهندسی اجتماعی بیان شود.
- عمق دفاع در سیستم جزء مهمی در امنیت است و از حمله‌های چندگانه جلوگیری می‌کند. باید از چک کردن‌های دولایه یا سه لایه استفاده شود.
- باید ممیزی‌های مستمری وجود داشته باشد و رویه‌های امنیتی با استفاده از کارمندان همواره تست شود. مثلاً چک شود که دستگاه‌های غیرمجاز به سیستم اطلاعاتی سازمان، متصل نشده باشند.
- تهدیدهای درونی شناسایی شوند. پیمانکاران و دانشی را که کارمندان هنگام ترک سازمان با خود می‌برند. کنترل شود.
- برای رسانه‌های مشکوک، مدیریت و برنامه‌ریزی وجود داشته باشد.

### فرهنگ امنیت

ایجاد فرهنگ امنیت اطلاعات در سازمان، فرایندی است اثر بخش که گامهای زیر را در بر خواهد داشت:

- ایجاد آگاهی از حملات امنیتی در کارمندان
- فراهم سازی ابزارهای مقابله
- برقراری ارتباطات دو طرفه میان پرسنل امنیت، مدیران و کارمندان

ایجاد فرهنگ امنیت، امری زمان بر بوده و به آن با عنوان سرمایه‌گذاری بلند مدت باید نگاه کرد که نیاز به تلاش مستمر، بهبود و نگه داری دارد.

## بررسی اعتبار

اعتبارسنجی مدارک و احراز هویت باید در سازمان نهادینه شود و برای تمام کسانی که به ادعا یا سمتشان شک می‌رود مورد استفاده قرار گیرد؛ چه یونیفرم سازمان را پوشیده باشد و چه ادعا کند که در حالت اضطراری هستند. بررسی اعتبار سه مرحله دارد:

- اعتبار سنجی مشخصات
- اعتبار سنجی رتبه کارمندی
- اعتبار سنجی «نیاز به دانستن»

چنین استراتژی‌های اعتبار سنجی فقط زمانی مؤثر خواهد بود که به‌عنوان سیاست‌های امنیتی توسط مدیر ارشد پشتیبانی شوند. از آنجایی که مهندس اجتماعی از توانایی دسترسی افراد به اطلاعات، سوء استفاده می‌کند؛ بنابراین اگر کسی مدیر ارشد را برای احراز هویتش به چالش بیندازد، نباید او را سرزنش کرد. اگر با کارمندان بطور مسالمت آمیزی رفتار نشود، آنها توانایی و دلگرمی خود را در چالش کشیدن هر کسی که ادعای ارشد بودن می‌کند را از دست خواهند داد؛ بنابراین باید به آنها آموزش داد تا به گونه‌ای دوستانه از دیگران بخواهند که خودشان را به سازمان بشناسانند.

## ممیزی پذیرش و کاربری سیاست‌ها

تدوین استراتژی‌ها، سیاست‌ها و کارمندان آموزش دیده در صورتیکه موافقتی با آن وجود نداشته باشد، کاملاً بی‌ارزش خواهد بود؛ بنابراین نیاز به ممیزی کاربری سیاست‌ها در سازمان می‌باشد. برای مثال، هنگامیکه تضمین کیفیت برای پروژه‌ای اجرا می‌شود، یکی از گام‌ها، ارزیابی پذیرش سیاست‌های امنیتی در سازمان می‌باشد. برای مثال رویه‌های ممیزی خاصی باید وجود داشته باشد تا مطمئن شویم کارمند Helpdesk، درباره پسورد، پشت تلفن یا از طریق نامه‌های رمزنگاری نشده، صحبت نمی‌کند. مدیران نیز باید بطور دوره‌ای دسترسی‌های کارمندانشان را بازنگری کنند. ممیزی امنیتی نیز باید اطمینان حاصل کند که افراد دیگر دسترسی‌های غیرلازم را ندارد. نقاط دسترسی نیز مانند درب‌ها و... باید همواره مانیتور شوند. بدین ترتیب اطمینان حاصل می‌شود که کارمندان سیاست‌های امنیتی را برای دسترسی به نقاط امن، رعایت می‌کنند. محل کار کارمندان نیز باید بطور تصادفی مورد بازرسی قرار گیرد تا مطمئن شویم اسناد محرمانه در کمدهای امن قرار گرفته‌اند. محل‌های کار نیز خارج از زمان های کاری، باید همواره قفل باشند. (آلن و همکاران، ۲۰۰۶)

## پیشینه تحقیق:

فرانکوس موتون(۲۰۱۸) در تحقیقی با عنوان « مدل شناسایی حملات مهندسی اجتماعی» به دنبال بازنگری در مدل های موجود در زمینه شناسایی حملات مبتنی بر مهندسی اجتماعی بوده است. وی در مطالعه خود نسبت به معرفی سه مدل جهت شناسایی حملات مهندسی اجتماعی اقدام نمود. در مدل اول که برای یک مرکز تلفن طراحی شده بود جهت منع حملات در ارتباطات دو طرفه مورد استفاده قرار گرفت. مدل دوم وی برای جلوگیری از حملات مهندسی اجتماعی در ارتباطات یک طرفه طراحی گردید. مدل سوم وی برای ممانعت از حملات در ارتباطات خودکار محدود طراحی گردید.

