Scientific Journal of Passive Defence
Vol. 15, No. 1, Spring 2024, Serial No. 57
ISSN: 2980-8030 , E-ISSN: 2008-6849

Defensive Tactics to Deal with Psychological Manipulation in the Field of Information Security

H. Hakim *, R. Esfehani

*Associate Professor, Allameh Tabataba'i University, Tehran, Iran

(Received: 14/06/2023, Revised: 24/12/2023, Accepted: 28/01/2024, Published: 04/05/2024)
DOR:20.1001.1.20086849.1403.15.1.2.9

ABSTRACT

Social engineering, which is referred to as the psychological manipulation of people in the field of information and cyber security, is a concept formed based on the exploitation of human vulnerabilities and thus creates a special type of attack which is formed on the basis of human characteristics and existing damages. The concept has become more useful and important due to the development of information and communications technology. Moreover, social engineering attacks are low-cost, highly effective, and, in their simplicity, they have certain elegance and complexities due to their human-centered nature. All these facts have caused security and military to have the same characteristics against these attacks and become more important. Hence, this paper addresses the concept and its different aspects and then, recommends military solutions for it intending to find proper tactics to provide a defense against social engineering attacks.

Keywords: Training, Defense, Attack, Social Engineering, Human

*Corresponding Author Email: hhakim@atu.ac.ir

نشریه علمی پدافند غیرعامل

سال پانزدهم، شماره ۱، بهار ۱۴۰۳، (پیاپی ۵۷): صص ۲۷-۱۳

علمی – پژوهشی

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

راهکنش‌های پدافندی جهت مقابله با فریب روانشناختی در حوزه امنیت اطلاعات

حمید حکیم[1*]، رضا اصفهانی[2]

DOR: 20.1001.1.20086849.1403.15.1.2.9

تاریخ دریافت: ۱۴۰۲/۰۳/۲۴ تاریخ پذیرش: ۱۴۰۲/۱۱/۳۰

تاریخ بازنگری: ۱۴۰۲/۱۰/۰۳ تاریخ انتشار: ۱۴۰۳/۰۲/۱۵

چکیده

مهندسی اجتماعی که در حوزه امنیت اطلاعات و سایبر از آن به عنوان فریب روانشناختی افراد یاد می‌شود، مفهومی است که بر پایه بهره‌برداری از آسیب‌پذیری‌های انسانی شکل گرفته و بر همین اساس نوع خاصی از حملات را رقم می‌زند که با نظر به ویژگی‌های انسانی و آسیب‌های موجود بر این مبنا شکل می‌گیرند. این مفهوم با گسترش فناوری اطلاعات و ارتباطات، کاربرد و اهمیت بیشتری یافته است؛ به علاوه حملات مهندسی اجتماعی، حملاتی با هزینه کم و اثربخشی بالا بوده و با توجه به ویژگی انسان محور بودن آنها، در عین سادگی از ظرافت و پیچیدگی‌های خاصی نیز برخوردار می‌باشند. همه این موارد موجب شده که امنیت و پدافند در برابر این حملات نیز چنین ویژگی‌هایی داشته و اهمیتی مضاعف بیابد. لذا نظر به این مهم، این مقاله با هدف یافتن راهکنش‌های مناسب جهت پدافند در برابر حملات مهندسی اجتماعی، ابتدا به این مفهوم و ابعاد مختلف آن پرداخته و سپس در مقام ارائه راهکارهای پدافندی برای آن برآمده است. در این پژوهش با روش دلفی و استفاده از نظر خبرگان جهت تعیین اولویت عوامل موثر در پدافند حملات مهندسی اجتماعی، آموزش به عنوان مهمترین عامل در این مهم شناخته شده و در حوزه آموزش نیز شبیه سازی و تست عملیاتی و تداوم آموزش به عنوان مهم‌ترین و تأثیرگذارترین ارکان آن تعیین شده‌اند.

کلیدواژه‌ها: آموزش، پدافند، حمله، مهندسی اجتماعی، انسان

[1] استادیار دانشگاه علامه طباطبایی، تهران، ایران (hhakim@atu.ac.ir)- نویسنده مسئول

[2] استادیار دانشگاه جامع امام حسین(ع)، تهران، ایران

ناشر: دانشگاه جامع امام حسین (ع)

۱- مقدمه

هر پدیده‌ای را می‌توان با توجه به پدیده‌های گذشته مورد نقد و بررسی قرار داد. بسیاری از مسائل که بشر امروزه با آنها مواجه است، در گذشته با اَشکال و روش‌های دیگری وجود داشته‌اند که سیر تکاملی آنها باعث شده است که به شکل فعلی ظاهر شوند. قطعاً شرایط محیطی و اقتضائات زمانی در این دگردیسی نقش مهمی ایفا می‌کنند. مهندسی اجتماعی نیز یکی از همین پدیده‌هاست. اگر بخواهند سوابق را بررسی کنند درمی‌یابند که مهندسی اجتماعی سیر تکامل یافته هکرهاست. با ظهور کامپیوتر در دروان جدید و فراگیر شدن آن از دهه ۷۰ میلادی مانند هر پدیده دیگری انحراف در کاربرد این ماشین نیز با ظهور هکرها بوجود آمد. البته هکرها همواره در جهت منفی حرکت نمی‌کردند و در برخی مواقع بعنوان همراه و عضوی رسمی از شرکت‌ها و سازمان‌ها در راه ایجاد امنیت سایبری تلاش می‌کردند. در گذشته هکرها با استفاده از حملات فناوری محور، آسیب‌های جبران ناپذیری به افراد و سازمان‌ها وارد می‌کردند و یا اطلاعات مورد نیاز خود را بدست می‌آوردند. اما با افزایش آگاهی و پیشرفت سامانه‌های امنیتی و کاربرد مداوم آن توسط کاربران، مهندسی اجتماعی را بعنوان روشی جایگزین انتخاب نمودند تا هم از فناوری و هم از افراد برای دست یابی به اهداف خود استفاده نمایند [۱]. انسان‌ها ضعیف‌ترین حلقه زنجیره امنیت سایبری هستند و این اساس حمله «مهندسی اجتماعی» است. مهندسین اجتماعی در واقع ادامه دهنده راه هکرها هستند. از مهندسان اجتماعی بعنوان هکر مردمی[1] هم نام می‌برند [۲]. هر چقدر هکر زمان بیشتری برای بدست آوردن اطلاعات صرف کند، احتمال دستگیری‌اش در پایان بیشتر می‌شود، هم چنین فناوری‌های نوین ابداع شده‌اند که کار را برای هکرها سخت کرده‌اند. به همین دلیل است که بسیاری از آنها به مهندسی اجتماعی روی آورده‌اند چون در بسیاری از موارد سوء استفاده از انسان بسیار راحت‌تر از سامانه است. مهندسان اجتماعی با تجربه طوری فعالیت می‌کنند که کاربران متوجه نمی‌شوند چه اتفاقی افتاده است و به کارهای معمول خود ادامه می‌دهند. البته در این میان اختلاف مهمی بین آنها وجود دارد. هکرها خود به دنبال سوء استفاده از امنیت سامانه‌ها و بهره‌برداری‌های غیر مجاز بودند [۳]، حال آنکه مهندسین اجتماعی شرایطی فراهم می‌نمایند که در آن، قربانیان خود بصورت آگاهانه و یا ناآگاهانه اطلاعات را در اختیار آنها قرار دهند. این نکات مهم بیش از هر چیزی، پیچیدگی و تأثیر شگرف مهندسی اجتماعی را نشان داده و اهمیت دفاع و مقابله در برابر آن را مشخص می‌سازد. بر همین اساس و با نظر به نبود اثر پژوهشی در حوزه پدافند غیرعامل حملات مهندسی اجتماعی، در این مقاله به این مهم پرداخته شده و هدف یافتن و ارائه روش‌های پدافند مهندسی اجتماعی می‌باشد. این پژوهش، ابتدا به روش‌های متداول حملات مهندسی اجتماعی پرداخته و پس از آن، از منظر سطوح مختلف و به شکلی جامع، پدافند و دفاع در برابر این حملات را مورد واکاوی قرار داده و در نهایت بر مبنای روش دلفی و با استفاده از نظر خبرگان به تعیین موثرترین عوامل و راهکنش‌ها در پدافند حملات مهندسی اجتماعی می‌پردازد.