کایل تورنتن(۲۰۱۷) در تحقیقی با عنوان «شناسایی انواع حملات مهندسی اجتماعی و راه کارهای مقابله با آن» ضمن تشریح تفصیلی حملات مهندسی اجتماعی به شناسایی و طبقه بندی انواع این حملات پرداخته است. وی ضمن بر شمردن تعدادی از حملات به راهبردهای مقابله با این حملات از جمله مدیریت آگاهانه، حفاظت فیزیکی، آموزش کارکنان، خط و مشی های امنیتی شفاف اشاره می نماید.

کوته اشمیت(۲۰۱۶) در تحقیقی با عنوان « امنیت سایبری، ریسک، و آسیب پذیری ها و شاخص های جلوگیری از حملات مهندسی اجتماعی » به بررسی تهدیدات این نوع از حملات در فضای سایبری اقدام نموده است. وی در تحقیق خود برتدوین استانداردها و خط و مشی های امنیتی برای دارایی های سخت افزاری و نرم افزاری شرکت ها و نیز آموزش قوانین و مقررات به کارکنان را در جلوگیری از حملات مهندسی اجتماعی موثر دانسته است.

مارتین لیختنشتاین (۲۰۱۵) در تحقیقی با عنوان « مهندسی اجتماعی و کاهش ریسک های انسانی» به بررسی عوامل موثر بر کاهش ریسک ناشی از حملات مهندس اجتماعی در اثر خطاهای نیروی انسانی سازمان ها پرداخته است. وی در این تحقیق با تمرکز بر عوامل انسانی به شناسایی هشت مولفه موثر در این زمینه پرداخته است. مهمترین این مولفه ها شامل آموزش منابع انسانی، تدوین خط و مشی های امنیتی شفاف، جلب اعتماد کارکنان و مدیریت دسترسی می باشد.

فرانکو موتون (۲۰۱۴) در تحقیقی با عنوان « چارچوب حملات مهندسی اجتماعی» ضمن بررسی الزامات امنیتی در زمینه مقابله با حمله نوع مهندسی اجتماعی به ارائه مولفه ها و عناصر دخیل در این امر پرداخته است. نتایج پژوهش وی بیانگر آن است که افزایس سطح آگاهی کارکنان سازمان به همراه کنترل موثر دسترسی ها از مهم ترین مولفه های چارچوب ارائه شده می باشد.

## روش شناسی تحقیق:

تحقیق حاضر از نظر هدف کاربردی می‌باشد. همچنین تحقیق حاضر از نظر گردآوری داده‌ها و اطلاعات و روش تجزیه و تحلیل توصیفی- پیمایشی می باشد. برای کسب اطمینان از اعتبار ابزار از ضریب آلفای کرونباخ استفاده می شود که بعد از توزیع ۲۰ پرسشنامه، پایایی متغیرهای پرسشنامه بصورت پیش آزمون و همچنین مقدار آلفای نهایی در جدول زیر آورده شده است .

$$\alpha = \left(\frac{j}{j-1}\right)\left(1 - \frac{\sum s^2 j}{s^2}\right)$$

در این فرمول $\alpha$ برآورد اعتبار آزمون، $J$ تعداد سوال های آزمون، $s^2 j$ واریانس زیر مجموعه $j$ ام و $s^2$ واریانس است .

**جدول۱:** پایایی متغیرهای تحقیق

| متغیر | آلفای کرونباخ |
|---|---|
| استفاده از تلفن همراه | ۰.۸۳۴ |
| آگاهی از مد | ۰.۷۲۴ |
| رهبری | ۰.۸۱۷ |
| آگاهی از سلامت | ۰.۷۲۴ |
| آسوده خاطر بودن | ۰.۷۴۳ |
| آگاهی از جامعه | ۰.۷۴۴ |
| آگاهی از هزینه | ۰.۸۴۱ |
| کاربردی بودن | ۰.۹۲۸ |

جامعه آماری این پژوهش شامل کارکنان سازمان هدف در شهر تهران می باشد. روش نمونه گیری تحقیق حاضر تصادفی ساده می باشد.

از آنجائی که جامعه آماری تحقیق حاضر شامل کارکنان سازمان هدف در شهر تهران بوده و تعداد آنها نامشخص می باشد، جهت تعیین حداقل حجم نمونه لازم، از فرمول کوکران برای جامعه نامحدود استفاده گردید:

$$n = \frac{z^2 pq}{d^2}$$

$$n = \frac{(1/96)^2 (0/5)(1-0/5)}{(0/5)(1-0/5)} \approx 178$$

که در آن:

n= حداقل حجم نمونه لازم

p= نسبت توزیع صفت در جامعه

zα/2= مقدار به دست آمده از جدول توزیع نرمال استاندارد (در این تحقیق و با در نظر گرفتن مقدار خطای ۰/۰۵، مقدار به دست آمده از جدول توزیع نرمال استاندارد ۱/۹۶ می‌باشد).

d= خطای پذیرفته شده توسط محقق یا بازه قابل تحمل از برآورد پارامتر مورد نظر (معمولاً در علوم اجتماعی برابر ۰/۰۵ در نظر گرفته می‌شود.).

نکته‌ای که لازم است در خصوص این فرمول، گفته شود آن است که چنان‌چه مقدار p در دسترس نباشد، می‌توان مقدار ۰/۵ را برای آن در نظر گرفت، که در این حالت، این فرمول بزرگترین و محافظه کارانه‌ترین عدد ممکن را به دست خواهد داد، که در این تحقیق نیز عدد ۰/۵ برای آن در نظر گرفته شد. با جایگذاری پارامترها در فرمول مذکور حجم نمونه لازم با اعمال ظریب امنیتی ۴۸۴ نفر خواهد بود.

## یافته های تحقیق:

### الف: یافته های جمعیت شناسی تحقیق

## بررسی وضعیت تحصیلات در نمونه آماری

**جدول ۲:** بررسی وضعیت تحصیلات در نمونه آماری

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1 | 8 | 8.9 | 8.9 | 8.9 |
| | 2 | 64 | 71.1 | 71.1 | 80.0 |
| | 3 | 14 | 15.6 | 15.6 | 95.6 |
| | 4 | 4 | 4.4 | 4.4 | 100.0 |
| | Total | 90 | 100.0 | 100.0 | |

با توجه به جدول شماره 2 می‌توان بیان نمود که فوق‌دیپلم ۸.۹ درصد، افراد لیسانس ۷۱.۱درصد، فوق‌لیسانس ۱۵.۶ درصد، و دکتری ۴.۴ درصد از کل نمونه تحقیق را تشکیل می‌دهند.

## بررسی وضعیت سن در نمونه آماری

**جدول ۳:** بررسی وضعیت سن در نمونه آماری

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1 | 38 | 42.2 | 42.2 | 42.2 |
| | 2 | 42 | 46.7 | 46.7 | 88.9 |
| | 3 | 10 | 11.1 | 11.1 | 100.0 |
| | Total | 90 | 100.0 | 100.0 | |

با توجه به جدول شماره ۳ می‌توان بیان نمود که ۴۲.۲ درصد افراد دارای سن بین ۲۰ تا ۳۰ سال، ۴۶.۷ درصد بین ۳۱ اتا ۴۱ سال، ۱۱.۱درصد بیش از ۴۲ سال سن داشته‌اند.

## بررسی وضعیت سابقه کاری

**جدول ۴:** بررسی وضعیت سابقه کاری در نمونه آماری

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1 | 41 | 45.6 | 45.6 | 45.6 |
| | 2 | 33 | 36.7 | 36.7 | 82.2 |
| | 3 | 4 | 4.4 | 4.4 | 86.7 |
| | 4 | 10 | 11.1 | 11.1 | 97.8 |
| | 5 | 2 | 2.2 | 2.2 | 100.0 |
| | Total | 90 | 100.0 | 100.0 | |

با توجه به جدول شماره۴ می‌توان بیان نمود که ۱۱.۱ درصد افراد نمونه آماری ما دارای سابقه کاری بین ۱۵ الی ۲۰ سال، ۴.۴ درصد دارای سابقه کاری بین ۱۰ الی ۱۵ سال، ۲.۲ درصد دارای

سابقه کاری ۲۰ سال به بالا، ۳۶.۷ درصد دارای سابقه کاری بین ۵ الی ۱۰ سال و ۴۵.۶ درصد دارای سابقه زیر ۵ سال بوده‌اند.

## ب) یافته‌های استنباطی:

در این بخش از تحقیق به بررسی الگوی تحقیق و همچنین تحلیل روابط بین متغیرهای تحقیق می‌پردازیم.

هر ۳ سوال یک عامل را بررسی می کند و هر سوال با ۵ گزینه ارزیابی می شود . در بررسی های انجام شده در نرم افزار SPSS دو گزینه ای که به عنوان ریسک پذیری بالا مورد نظر بود یک، و سه گزینه ی دیگر صفر در نظر گرفته شده اند.

در ادامه به بررسی رابطه بین هر یک از عوامل با سن، جنسیت، سابقه کاری، تاهل، تحصیلات و واحد سازمانی از طریق انجام آزمون مربع کای[3] در نرم افزار SPSS پرداخته شده است.

آزمون خی‌دوی یا آزمون کی دو یا خی دو یا مربع کای از آزمون‌های آماری و از نوع ناپارامتری است و برای ارزیابی همقوارگی متغیرهای اسمی به کار می‌رود.

$$\chi^2 = \sum_{t=1}^{m} \frac{(O_t - E_t)^2}{E_t}$$

فراوانی‌های مشاهده شده = O

فراوانی‌های مورد انتظار = E

اگر میزان بدست آمده برای این آزمون کمتر از ۰.۱ باشد، نشان دهنده میزان اختلاف معنی دار بین متغیرها است.