۱-۱- تعریف مهندسی اجتماعی

در مقام تعریف پایه‌ای، باید بیان داشت مهندسی اجتماعی حوزه‌ای در علوم اجتماعی است که در جهت تحت تأثیر قرار دادن نگرش‌ها و رفتار اجتماعی در مقیاس بزرگ توسط دولت‌ها، رسانه‌ها و یا گروه‌های خصوصی برای ایجاد ویژگی‌های خاص در یک جامعه هدف تلاش می‌کند. اما کاربست این مفهوم امروزه با تغییرات و گستردگی در مقیاس و سطح تأثیر و البته با حفظ دال محوری خود مبنی بر توجه به ویژگی‌های روانشناختی انسان در حوزه امنیت اطلاعات و سایبر مطرح می‌باشد. مهندسی اجتماعی هنر بهره برداری از رفتارهای آسیب پذیر انسان‌ها برای ایجاد شکاف امنیتی بدون هیچ ظن و گمانی از سوی قربانی است. مهندسی اجتماعی انسان‌ها را با روش‌های مختلف فریب داده و با متقاعد کردنشان از آنها برای دستیابی به اطلاعات سوء استفاده می‌کند. مهندسی اجتماعی برای تغییر رفتار افراد استفاده می‌شود [۴]. یک مهندس اجتماعی باید نگرش‌ها و باورهای مخاطبان خود را به خوبی ارزیابی کند و راهکنش‌های خود را برای اثرگذاری بیشتر با آنها منطبق نماید [۵]. برای تعریف مهندسی اجتماعی می‌توان از منابع مختلفی بهره‌گیری کرد. با توجه به اینکه نکات مشترک زیادی در منابع مختلف وجود دارد، می‌توان چند نمونه از آنها را ذکر نمود:

- مهندسی اجتماعی هنر بهره برداری از ویژگی‌های انسانی برای دست یابی به اطلاعات است [۶].
- مهندسی اجتماعی هنر یا بهتر بگوییم دانش به حرکت درآوردن انسان‌ها برای فعالیت در برخی از جنبه‌های زندگی‌شان است. این فعالیت‌ها ممکن است جزء علایق فرد باشد یا نباشد [۷].

[1] People Hacker

- تلاش موفق یا ناموفق برای اثرگذاری بر فرد به منظور آشکار کردن اطلاعات یا انجام رفتاری که منجر به دسترسی غیر مجاز یا افشاء غیر مجاز اطلاعات یک سامانه، شبکه یا داده‌ها شود [۸].
- مجموعه یکپارچه‌ای از ابزارها که طراحی شده‌اند برای حملات پیشرفته به عناصر انسانی [۶].

مهندسی اجتماعی به شدت بر شش اصل تأثیرگذاری (متقاعد سازی) که توسط رابرت سیالدینی ایجاد شده است، متکی است. نظریه نفوذ(تأثیر) سیالدینی [۹] مبتنی بر شش اصل کلیدی است: مقابله یا عمل متقابل، تعهد و ثبات، تایید و اثبات اجتماعی (اجماع)، اعتبار و صلاحیت، آشنایی/دوست داشتن، کمیابی.

آنچه مهندسی اجتماعی را به طور خاصی خطرناک می‌سازد این است که به جای آسیب پذیری در نرم افزار و سیستم عامل، متکی به خطای انسانی است. در واقع اشتباهات انجام شده توسط کاربران قانونی بسیار کمتر قابل پیش بینی هستند و شناسایی و خنثی کردن آنها دشوارتر از یک نفوذ مبتنی بر بدافزار است.

در زمینه امنیت اطلاعات، مهندسی اجتماعی دستکاری روانی (فریب روانشناختی) افراد برای انجام اقدامات یا افشای اطلاعات محرمانه است. یک نوع ترفند اطمینان برای جمع‌آوری اطلاعات، کلاهبرداری یا دسترسی به سیستم، که با یک "جرم" سنتی تفاوت دارد زیرا اغلب یکی از چندین مرحله در یک طرح کلاهبرداری پیچیده‌تر است [۱۰]. همچنین این گونه تعریف شده است: «هر عملی که شخص را تحت تأثیر قرار دهد تا اقدامی را انجام دهد که ممکن است به نفع او باشد یا نباشد [۱۱].

۱-۱-۱- چرخه حیات مهندسی اجتماعی

برای مهندسی اجتماعی چرخه حیاتی به شکل زیر در نظر گرفته می‌شود. بدیهی است که شناخت این چرخه نقش مهمی در پدافند آن می‌تواند داشته باشد.

جمع آوری اطلاعات: جمع آوری اطلاعات اولین و مهم‌ترین مرحله چرخه حیات است و نیاز به صبر زیاد و شناخت عادات دقیق قربانی دارد. این مرحله که اطلاعات مربوط به علایق قربانی و اطلاعات شخصی را جمع آوری می‌نماید، میزان موفقیت حمله کلی را تعیین می کند.

تعامل با قربانی: پس از جمع‌آوری اطلاعات مورد نیاز، مهاجم بدون اینکه قربانی چیز نامناسبی پیدا کند، به آرامی با قربانی گفتگو می‌کند.

حمله: این مرحله عموماً پس از یک دوره طولانی درگیر شدن با هدف اتفاق می‌افتد و در این مرحله اطلاعات از هدف با استفاده از مهندسی اجتماعی بازیابی می‌شود. در این مرحله، مهاجم نتایج را از هدف دریافت می‌کند.

تعامل بسته: این آخرین مرحله است که شامل قطع آهسته ارتباط توسط مهاجم بدون ایجاد هرگونه سوء ظنی در قربانی است. به این ترتیب، انگیزه برآورده می‌شود و همچنین قربانی به ندرت متوجه می‌شود که حمله حتی اتفاق افتاده است [۱۲].

۲- روش‌ها و حملات مهندسی اجتماعی

همه روش‌های مهندسی اجتماعی مبتنی بر ویژگی‌های خاص تصمیم‌گیری انسانی هستند که به عنوان سوگیری‌های شناختی شناخته می‌شوند [۱۳]. این سوگیری‌ها، که گاهی اوقات "اشکالات در سخت افزار انسانی" نامیده می‌شوند، در ترکیب‌های مختلف برای ایجاد روش‌های حمله مورد سوء استفاده قرار می‌گیرند. حملات مورد استفاده در مهندسی اجتماعی را می‌توان برای سرقت اطلاعات محرمانه کارکنان مورد استفاده قرار داد. رایج‌ترین نوع از حملات مهندسی اجتماعی مجرمانی هستند که خود را به عناوین مختلفی چون متخصص و یا نقش‌هایی که حالت حامی، دلسوز و کمک کننده دارند نشان داده تا اسرار و اطلاعات را به سرقت ببرند.