این آزمون تنها راه حل موجود برای آزمون همگنی در مورد متغیرهای مقیاس اسمی با بیش از دو مقوله‌است، بنابراین کاربرد خیلی زیادتری نسبت به آزمونهای دیگر دارد. این آزمون نسبت به حجم نمونه حساس است.

آزمون کای اسکوئر برای تعیین تفاوت‌ها میان چند چیز هم بکار می‌رود.

[3] Chi-squared test

## بررسی رابطه بین متغیرهای دموگرافی با عامل ترس

### بررسی رابطه بین جنسیت و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۵**:بررسی رابطه بین جنسیت و ترس

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | 2.992[a] | 1 | .084 | | |
| Continuity Correction[b] | 2.052 | 1 | .152 | | |
| Likelihood Ratio | 3.430 | 1 | .064 | | |
| Fisher's Exact Test | | | | .136 | .071 |
| Linear-by-Linear Association | 2.958 | 1 | .085 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۵ برای Pearson Chi-Square که برابر است با ۰.۰۸۴ اختلاف معنا داری از لحاظ ترس در میان مردان و زنان وجود دارد.

### بررسی رابطه بین سن و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

جدول ۶: **بررسی رابطه بین سن و ترس**

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | .911[a] | 2 | .634 |
| Likelihood Ratio | .920 | 2 | .631 |
| Linear-by-Linear Association | .535 | 1 | .465 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۶ برای Pearson Chi-Square که برابر است با ۰.۶۳۴ اختلاف معنا داری از لحاظ ترس در رده های سنی مختلف وجود ندارد.

## بررسی رابطه بین تحصیلات و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۷:** بررسی رابطه بین تحصیلات و ترس

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 9.149[a] | 3 | .027 |
| Likelihood Ratio | 14.031 | 3 | .003 |
| Linear-by-Linear Association | 6.668 | 1 | .010 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۷ برای Pearson Chi-Square که برابر است با ۰.۰۲۷ اختلاف معنا داری از لحاظ ترس در رده های تحصیلی مختلف وجود دارد.

## بررسی رابطه بین سابقه کاری و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۸** :بررسی رابطه بین سابقه کاری و ترس

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 3.973[a] | 4 | .410 |
| Likelihood Ratio | 5.585 | 4 | .232 |
| Linear-by-Linear Association | 1.605 | 1 | .205 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۸ برای Pearson Chi-Square که برابر است با ۰.۴۱۰ اختلاف معنا داری از لحاظ ترس با سابقه کاری وجود ندارد.

## بررسی رابطه بین واحد سازمانی و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۹** : بررسی رابطه بین واحدسازمانی و ترس

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .013[a] | 1 | .908 | | |
| Continuity Correction[b] | .000 | 1 | 1.000 | | |
| Likelihood Ratio | .013 | 1 | .908 | | |
| Fisher's Exact Test | | | | 1.000 | .564 |
| Linear-by-Linear Association | .013 | 1 | .909 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۹ برای Pearson Chi-Square که برابر است با ۰.۹۰۸ اختلاف معنا داری از لحاظ ترس در واحدهای سازمانی مختلف وجود ندارد.

## بررسی رابطه بین متغیرهای دموگرافی با عامل طمع

## بررسی رابطه بین جنسیت و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۰**: بررسی رابطه بین جنسیت و طمع

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | 8.473[a] | 1 | .004 | | |
| Continuity Correction[b] | 6.661 | 1 | .010 | | |
| Likelihood Ratio | 7.380 | 1 | .007 | | |
| Fisher's Exact Test | | | | .007 | .007 |
| Linear-by-Linear Association | 8.379 | 1 | .004 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۱۰ برای Pearson Chi-Square که برابر است با ۰.۰۰۴ اختلاف معنا داری از لحاظ طمع در بین مردان و زنان وجود دارد.

## بررسی رابطه بین سن و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۱:** بررسی رابطه بین سن و طمع

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 3.297[a] | 2 | .192 |
| Likelihood Ratio | 5.330 | 2 | .070 |
| Linear-by-Linear Association | 2.527 | 1 | .112 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۱۰ برای Pearson Chi-Square که برابر است با ۰.۱۹۲ اختلاف معنا داری از لحاظ طمع در رده های سنی مختلف وجود ندارد.

## بررسی رابطه بین ازدواج و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول۱۲:** بررسی رابطه بین ازدواج و طمع

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .150[a] | 1 | .699 | | |
| Continuity Correction[b] | .008 | 1 | .931 | | |
| Likelihood Ratio | .154 | 1 | .695 | | |
| Fisher's Exact Test | | | | 1.000 | .478 |
| Linear-by-Linear Association | .148 | 1 | .700 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول 11 برای Pearson Chi-Square که برابر است با ۰.۶۹۹ اختلاف معنا داری از لحاظ طمع با ازدواج وجود ندارد.