اساس حملات مهندسی اجتماعی «سوء استفاده از احساسات» است. بسیاری از مهندسان اجتماعی روی حس ترس، کنجکاوی، طمع و دلسوزی قربانیان خود تمرکز می کنند، چون این احساسات بین انسان های سراسر دنیا مشترک است و واکنش ما به آن‌ها تقریباً مشابه است.

حملات مهندسی اجتماعی اشکال مختلفی دارد و می‌توانند در هر جایی که با تعاملات انسانی دخیل است انجام شود. همانطور که در چرخه حیات مهندسی اجتماعی بیان شد، اولین مرحله برای هر گونه تهاجمی ابتدا جمع آوری اطلاعات درباره حریف است. مهندسان اجتماعی هم مانند هکرهای قدیمی بیشتر زمان خود را به ایجاد آمادگی بیشتر از طریق جمع آوری اطلاعات می‌پردازند [۱]. پس از جمع آوری اطلاعات لازم، مهندسان اجتماعی به دنبال یافتن روشی مناسب برای حمله هستند. یک مهندس اجتماعی می‌تواند از ابزارهای مختلف فناوری استفاده کند تا به اهداف خود دست یابد. روش‌هایی مانند فیشینگ، حمله چاله آبیاری، طعمه گذاری، چیزی بجای دیگری، ترس افزار، کلاهبرداری نیجریه‌ای از جمله روش‌های متداول در مهندسی اجتماعی هستند که در ادامه برخی از مهم‌ترین آنها بیان می‌شود.

۲-۱- فیشینگ[1]

فیشینگ روشی است برای به دست آوردن اطلاعات خصوصی با کلاهبرداری. به طور معمول، فیشر ایمیلی را ارسال می‌کند که به نظر می‌رسد از یک تجارتخانه قانونی - یک بانک یا شرکت کارت اعتباری - درخواست "تأیید" اطلاعات و هشدار درباره عواقب ناگوار در صورت عدم ارائه آن را می‌دهد. ایمیل معمولاً حاوی پیوندی به یک صفحه وب تقلبی است که مشروع به نظر می‌رسد - با آرم و محتوای شرکت - و دارای فرمی است که همه چیز را از آدرس خانه گرفته تا پین کارت اِی تی اِم[2] یا شماره کارت اعتباری درخواست می‌کند. با تقلید از کدهای اچ تی اِم اِل[3] و لوگوهای یک سازمان قانونی، نسبتاً ساده است که یک وب سایت جعلی معتبر به نظر برسد [۱۴].

فیشینگ صوتی[4]، فیشینگ پیامکی[5] [۱۵]، و فیشینگ نیزه‌ای[6] [۱۶] از روش‌های دیگری هستند که در زمره فیشینگ قرار می‌گیرند.

۲-۲- نرم افزار تبلیغاتی[7]

در این روش نیز بر پایه احساسات انسان، بدافزار مرورگر شما را مجبور می‌کند به سمت تبلیغات وب هدایت شوید و این نیز اغلب دانلود بیشتر نرم افزارهای مخرب را به همراه دارد. این نرم افزارهای تبلیغاتی مزاحم اغلب به برنامه‌های "رایگان" وسوسه انگیز مانند بازی‌ها یا افزونه‌های مرورگر منتقل می‌شوند.

۲-۳- بهانه سازی[8]

بهانه سازی، عمل ایجاد و استفاده از یک سناریوی ابداع شده (بهانه) برای درگیر شدن با قربانی هدفمند است، به نحوی که احتمال افشای اطلاعات یا انجام اقداماتی را که در شرایط عادی غیرممکن است را افزایش دهد [۱۷]. یک دروغ مفصل، اغلب شامل تحقیقات یا تنظیمات قبلی و استفاده از این اطلاعات برای جعل هویت (به عنوان مثال، تاریخ تولد، شماره ملی، آخرین مبلغ صورت حساب) برای ایجاد مشروعیت در ذهن هدف است [۱۸]. به عنوان پس‌زمینه، بهانه‌سازی را می‌توان به‌عنوان اولین تکامل مهندسی اجتماعی تفسیر کرد و همچنان به عنوان روشی در مهندسی اجتماعی که فناوری‌های امروزی را در بر می‌گیرد، توسعه می‌یابد. نمونه‌های فعلی و گذشته بهانه سازی این پیشرفت را نشان می‌دهد.

این روش می‌تواند برای فریب دادن یک کسب و کار در افشای اطلاعات مشتری و همچنین توسط مهاجم برای به دست آوردن سوابق تلفنی، سوابق خدماتی، سوابق بانکی و سایر اطلاعات به طور مستقیم از نمایندگان خدمات شرکت استفاده شود [۱۹]. سپس می‌توان از این اطلاعات برای ایجاد مشروعیت بیشتر تحت سؤالات سخت تر با یک مدیر استفاده کرد، به عنوان مثال، برای ایجاد تغییرات حساب، دریافت مانده های خاص و غیره.

بهانه سازی همچنین می تواند برای جعل هویت همکاران، پلیس، بانک، مقامات مالیاتی، روحانیون، بازرسان بیمه یا هر فرد دیگری که می توانست در ذهن قربانی مورد نظر قدرت یا حق دانستن داشته باشد، استفاده شود. مهاجم باید به سادگی پاسخ سوالاتی را که ممکن است قربانی بپرسد آماده کند. در برخی موارد، تنها چیزی که لازم است صدایی معتبر، لحنی جدی و توانایی تفکر روی پای خود برای ایجاد یک سناریوی بهانه ای است.

۲-۴- حفره آب[9]

حفره آب یک روش مهندسی اجتماعی هدفمند است که از اعتماد کاربران به وب سایت‌هایی که مرتباً بازدید می‌کنند، سرمایه گذاری می‌کند. قربانی برای انجام کارهایی که در موقعیت‌های متفاوت انجام نمی‌دهد احساس امنیت می‌کند. برای مثال، یک فرد محتاط ممکن است عمداً از کلیک کردن روی پیوند در یک ایمیل ناخواسته اجتناب کند، اما همان شخص در دنبال کردن پیوندی در وب سایتی که اغلب از آن بازدید می کند تردیدی ندارد. بنابراین، مهاجم یک تله برای طعمه بی احتیاط در یک چاله آبیاری مطلوب آماده می‌کند. این روش با موفقیت برای دستیابی به برخی از سیستم‌های (ظاهراً) بسیار امن استفاده شده است [۲۰].

مهاجم ممکن است با شناسایی یک گروه یا افراد برای هدف قرار دادن اقدام کند. این آماده سازی شامل جمع آوری اطلاعات در مورد وب سایت‌هایی است که اهداف اغلب از سیستم ایمن بازدید می‌کنند. جمع‌آوری اطلاعات تأیید می‌کند که هدف‌ها از وب‌سایت‌ها بازدید می‌کنند و سیستم اجازه چنین بازدیدهایی را می دهد. سپس مهاجم این وب سایت‌ها را از نظر آسیب پذیری

[1] Phishing
[2] ATM
[3] HTML
[4] Vishing
[5] SMS-Phishing
[6] Spear phishing
[7] ADware
[8] Pretexting
[9] Water Hole

آزمایش می‌کند تا کدی را تزریق کند که ممکن است سیستم بازدید کننده را با بدافزار آلوده کند. تله کد تزریق شده و بدافزار ممکن است برای گروه هدف خاص و سیستم‌های خاصی که استفاده می کنند تنظیم شوند. با گذشت زمان، یک یا چند عضو از گروه هدف آلوده می‌شوند و مهاجم می‌تواند به سیستم امن دسترسی پیدا کند.

۲-۵- طعمه گذاری[1]

طعمه گذاری مانند اسب تروا در دنیای واقعی است که از رسانه‌های فیزیکی استفاده می‌کند و بر کنجکاوی یا طمع قربانی تکیه می‌کند. این حملات از یک وعده دروغین برای تحریک طمع یا کنجکاوی قربانی استفاده می‌کنند. آنها کاربران را به دامی سوق می‌دهند که اطلاعات شخصی آنها را دزدیده یا سیستم‌های آنها را به بدافزار آلوده می‌کند. در این حمله، مهاجمان فلاپی دیسک‌های آلوده به بدافزار، سی‌دی رام‌ها یا درایوهای فلش USB را در مکان‌هایی که مردم آنها را پیدا می‌کنند (حمام، آسانسور، پیاده‌رو، پارکینگ و غیره) رها می‌کنند، به آنها برچسب‌های قانونی و کنجکاوی برانگیز زده و منتظر قربانیان می‌نشینند.

به عنوان مثال، یک مهاجم ممکن است فلش یا دیسکی با نشان‌واره شرکت ایجاد کند که از وب‌سایت هدف در دسترس است، و روی آن برچسب "اجرای حقوق و دستمزد" بگذارد. سپس مهاجم دیسک را در کف آسانسور یا جایی در لابی شرکت هدف رها می‌کند. ممکن است یک کارمند ناآگاه آن را پیدا کند و برای ارضای کنجکاوی خود دیسک را در رایانه قرار دهد، یا یک مراجعه کننده خوب ممکن است آن را پیدا کند و به شرکت برگرداند. در هر صورت، فقط قرار دادن دیسک در رایانه، بدافزار را نصب می‌کند و به مهاجمان امکان دسترسی به رایانه شخصی قربانی و شاید شبکه رایانه داخلی شرکت هدف را می‌دهد. هر رسانه قابل جابجایی که در مکان‌های فرصت طلبانه یا آشکار باقی مانده است می‌تواند با نرم افزاری مخرب همراه باشد. این ابزار ممکن است یک CD، DVD، یا درایو فلشUSB، و یا رسانه‌ای دیگر باشد. افراد کنجکاو آن را می‌گیرند و به رایانه وصل می‌کنند و میزبان و هر شبکه متصل را آلوده می‌کنند. هکرها ممکن است به آنها برچسب‌های فریبنده‌ای مانند "حقوق کارکنان" یا "محرمانه" بزنند [۲۱].

در یک مطالعه انجام شده در سال ۲۰۱۶ از محققان دانشگاه ایلینویز، ۲۹۷ درایو USB در محوطه دانشگاه ایلینویز انداخته شد. درایوها حاوی فایل‌هایی بودند که به صفحات وب متعلق به محققان آن دانشگاه پیوند داشتند. از این تعداد ۲۹۰ (۹۸٪) از آنها برداشته شده و به رایانه ها متصل شدند. در آزمایشات مشابه دیگر نیز، تقریبا چنین نتایجی بدست آمده است [۲۲].

۲-۶- ترس افزار (القای ترس)[2]

ترس افزار شامل بمباران قربانیان با هشدارهای دروغین و تهدیدات ساختگی است. در واقع کاربران را فریب می‌دهند که سیستم‌شان به بدافزار آلوده است، و باعث می‌شود نرم افزاری نصب کنند که هیچ منفعتی (به جز برای مجرم) ندارد یا خود یک بدافزار است. از ترس افزار به عنوان نرم افزار فریب، نرم افزار اسکنر سرکش و کلاهبرداری نیز یاد می‌شود.

یک مثال متداول، بنرهای پنجره‌ای با ظاهر قانونی است که هنگام مرور وب در مرورگر شما ظاهر می‌شوند و متن‌هایی از جمله "کامپیوتر شما ممکن است به برنامه های جاسوسی مضر آلوده شود" را نشان می‌دهد. این برنامه یا نصب این ابزار (که اغلب به بدافزار آلوده است) را برای شما پیشنهاد می‌کند، یا شما را به یک سایت مخرب هدایت می‌کند که رایانه شما آلوده می‌شود. ترس افزار همچنین از طریق ایمیل اسپم توزیع می‌شود که هشدارهای جعلی را تایید می‌کند، و یا پیشنهاداتی برای کاربران برای خرید خدمات بی‌ارزش و مضر ارائه می‌دهد.

۲-۷- چیزی در برابر چیزی (جبران لطف)[3]

یک مهاجم با شماره‌های تصادفی یک شرکت تماس می‌گیرد و ادعا می‌کند که از پشتیبانی فنی تماس می‌گیرد. مهاجم مدعی است "کمک" می‌کند تا مشکل را حل کند و در این فرآیند، کاربر دستوراتی را تایپ می‌کند که به مهاجم اجازه دسترسی یا راه اندازی بدافزار را می‌دهد.

در یک نظرسنجی امنیت اطلاعات در سال ۲۰۰۳، ۹۱ درصد از کارکنان اداری در ازای دریافت یک خودکار ارزان، در پاسخ به سؤال نظرسنجی رمز عبور خود را به محققان دادند [۲۳]. بررسی‌های مشابه در سال‌های بعد نتایج مشابهی را با استفاده از

[1] Baiting

[2] Scareware

[3] Quid pro quo

شکلات‌ها و دیگر فریب‌های ارزان به‌دست آورد، اگرچه آنها هیچ تلاشی برای تأیید گذرواژه‌ها انجام ندادند [۲۴].

۲-۸- جعل هویت[1]

جعل هویت به معنای تظاهر به شخص دیگری با هدف دسترسی به یک سیستم یا ساختمان می‌باشد. جعل هویت یک شخص و معرفی کردن خود به جای دیگری مانند تعمیرکار، سرویس‌کار، تحویل دهنده غذا، پلیس و... برای ورود به یک ساختمان یا سازمان. این حمله می‌تواند از طریق تلفن یا ایمیل هم صورت بگیرد و الزامی نیست که حتما فیزیکی باشد.

۲-۹- زباله‌گردی[2]

یکی از راحت‌ترین روش‌های پیدا کردن اطلاعات یک سازمان است. در روش زباله‌گردی کافی است که زباله‌های سازمان را با خود به یک محیط خلوت ببرید و شروع به بررسی کاغذها و قطعات دور ریخته شده کنید تا بتوانید انواع اطلاعات سازمانی مانند نامه‌ها، پسورد، نام کاربری، آی‌پی[3]های سازمان، ایمیل و ... را پیدا کنید.

۳- پدافند در برابر حملات مهندسی اجتماعی

روش‌های متفاوتی برای پدافند و مقابله با این حملات وجود دارند. در واقع همانطور که راه‌های حمله مختلفند، راه‌های مقابله نیز متنوع هستند. قبل از بررسی راه‌های مقابله باید به دو جنبه اصلی مهندسی اجتماعی توجه شود:

۱) دیدگاه روانشناختی: به وضعیت احساسی و توانایی‌های شناختی فرد تکیه می‌کند. در واقع فرد را از نظر پتانسیل احساسی برای مغلوب شدن در برابر حملات مورد بررسی قرار می‌دهند. هر فردی با توجه به خصوصیات رفتاری و شخصیتی‌اش، پتانسیل خاصی برای تحت تأثیر قرار گرفتن دارد.

۲) دیدگاه علوم کامپیوتری: به حساسیت اطلاعات تأکید می‌کند. در واقع گفته می‌شود که فرد به چه میزان آمادگی اطلاعاتی برای مقابله با حملات را دارد. میزان دانش و آگاهی وی برای اینکه تحت تأثیر حملات قرار نگیرد به چه میزان است [۲۵].