## بررسی رابطه بین تحصیلات و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول۱۲:** بررسی رابطه بین تحصیلات و طمع

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 4.745[a] | 3 | .191 |
| Likelihood Ratio | 7.199 | 3 | .066 |
| Linear-by-Linear Association | .151 | 1 | .697 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول 12برای Pearson Chi-Square که برابر است با ۰.۱۹۱ اختلاف معنا داری از لحاظ طمع در رده های تحصیلی مختلف وجود دارد.

## بررسی رابطه بین سابقه کاری و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۳:** بررسی رابطه بین سابقه کاری و طمع

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 4.053[a] | 4 | .399 |
| Likelihood Ratio | 6.485 | 4 | .166 |
| Linear-by-Linear Association | 3.443 | 1 | .064 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول 13 برای Pearson Chi-Square که برابر است با ۰.۳۹۹ اختلاف معنا داری از لحاظ طمع با سابقه کاری وجود ندارد.

## بررسی رابطه بین واحد سازمانی و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۴:** بررسی رابطه بین واحدسازمانی و طمع

| **Chi-Square Tests** | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .986[a] | 1 | .321 | | |
| Continuity Correction[b] | .497 | 1 | .481 | | |
| Likelihood Ratio | .947 | 1 | .330 | | |
| Fisher's Exact Test | | | | .389 | .237 |
| Linear-by-Linear Association | .975 | 1 | .323 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول 14 برای Pearson Chi-Square که برابر است با ۰.۳۲۱ اختلاف معنا داری از لحاظ طمع در واحدهای سازمانی مختلف وجود ندارد.

## بررسی رابطه بین متغیرهای دموگرافی با عامل اطاعت

## بررسی رابطه بین جنسیت و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۵:** بررسی رابطه بین جنسیت و اطاعت

| **Chi-Square Tests** | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |

| | | | | | |
|---|---|---|---|---|---|
| Pearson Chi-Square | 2.532[a] | 1 | .112 | | |
| Continuity Correction[b] | 1.590 | 1 | .207 | | |
| Likelihood Ratio | 2.305 | 1 | .129 | | |
| Fisher's Exact Test | | | | .183 | .106 |
| Linear-by-Linear Association | 2.503 | 1 | .114 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۱۵ برای Pearson Chi-Square که برابر است با ۰.۱۱۲ اختلاف معنا داری از لحاظ اطاعت در بین مردان و زنان وجود دارد.

## بررسی رابطه بین سن و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۶:** بررسی رابطه بین سن و اطاعت

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 16.293[a] | 2 | .000 |
| Likelihood Ratio | 13.119 | 2 | .001 |
| Linear-by-Linear Association | 9.459 | 1 | .002 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۱۶ برای Pearson Chi-Square که برابر است با ۰.۰۰۱ اختلاف معنا داری از لحاظ اطاعت در رده های سنی مختلف وجود دارد.

## بررسی رابطه بین ازدواج و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۷:** بررسی رابطه بین ازدواج و اطاعت

| Chi-Square Tests |
|---|

| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
|---|---|---|---|---|---|
| Pearson Chi-Square | 7.792[a] | 1 | .005 | | |
| Continuity Correction[b] | 6.205 | 1 | .013 | | |
| Likelihood Ratio | 12.211 | 1 | .000 | | |
| Fisher's Exact Test | | | | .005 | .002 |
| Linear-by-Linear Association | 7.705 | 1 | .006 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۱۷ برای Pearson Chi-Square که برابر است با ۰.۰۰۵ اختلاف معنا داری از لحاظ اطاعت با ازدواج وجود دارد.

## بررسی رابطه بین تحصیلات و عامل اطاعت پذیری

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۸:** بررسی رابطه بین تحصیلات و اطاعت

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 7.868[a] | 3 | .049 |
| Likelihood Ratio | 7.166 | 3 | .067 |
| Linear-by-Linear Association | .634 | 1 | .426 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۱۸ برای Pearson Chi-Square که برابر است با ۰.۰۴۹ اختلاف معنا داری از لحاظ اطاعت در رده های تحصیلی مختلف وجود دارد.

## بررسی رابطه بین سابقه کاری و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۱۹:** بررسی رابطه بین سابقه کاری و اطاعت پذیری

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 2.515[a] | 4 | .642 |
| Likelihood Ratio | 3.149 | 4 | .533 |
| Linear-by-Linear Association | .027 | 1 | .870 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۱۹ برای Pearson Chi-Square که برابر است با ۰.۶۴۲ اختلاف معنا داری از لحاظ اطاعت با سابقه کاری وجود ندارد.

## بررسی رابطه بین واحد سازمانی و عامل اطاعت پذیری

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۰:** بررسی رابطه بین واحدسازمانی و اطاعت پذیری

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .026[a] | 1 | .873 | | |
| Continuity Correction[b] | .000 | 1 | 1.000 | | |
| Likelihood Ratio | .026 | 1 | .872 | | |
| Fisher's Exact Test | | | | 1.000 | .561 |
| Linear-by-Linear Association | .025 | 1 | .873 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۲۰برای Pearson Chi-Square که برابر است با ۰.۸۷۳ اختلاف معنا داری از لحاظ اطاعت در واحدهای سازمانی مختلف وجود ندارد.