برای ایجاد یک روش دفاعی مناسب باید به هر دو جنبه توجه داشت.

۳-۱- امنیت فضای سایبری[4]

دفاع در برابر مهندسی اجتماعی بعنوان بخشی از امنیت فضای سایبری مورد توجه قرار می‌گیرد. برخلاف باور عموم که بیشترین آسیب پذیری در سیستم‌های اطلاعاتی را در حوزه نرم افزار می‌دانند، این عامل انسانی است که بیشترین میزان ریسک را دارد [۶]. البته در مورد فناوری‌های نوین، دیگر انسان بعنوان ضعیف‌ترین رابط در حملات مهندسی اجتماعی نیست بلکه نحوه استفاده او از سیستم‌های جدید هم مطرح است [۲۶]. حملات مهندسی اجتماعی می‌تواند بعد از حمله اثرات مخربی بر روی قربانی داشته باشد مثلاً خودکشی. مسائل اخلاقی متعددی نیز در رابطه با حملات مهندسی اجتماعی وجود دارد. تبعات چنین حملاتی را می‌توان کاهش داد اگر فعالیت‌های درستی انجام گیرد [۲۵]. امنیت اطلاعات یک سازمان به فاکتورهای مختلف بستگی دارد. یکی از آنها آگاهی و هوشیاری کارکنان است. انسان‌ها اغلب ضعیف‌ترین حلقه در زنجیره امنیت هستند. به همین منظور ایجاد برنامه‌های کنترلی برای کارکنان بسیار مهم است. در حالیکه بسیاری از سازمان‌ها اهمیت و ارزش داشتن کنترل‌های داخلی را تشخیص داده‌اند، بسیاری از آنها نیز خطرات همراه با حملات مهندسی اجتماعی را نشناخته‌اند [۷]. برخی از مهم‌ترین توانایی‌های مطلوب در یک اکوسیستم سایبری به شرح ذیلند:

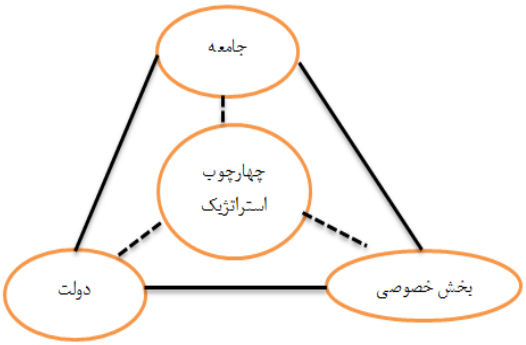
۱) تشخیص هویت خودکار، انتخاب و ارزیابی فعالیت‌های دفاعی[5]
۲) احراز هویت[6]
۳) آگاهی و آموزش عمومی[7]
۴) توانایی مبادله و استفاده از اطلاعات[8]
۵) یادگیری و تکامل ماشینی[9]
۶) پوشیدگی[10]
۷) مدیریت داده‌ها بر مبنای ریسک[11]
۸) امنیت درونی[12]
۹) فضاهای مناسب مورد اعتماد[13]

البته امنیت سایبری فقط بخشی از یک برنامه امنیتی جامع است. اگر در نظر دارند که فضای جامعه را ایمن کنند و افراد و

[1] Impersonation
[2] Dumpster Diving
[3] IP

[4] Cyber System Security
[5] Automated identification,selection & assessment of defensive actions
[6] Authentication
[7] General awareness & education
[8] interoperability
[9] Machine learning & evolution
[10] Privacy
[11] Risk-based data management
[12] Security built in
[13] Tailored trustworthy spaces

سازمان‌ها را از خطرات مهندسی اجتماعی مصون بدارند باید چهارچوب ذیل را رعایت نمود.



شکل (۱): چهارچوب کلی امنیتی [۶]

شکل (۱) نشان دهنده تعامل سه جزء اصلی امنیت می‌باشد. دولت، بخش خصوصی و جامعه هر کدام به دنبال این هستند که منفعت زیادی از یک استراتژی سایبری موفق و فکر شده ببرند. هر سه این بخش‌ها با یکدیگر همکاری می‌کنند تا بنیانی قدرتمند از نوآوری، تنوع اقتصادی، رشد بلند مدت و مزیت رقابتی پایدار ایجاد کنند. دولت می‌تواند از توانایی‌های سایبری برای توسعه خدمات عمومی و حفاظت از دارایی‌های مهم استفاده کند. بخش خصوصی تقریباً در هر صنعتی می‌تواند از توانایی‌های سایبری برای توسعه محصولات و خدمات، کاهش هزینه‌ها و دست یابی به مشتریان بیشتر استفاده نماید. در جهان سایبری یکپارچه، امنیت و ثبات مورد علاقه همه ذی نفعان است. همه این ذی نفعان جامعه را تشکیل می‌دهند. اگر محیط سایبری امن و مورد اعتماد همه شهروندان باشد. افراد جامعه علاقمندند که از توانایی‌های این محیط بطور کامل استفاده نمایند.

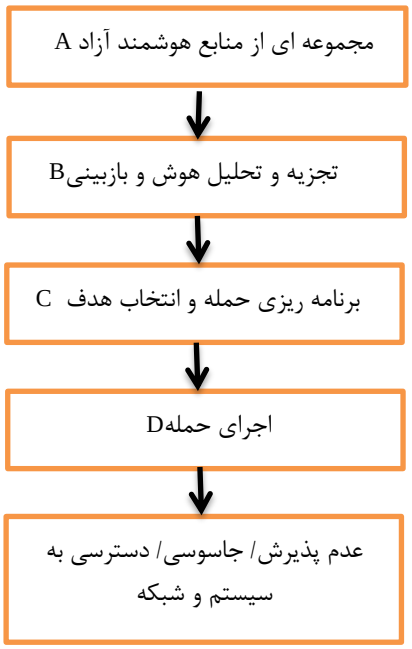
پنج ستون اصلی در یکپارچگی سایبری عبارتند از:

- سیاست و خط مشی
- مدیریت
- فناوری
- مردم
- عملکرد [۲۷]

مؤسسه مایکروترند[1] در سال ۲۰۱۲ برخی نکات ساده امنیت سایبری را بیان کرد:

۱) وب سایت‌هایی که مورد اعتماد هستند را ثبت[2] کنید
۲) هرگز لینک‌های مشکوک را باز نکنید
۳) هرگز از تهدیدات و پیام‌های تهدید نهراسید
۴) به دوستان و آشنایانتان اطلاع رسانی کنید. کمک کنید که آنها در دام جنایت‌های سایبری نیفتند.
۵) از رمز عبورهای متفاوت استفاده کنید. رمزهای عبور قدرتمند داشته باشید و بصورت مرتب آن را تغییر دهید [۲۸]. افرادی که از رمزهای یکسانی برای سیستم‌های مختلف استفاده می‌کنند، راحت‌تر آن را افشاء می‌کنند.

اگر بخواهند در مقابل حملات سایبری ایستادگی کنند باید آنها را بشناسند. شکل (۲) آناتومی این حملات را بطور کامل نشان می‌دهد.



A	B	C	D
شبکه‌های همتا (جفت)	ضروریات	آماده بهره برداری	**ایجاد ابهام**
موتورهای جست و جو	اطلاعات سیستم	اطلاعات هدف	**بی نشان کردن**
شبکه‌های اجتماعی	داده‌های زنجیره تأمین	سیستم‌های هدف	**زمان بندی کردن**
سایت‌های کاری	اعتبارنامه (اختیارات)	کارمندان هدف	
	کاربران ویژه		

شکل (۲): آناتومی حملات سایبری [۲۹]

[1] Micro trend
مؤسسه‌ای است که در زمینه خدمات امنیتی بخصوص در فضای سایبر فعالیت می‌کند .

[2] Bookmark

اگر نتوان امنیت اطلاعاتی سازمان را تأمین کرد با مشکلات زیادی مواجه می‌شوند که مهم‌ترین آنها عبارتند از:

- اطلاعات توسط دیگران جمع آوری می‌شود
- اعتبار و تصویر سازمان در جامعه مخدوش می‌شود
- سخت افزار، نرم افزار، داده‌ها و کارکنان سازمان ممکن است خسارت ببینند
- مشکل عدم دسترسی به موقع به داده‌های مهم افزایش می‌یابد
- خسارت مالی ایجاد می‌شود
- زمان از دست می‌رود
- حتی ممکن است زندگی افراد از دست برود [۳۰]

۳-۲- روش های دفاعی

با توجه به پیچیدگی مهندسی اجتماعی ارائه یک روش خاص و منحصر بفرد برای مقابله آن امکان پذیر نیست اما می‌توان روش‌های مختلفی را با پیچیدگی‌های متفاوت برای دفاع بیان نمود. در ادامه این بخش به معرفی و توضیح این روش‌ها پرداخته می‌شود.

۳-۲-۱- سؤالات ساده

می‌توان چند سؤال ساده را در نظر گرفت که کاربران در مواجهه

با درخواست‌های اطلاعاتی از خودشان بپرسند تا مطمئن شوند که از آنها سوء استفاده نشود:

۱) مشروعیت: آیا درخواست مشروع و معمول به نظر می‌رسد؟ برای مثال باید از شما چنین اطلاعاتی درخواست می‌شد یا نه؟

۲) اهمیت: ارزش اطلاعاتی که از شما خواسته شده چقدر است؟ چطور می‌توان از آنها سوء استفاده کرد؟

۳) منبع: آیا مطمئن هستید که منبع درخواست معتبر و واقعی باشد؟ آیا راهی برای بررسی این مسأله دارید؟

۴) زمان بندی: آیا باید هم اکنون پاسخ دهید؟ اگر هم چنان شک دارید زمان بگذارید تا مطمئن شوید و یا درخواست کمک کنید؟ [۳۱]

اینها سؤالات ساده‌ای هستند که می‌توانند فرد را در مواجهه با درخواست‌های غیر منطقی یاری نمایند. این سؤالات در واقع ناشی از یک فرآیند سه مرحله‌ای برای حفظ امنیت اموال و سیستم‌های ذهنی (فکری) در برابر دسترسی‌های ناخواسته هستند. (شکل ۳)

شکل (۳): فرآیند سه مرحله‌ای حفظ اموال و سیستم‌های ذهنی [۳۲]

۳-۲-۲- هکرهای اخلاق‌مدار[1]

هکرها در مواقعی بعنوان پرسنل مثبت در سازمان‌ها مورد استفاده قرار می‌گیرند. در واقع بسیاری از هکرها پس از شناسایی به عضویت سازمان‌ها در می‌آیند و با استفاده از شبیه‌سازی حملات در سازمان‌ها به آنها کمک می‌کنند تا سامانه‌های دفاعی خود را تقویت نمایند [۷]. بسیاری از هکرها بعد از اینکه شناسایی می‌شوند و دوران محکومیت خود را سپری می‌کنند بعنوان مشاور و یا مسئولین امنیتی سازمان‌ها استخدام می‌شوند چون این افراد آشنایی کامل با خصوصیات حملات و نحوه مقابله با آنها را دارند. کوین میتنیک[2] که خود از پیشگامان مطرح نمودن موضوع مهندسی اجتماعی است، یکی از همین افراد است که بعنوان مشاور امنیتی سازمان های متعددی فعالیت می‌کند.

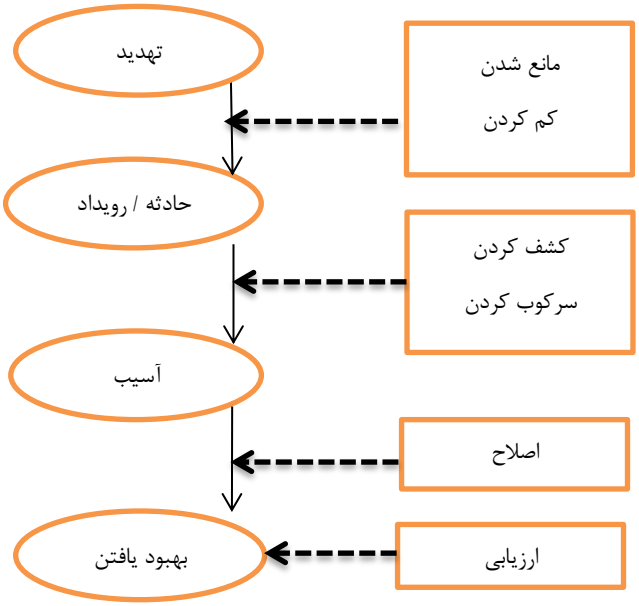
۳-۲-۳- خط مشی مهندسی اجتماعی

خط مشی مهندسی اجتماعی شامل استانداردها و راهنماهایی می‌شود که افراد و سیستم‌ها باید برای رسیدن به اهداف امنیتی مورد استفاده قرار دهند. این خط مشی باید یکپارچه و شفاف باشد و بخوبی ثبت و نگهداری شود تا بیشترین اثربخشی را داشته باشد و در دسترس کلیه پرسنل باشد و از دسترس افراد غیر مجاز دور باشد. این خط مشی‌ها نحوه تقابل سازمان را بر پایه اهداف امنیتی تعیین شده تعریف می‌کنند. کاربردی بودن و امنیت اغلب متناقض هستند. چالشی که وجود دارد اینست که امنیت را با روش‌هایی تأمین نمود که کاربر آنها را بعنوان مزاحمت نشناسد و تمایل به کم کردن آنها نداشته باشد. این کار

[1] Ethical hacker
[2] Kevin mitnick

نه تنها باعث افزایش حملات مهندسی اجتماعی می‌شود بلکه موجب حملات دیگر نیز خواهد شد. طراحی امنیتی باید طوری باشد که مزاحم کاربر نباشد و در صورت امکان حتی کاربر آن را نبیند. فقط تدوین خط مشی کافی نیست بلکه سازمان باید مطمئن شود که کارمندان آن را درک کرده‌اند و تبعات آن را می‌دانند [۴]. روش‌های کنترل خط مشی در شکل (۴) نشان داده شده است. این خط مشی امنیت سازمان را در سه بعد طبقه بندی می‌کند:

- دلیل حفاظت: محافظت از محرمانه بودن، کامل بودن و یا در دسترس بودن
- نوع: فیزیکی، ذهنی یا سازمانی
- زمان عمل: اصلاح کننده، سرکوب کننده، مانع شونده، کشف کننده



شکل (۴): عملکرد کنترلی در خط مشی مهندسی اجتماعی [۲]

عملکرد کنترلی با جایگاه و تأثیر آن در فرآیند مدیریت امنیت مرتبط است. در شکل فوق این ارتباط نشان داده شده است که به شرح ذیل می باشد:

- کنترل پیشگیری کننده: که باید برای جلوگیری از وقوع حملات انجام شود
- کنترل کاهنده: برای کاهش خسارت و آسیب‌های ناشی از حملات موفق لازم است.
- کنترل اکتشافی: برای شناسایی حملات در هنگام وقوع انجام می‌شود تا بتواند به توسعه و تحقق کنترل پیشگیری کننده کمک نماید.
- کنترل سرکوب‌گر: برای جلوگیری از استمرار حمله و کاهش خسارات صورت می‌گیرد.
- کنترل اصلاح کننده: برای بازسازی بعد از حمله بکار می‌رود.
- کنترل ارزیابی: بعد از رخ دادن حمله و پایان آن، برای بررسی دلایل، تبعات و راه حل‌های جلوگیری از آن در آینده، انجام می‌شود.