## بررسی رابطه بین متغیرهای دموگرافی با عامل خیرخواهی

### بررسی رابطه بین جنسیت و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۱**: بررسی رابطه بین جنسیت و خیرخواهی

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .366[a] | 1 | .545 | | |
| Continuity Correction[b] | .113 | 1 | .737 | | |
| Likelihood Ratio | .368 | 1 | .544 | | |
| Fisher's Exact Test | | | | .599 | .370 |
| Linear-by-Linear Association | .362 | 1 | .547 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول 21 برای Pearson Chi-Square که برابر است با ۰.۵۴۵ اختلاف معنا داری از لحاظ خیرخواهی در بین مردان و زنان وجود ندارد.

### بررسی رابطه بین سن و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۲**: بررسی رابطه بین سن و خیرخواهی

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 6.405[a] | 2 | .041 |
| Likelihood Ratio | 6.484 | 2 | .039 |
| Linear-by-Linear Association | 1.933 | 1 | .164 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۲۲ برای Pearson Chi-Square که برابر است با ۰.۰۴۱ اختلاف معنا داری از لحاظ خیرخواهی در رده های سنی مختلف وجود دارد.

## بررسی رابطه بین ازدواج و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۳:** بررسی رابطه بین ازدواج و خیرخواهی

| Chi-Square Tests | | | | | |
|---|---|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
| Pearson Chi-Square | .063[a] | 1 | .802 | | |
| Continuity Correction[b] | .000 | 1 | .996 | | |
| Likelihood Ratio | .063 | 1 | .802 | | |
| Fisher's Exact Test | | | | 1.000 | .499 |
| Linear-by-Linear Association | .062 | 1 | .803 | | |
| N of Valid Cases[b] | 95 | | | | |

با توجه به مقدار به دست آمده از جدول ۲۳ برای Pearson Chi-Square که برابر است با ۰.۸۰۲ اختلاف معنا داری از لحاظ خیرخواهی با ازدواج وجود ندارد.

## بررسی رابطه بین تحصیلات و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۴:** بررسی رابطه بین تحصیلات و خیرخواهی

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 13.053[a] | 3 | .005 |
| Likelihood Ratio | 15.448 | 3 | .001 |
| Linear-by-Linear Association | .800 | 1 | .371 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۲۴ برای Pearson Chi-Square که برابر است با ۰.۰۰۵ اختلاف معنا داری از لحاظ خیرخواهی در رده های تحصیلی مختلف وجود دارد.

## بررسی رابطه بین سابقه کاری و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۵**: بررسی رابطه بین سابقه کاری و اطاعت

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 22.400[a] | 4 | .000 |
| Likelihood Ratio | 27.993 | 4 | .000 |
| Linear-by-Linear Association | 10.302 | 1 | .001 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۲۵ برای Pearson Chi-Square که برابر است با ۰.۰۰۱ اختلاف معنا داری از لحاظ خیرخواهی با سابقه کاری وجود دارد.

## بررسی رابطه بین واحد سازمانی و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از **۰.۱** است.

**جدول ۲۶**: بررسی رابطه بین واحدسازمانی و خیرخواهی

| Chi-Square Tests | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 1.888[a] | 2 | .389 |
| Likelihood Ratio | 2.278 | 2 | .320 |
| Linear-by-Linear Association | .435 | 1 | .510 |
| N of Valid Cases | 95 | | |

با توجه به مقدار به دست آمده از جدول ۲۶ برای Pearson Chi-Square که برابر است با ۰.۳۸۹ اختلاف معنا داری از لحاظ خیرخواهی در واحدهای سازمانی مختلف وجود ندارد.

## بحث و نتیجه‌گیری:

کلید دفاع در برابر حملات مهندسی اجتماعی در آن است که بدانیم آسیب پذیری‌ها و تهدیدها چه چیزهایی هستند و سپس در برابر این ریسک‌ها به مقابله بپردازیم. دفاع باید چندین لایه حفاظتی داشته باشد، بطوریکه اگر هکری توانست از سطحی نفوذ کند، در لایه‌های دیگر به دام بیفتد از آنجایی که ثابت شده‌است حملات مهندسی اجتماعی بسیار موفقیت آمیز بوده‌اند، بنابراین داشتن راهبرد چند لایه‌ای در این زمینه حیاتی خواهد بود، در برخی نقاط نیز راهبرد بیشتر از دفاع باید در نظرگرفته شود. زیرا حمله کننده با حملات بسیار خود بالاخره سعی می‌کند تا نقاط ضعیف را شناسایی کند و بهمین دلیل است که سازمان باید در برابر حملات دفاعی محکم داشته باشد یا حداقل تشخیص دهد که مورد حمله قرار گرفته‌است.