۳-۲-۴- آموزش

با توجه به منابع متعددی که مورد بررسی قرار گرفتند، باید عنوان کرد که مهم‌ترین روش در مقابله با مهندسی اجتماعی، آموزش فراگیر افراد و سازمان‌هاست. هرچقدر که بشر بیشتر پیشرفت می‌کند بیشتر خودش را تهدید می‌کند. در طول ۲۰۰ سال گذشته معنای مالکیت نیز تغییر کرده است و علاوه بر زمین، ملک و غیره، تفکرات، اطلاعات و هنرهای ما نیز جزء اموال ما هستند [۳۲]. انسان‌ها اصلی‌ترین طعمه در مهندسی اجتماعی هستند. حتی این تفکر که ممکن است جنسیت در میزان هوشمندی در برابر این حملات اثرگذار باشد نیز مورد قبول نیست. در تحقیقی که در سال ۲۰۰۷ انجام شد نشان داده شد که تفاوت قابل ملاحظه‌ای بین زنان و مردان برای افشاء رمزهای عبورشان وجود ندارد. کارمندان باید بدانند که چه نوع از اطلاعات مورد استفاده حمله کننده‌ها قرار می‌گیرد، چه مکالماتی مشکوک هستند، چگونه اطلاعات سری را تشخیص دهند و چگونه در زمان لازم "نه" بگویند. بیشتر کارمندان ارزش اطلاعاتی که در اختیار دارند را نمی‌دانند، اولین مرحله در برنامه‌های آموزشی، نشان دادن میزان اهمیت اطلاعات به کارمندان است. اکثر مهاجمان قبل از حمله، دوستی بلند مدتی با کارمندان برقرار می‌کنند. کارمندان باید بدانند که هر کس در ظاهر دوست آنهاست ممکن است واقعاً اینطور نباشد [۳۳]. حمایت مدیریت در زمینه آموزش بسیار مهم است. بدون حمایت و پشتیبانی مدیریت برنامه‌های آموزشی شکست می‌خورند و خط مشی‌ها دنبال نمی‌شوند. اگر بخواهند ویژگی‌های اصلی یک مهندسی اجتماعی قوی را نام ببرند، به شرح ذیل می‌باشند:

۱- هنر تأثیرگذاری و ترغیب
۲- تمایل به فریب دادن دیگران

مشاهده می‌شود که هر دو این خصوصیات ارتباط مستقیم با انسان دارند، پس مهم‌ترین و ضعیف‌ترین حلقه برای ایجاد امنیت در سیستم‌ها انسان است. مهندسی اجتماعی عموماً موفق است چون افراد بطور طبیعی بدنبال کمک کردن هستند. مثلاً منشی‌ها و کمک‌ها کارشان همین است. البته متأسفانه در حال حاضر سازمان‌ها به خطرات فیزیکی و فنی اهمیت بیشتری می‌دهند تا خطرات انسانی، که این مسأله روند صحیحی نیست. در سال ۲۰۱۲ در انستیتو امنیت کامپیوتر تحقیقی انجام شد که در آن از ۴۷۵ پاسخگو تنها ۴۸٪ بیان کردند که کمتر از یک درصد بودجه امنیت فناوری اطلاعات خود را برای آموزش و آگاهی بخشی کارمندان صرف می‌کنند و تنها ۹٪ آنها بیش از ۵٪ بودجه خود را در این مسیر هزینه می‌کنند [۳۴]. برای رفع این نقص در افراد راهی جز آموزش وجود ندارد. همانطور که در مسائل دیگر اجتماعی و سازمانی تلاش می‌شود تا آگاهی جامعه و سازمان بالا رود، در مورد مهندسی اجتماعی نیز باید به همین صورت عمل شود. حتی دولت‌ها نیز موظفند در این زمینه اطلاع رسانی کنند و برنامه‌های آموزشی را به اجرا دربیاورند. مثلاً در طی جنگ جهانی دوم دولت آمریکا کمپینی را برای امنیت عملیات‌ها ایجاد کرد با شعار " دهانتان را باز کنید، کشتی ها غرق می‌شوند[1]" که نشان دهنده اهمیت حفظ اطلاعات بود [۳۲]. ورکمن[2] بیان می‌کند که آموزش یک عنصر مهم در برخورد با مهندسی اجتماعی است چون می‌تواند به افراد کمک کند که برای اعتماد کردن به دنبال چه چیزی باشند [۷]. یکی از روش‌های مؤثر آموزشی برای آگاه نمودن کاربران، قرار دادن آنها در موقعیت‌های آزمایشی است. باید آنها را در معرض یک فریب قرار داد و واکنش آنها را مورد بررسی قرار داد. در یک مورد واقعی در یکی از شرکت‌های بزرگ یک دوره آموزشی یک ماهه را برای ۵۰۰ نفر از کارمندان خود برگزار کردند که این امر باعث کاهش ۵۰ درصدی افراد فریب خورده شد [۵]. برنامه آگاهی امنیتی باید آگاهی مستمری از خط مهندسی اجتماعی در میان کارمندان سازمان بدهد. این برنامه باید شامل آموزش‌هایی باشد که به افراد یاد دهد چطور حملات را شناسایی کنند و با استفاده از خط مشی‌ها و رویه‌ها آن را خنثی نمایند. هدف نهایی برنامه آگاهی، ایجاد یک فرهنگ است که در آن افراد بطور مستمر از خطرات مهندسی اجتماعی آگاه باشند و آماده مقابله باشند [۳۵]. یکی از روش‌های ساده‌ای که در سازمان‌ها جهت آگاهی بخشی به افراد به کار می‌رود، استفاده از پوسترها و بولتن‌های آموزشی است. یک پوستر خوب برای مقابله با مهندسی اجتماعی در سازمان باید چهار ویژگی داشته باشد:

۱- محتویات گسترده در هر پوستر و به روز بودن
۲- جزئیات زیادی در آن نباشد و گیرا باشد
۳- پیام دقیق و قابل درک باشد
۴- اطلاعات برقراری تماس با مسئول در صورت مشاهده حمله را داشته باشد

اگر شما خودتان به حملات مهندسی اجتماعی علاقه‌ای ندارید نمی‌توانید از کارکنانتان هم چنین انتظاراتی داشته باشید. باید منابعی را برای ارزیابی ریسک، تعریف خط مشی‌ها و مطمئن شدن از اینکه کارکنانتان انتظارات شما را می‌دانند اختصاص دهید. سطوح شغلی مختلف آموزش‌های مختلفی را نیز می‌طلبند. پرسنل فناوری اطلاعات نیاز به دانش امنیتی عمیق‌تری نسبت به دیگران دارند. حتی پرسنلی که وظایف امنیتی را بر عهده دارند اگر خودشان نیز کاربر کامپیوتر نباشند باید آشنایی کلی با فناوری داشته باشند. هم چنین بخش‌هایی که هدف اصلی تهاجم مهندسان اجتماعی قرار می‌گیرند مانند واحد منابع انسانی، باید مورد توجه خاصی برای آموزش قرار گیرند.