**شکل ۲:** الگوی پیشنهادی صیانت از کارکنان در برابر حملات مهندسی اجتماعی

### سطح ۱: تدوین خط و مشی های امنیتی مناسب:

هیچ سنگری بدون پایه‌های مستحکم و پایدار، دوام پیدا نخواهد کرد. اساس امنیت اطلاعات سیاست‌های آن است. سیاست‌های امنیتی، استانداردها و سطوح امنیتی شبکه را تعیین می‌کند. این بنیان زمانی حیاتی تر می‌گردد که سیاست‌های امنیتی بخواهد شبکه را از حملات مهندسی اجتماعی مصون بدارد. سیاست‌های مهندسی اجتماعی به کارمندان چگونگی پاسخ دهی به درخواست‌های مشکوک را می‌آموزد. سیاست‌های تثبیت شده، کمک می‌کند که کاربر نهایی حس کند، چاره‌ای جز مقاومت در برابر خواست هکران ندارد. کاربران نهایی نیز نباید نقش تصمیم گیرنده برای در اختیار گذاری اطلاعات، را داشته باشند. نکته جالب دیگری که در تئوری تحریک و تشویق وجود دارد، فرا شناخت می‌باشد. فراشناخت، توانمندی است که با آن از اندیشه و فرایند فکر کردن دیگران می‌توان آگاه شد. با توجه به مطالعات انجام شده درباره فراشناخت در تئوری تحریک، محققان به این نتیجه رسیده‌اند که یکی از راه‌های مقاوم‌سازی در برابر حملات، توسعه اعتماد به فکر، در کارمندان می‌باشد. نتایج این بخش با یافته های اشمیت(۲۰۱۶) در مورد اولویت تدوین سیاست ها و خط و مشی های امنیتی در برابر حملات مهندسی اجتماعی تطابق دارد. سیاست‌های امنیتی واضح و روشن، خطر تأثیر گذاری متجاوزان بر روی کارمندان را کاهش می‌دهد. سیاست امنیتی باید حوزه‌های خاصی را مد نظر قرار دهند تا بتوانند بعنوان پایه‌های مقاومت مهندسی اجتماعی به حساب آیند. کنترل دسترسی به اطلاعات، راه‌اندازی حساب‌ها، تأیید دسترسی و تغییر در کلمات عبور باید در نظر گرفته شود.

### سطح ۲: آموزش همگانی کارکنان

پس از تثبیت سیاست‌های امنیتی، تمام کارمندان باید برای آگاهی‌های امنیتی آموزش ببینند. سیاست امنیتی همانگونه که انگیزه‌های امنیتی را بوجود می‌آورند، چارچوب آموزش را نیز تعیین خواهند کرد. سیاست‌هایی که با تفکر تدوین شده باشند و به کارمندان آموزش داده شده باشند در پاسخگویی کارمندان به درخواست‌های مختلف، متجاوزان تمایز ایجاد خواهند کرد. آگاهی‌های امنیتی خیلی پیچیده‌تر از آنست که به کارمندان بگوییم که پسوردشان را به کسی ندهند. بطوریکه هکر معروف کوین میتنیک گفته‌است: «من هرگز از کسی نخواسته‌ام که پسوردش را به من بدهد.» نکته در اینجاست که هدف هکر پیچیده‌تر بوده و سعی در ایجاد اطمینان در فرد و سوء استفاده از آن می‌باشد. کارمندان باید آگاه باشند که مهاجم مهندسی اجتماعی به چه اطلاعات اولیه‌ای نیاز خواهد داشت و از چه گفتگوهایی در راه رسیدن به آن استفاده خواهد کرد. همچنین کارمندان باید بدانند چگونه اطلاعات محرمانه را تشخیص دهند و مسئولیتشان را در قبال محافظت از آن بدانند.

آنها باید بدانند که چگونه در مقابل خواسته‌های غیرمجاز «نه» بگویند و چه زمانی برای گفتن این کلمه مناسب است! برنامه‌های آموزشی نیز باید از سیاست‌های امنیتی پیروی کند.

### سطح ۳: آموزش پرسنل کلیدی سازمان

نه تنها تمام کارمندان باید آگاهی‌های امنیتی را آموزش ببینند، بلکه در دفاع چند لایه، باید آموزش مقاومت برای پرسنل کلیدی نیز وجود داشته باشد. پرسنل کلیدی شامل کارکنان عملیاتی بخش های سایبری و مجازی، تحلیل گران سیستم های اطلاعاتی و به طور کلی هر یک از کارکنان که با فضای سایبری سر و کار دارند را شامل می‌شود یا بطورکلی هر کسی که کار یاری رسانی و رویارویی با دیگران را در سازمان ایفا می‌کند. آموزش مقاومت منجر می‌شود که کارمندان از متقاعد شدن و افشای اطلاعات مورد نیاز هکر، دوری جویند. روش‌های آموزش مقاومت شامل:

- واکسیناسیون: این روش منطبق با ایده واکسیناسیون بوده، بطوریکه ضعیف شده آن چیزی که هکرها از کارمندان می‌خواهند را، به کارمندان آموزش می‌دهیم. هکر نیز از روش‌های مشابه پیروی خواهد کرد؛ بنابراین واکسن از توسعه یک روش جلوگیری می‌کند.
- پیش آگاهی: قبل از آنکه اتفاقی رخ دهد در مورد آن اخطار داده و بصورت پیام بگوش همه می‌رسانیم، در اخطار نه تنها از امکان حمله مهاجم اجتماعی خبر می‌دهیم بلکه روش‌ها و چگونگی حمله را نیز بیان می‌کنیم.
- سنجش واقعیت: یکی از دلایل آموزش آگاهی امنیتی به این خاطر است که همگان نسبت به آسیب پذیریشان بطور غیر واقعی خوش بین هستند. این برداشت خیلی‌ها را از دیدن ریسک‌های به حق، دور می‌کند.

### سطح ۴: تثبیت و یادآوری

دفاع چند لایه نیاز به یادآوری‌های متمادی از اهمیت آگاهی دارد. تلنگری کوتاه مدت برای مقابله با نفوذگر، فقط در زمان کوتاهی مؤثر خواهد بود. یادآوری‌های متوالی و خلاقانه، برای هشیاری افراد از خطرهای موجود، مورد نیاز است.

### سطح ۵: مین گذاری برای آشکارسازی حملات

SELM ها، تله‌هایی در سیستم هستند که حمله‌ها را آشکار کرده و از وقوع آن جلوگیری می‌کنند. درست مثل میدان مین در صحنه نبرد. همانگونه که مین در صورت مقابله با متجاوز منفجر می‌شود، مهاجم را زمین گیر کرده و حمله را متوقف می‌سازد. SELM به قربانی هشدار می‌دهد که حمله‌ای در حال صورت گرفتن است و وضعیت امنیتی جدیدی را باید در پی گرفت.

### سطح ۶: سطح تهاجمی

آخرین سطح دفاعی، پاسخ دهی به رویدادها می‌باشد. بدین ترتیب شبکه دیگر اجازه نمی‌دهد که مهاجم اجتماعی بتواند با کارمندان بی‌توجه به امنیت در سازمان، صحبت کند؛ بنابراین نیاز است که فرایندهای پاسخ دهی کاملاً معین باشند تا کارمندان به محض آنکه به فرد یا رفتاری مشکوک شدند، بتوانند آن را به گوش همگان برسانند. برای اثر بخشی بیشتر، باید فرد یا بخشی را برای رهگیری دقیق این رویدادها داشته باشیم،

## تشکر و قدردانی

## فهرست منابع:


- دانایی فر، حسن و دیگران(۱۳۹۲). روش شناسی پژوهش کیفی در مدیریت. تهران. انتشارات صفار.
- قوچانی، محمد مهدی، موسوی، امیر، حسین پور، داود(۱۳۹۴). حفاظت و امنیت اطلاعات با ارائه الگوی مفهومی مهندسی اجتماعی. فصلنامه پژوهش های حفاظتی- امنیتی . دانشگاه جامع امام حسین (ع) سال سوم. شماره ۱۴. صص.۸۴.
- Allen, M. (June2006). The use of "Social Engineering" as a means of violating compute systems. http://www.sans.org/rr/paper.php?id=529.
- BilgeKarabacak, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security*, 413-419.
- Francois Mouton, M. M. (2018). Social Engineering Attack Model. *Defence Peace Safety & Security, Council for Industrial and Scientific Research, South Africa: 9.*
- Fan,Wenjun, Lwakatare, Kevin. Rong, Rong. (2017) Social Engineering: I-E based model of Human Weakness for Attack and Defense Investigations. Computer Network and Information Security. Vol 5.no 12.
- Gartner. (2002). There Are No Secrets: Social Engineering and Privacy. *Social Engineering:Exposing the Danger Within.*
- Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* the United States of America: Wiley Publishing, Inc.
- Hanan Sandouka, D. C. (2009). Social Engineering Detection using Neural Networks. *International Conference on CyberWorlds, UK: 6.*
- Labs, K. (2015). *http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf.*

- Labs, M. (2015). *http://www.mcafee.com/us/resources/misc/infographic-phishing-quiz.pdf.*
- Lichtenstein, M. (2015). Social Engineering Mitigating Human Risk in Mitigating Human Risk in. *VASCO Data Security*.
- Krombholz, Kathrina, Hobel, Heidelinde. Huber, Markuse.(2015). Advanced social engineering attacks. Journal of information Security and Applications, Vol 22.no 3.
- M. Junger, L. M.-J. ( January 2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, Volume 66,* Pages 75-87.
- MITNICK, K. D. (2004). *THE ART OF DECEPTION Controlling the Human Element of Security.*
- Ram Bhakta, I. G. (2015). Semantic Analysis of Dialogs to Detect Social Engineering Attacks. *International Conference on Semantic Computing,USA: 4.*
- Ravne, M. H. (2005). Fighting Social Engineering. *URL:www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-۲۸۱.pdf.*