۳-۲-۵- مدل مدیریت ریسک مهندسی اجتماعی

این مدل یکی دیگر از روش‌هایی است که سازمان‌ها مورد استفاده قرار می‌دهند تا بتوانند فرآیند جامعی برای مقابله با مهندسی اجتماعی داشته باشند.

ریسک مهندسی اجتماعی می‌تواند کل استخدام یک فرد در سازمان را تحت تأثیر قرار دهد. قبل از استخدام کردن فرد بهتر است سابقه او را مورد بررسی قرار دهید که مورد جنایی یا مشکوکی در پرونده وی نباشد. در زمان استخدام فرد باید بپذیرد که خط مشی‌ها و اصول امنیتی سازمان را بپذیرد و در صورت تغییر با رویه‌های جدید خود را سازگار کند. برای آگاهی از اینکه

[1] Loose Lips, Sink Ships
[2] Workmann

آیا کارمند از وظایف امنیتی خود آگاه است می‌توان یک آزمون فیزیکی یا مجازی، ذهنی ترتیب داد. تحقیقی در بی بی سی[1] انجام شد که نشان داد ۷۰٪ افراد حاضرند در برابر یک شکلات رمز عبور خود را فاش کنند. البته اینکه چه تعداد از این رمزها صحیح است مشخص نیست اما باید بدانید که برای یک مهندس اجتماعی حتی یک رمز عبور هم کافیست تا به اهدافش دست یابد [۳۶].

مدل مدیریت ریسک مهندسی اجتماعی باید بتواند با فرآیندها و مدل‌های امنیتی فعلی ارتباط برقرار کند.

سازمان‌ها می‌توانند از مدیریت ریسک مهندسی اجتماعی به دلایل زیر استفاده کنند:

- به سازمان‌ها کمک می‌کند که سطح ایمنی خود را منطبق با استراتژی خود نماید
- به سازمان‌ها کمک می‌کند که از پاسخ‌های ریسک مختلف شناسایی و انتخاب کند
- به آنها کمک می‌کند که ریسک‌های مشترک و مرتبط و اثرات آنها را شناسایی کند
- به آنها کمک می‌کند که عدم اطمینان و در نهایت خسارت و زیان را کاهش دهد [۳۷]

اگر بخواهند که بطور خلاصه مراحل دفاع چند لایه در برابر حملات مهندسی اجتماعی را ذکر کنند به ترتیب ذیل می‌باشند:

۱) ایجاد خط مشی امنیتی در جهت مقابله با مهندسی اجتماعی: برای اینکه بتوان دفاع هدفمندی در برابر مهندسی اجتماعی داشت، سازمان باید یک خط مشی مشخص و برنامه ریزی شده داشته باشد. این خط مشی به سازمان کمک می‌کند که بتواند در مقابل انواع حملات و تهاجم‌ها مقاومت نماید و روش‌های مختلف دفاعی را بکار گیرد.

۲) آموزش آگاهی دهنده امنیتی برای تمام کاربران: یکی از آموزش‌هایی که لازم است تا همه افراد سازمان ببینند، آموزش آگاهی دهنده برای آشنایی با خطرات فضای سایبر است. تمام افراد سازمان چه در واحد فناوری اطلاعات باشند و یا دسترسی به اطلاعات طبقه بندی شده داشته باشند یا نه، باید آگاهی نسبی از مباحث امنیتی در فضای مجازی داشته باشند.

۳) آموزش پایداری برای نفرات کلیدی سازمان: افرادی هستند که در بعد اطلاعاتی و امنیتی در سازمان اهمیت بسیاری دارند. این افراد یا در واحد فناوری اطلاعات کار می‌کنند و یا در سطوح مدیریتی قرار دارند. هم چنین افرادی که بعنوان منشی فعالیت می‌کنند نیز در معرض خطرات بسیاری هستند. این گروه افراد نیازمند آموزش‌های دیگری غیر از آموزش‌هایی هستند که به همه افراد داده می‌شود. اینها باید نحوه مقابله با حملات احتمالی و روش‌های دفع آنها را بطور کامل بشناسند تا بتوانند در واقع لزوم به سازمان کمک کنند.

۴) یادآوری مستمر: یکی از نکات بسیار مهم در بحث آموزش یادآوری و بازآموزی است. آموزش یک فرآیند دائمی و پیوسته است. چون خطرات سایبری و روش‌های حمله بطور دائم در حال پیشرفت و بروزرسانی هستند پس مباحث آموزشی نیز باید بطور مستمر مورد توجه قرار گیرند.

۵) مین گذاری برای مهندسی اجتماعی ۲ : سازمان‌ها برای مقابله با مهندسی اجتماعی دام‌هایی ایجاد می‌کنند تا بتوانند نقاط ضعف خود را بیابند. این دام‌ها به سازمان برای دفع حملات و مقابله با مهاجمان کمک می‌کنند.

۶) پاسخ واقعی: زمانی که سازمان با حملات مواجه می‌شود، نیاز دارد تا یک پاسخ مناسب برای دفع آنها داشته باشد. روش‌های دفاعی که در این پژوهش ذکر شدند، در این مرحله مورد استفاده قرار می‌گیرند تا بتوانند موجب جلوگیری از ایجاد آسیب‌های بیشتر شوند و سازمان را برای ادامه مسیر یاری کنند.

۳-۳- جدول جامع دفاعی

اگر بخواهند که مهم‌ترین روش‌های ذکر شده برای حملات مهندسی اجتماعی و راه‌های مقابله با آنها را بصورت مدون در یک جدول بیاورند، می‌توان از جدولی که مؤسسه وریزون در سال ۲۰۱۲ تهیه نموده است، استفاده نمود. (جدول ۱)

[1] BBC

[2] SELM

جدول (۱): جدول جامع دفاعی [۳۸]

حوزه ریسک	تاکتیک حمله	استراتژی مقابله
تلفن (منشی)	جعل هویت و ترغیب	آموزش کارمندان و منشی‌ها که هیچ وقت رمزهای عبور و اطلاعات دیگر را از طریق تلفن افشاء نکنند
ورودی ساختمان	دسترسی فیزیکی غیر مجاز	حفاظ امنیتی قدرتمند، آموزش کارکنان و حضور نیروهای حفاظتی
دفتر کار	مخفیانه نگاه کردن	در حضور دیگران هیچ رمز عبوری را وارد نکنید
تلفن (منشی)	جعل هویت در تماس های منشی	تمام کارمندان و منشی‌ها باید یک PIN اختصاصی داشته باشند
ساختمان	گشتن در راهروها به دنبال اتاق‌های باز	تمام مهمان‌ها باید اسکورت داشته باشند
دبیرخانه	قرار دادن نامه‌های جعلی	دبیرخانه را قفل کنید و از طریق دوربین تحت نظر داشته باشید
اتاق ماشین آلات و ارتباطات	تلاش برای دسترسی، جابجایی تجهیزات و یا الحاق آنالیزگر اسناد برای ربودن داده‌های سری	درب این اتاق‌ها را بسته نگه دارید
تلفن	سرقت خطوط تلفنی	تماس‌های راه دور و خارج از کشور را کنترل کنید و در صورت لزوم ردیابی کنید
زباله‌ها	گشتن زباله‌ها	تمام زباله‌ها را در مکانی امن و تحت نظر قرار دهید. داده‌های مهم را خرد کنید و اطلاعات دیجیتالی را پاک نمایید
اینترنت/ اینترانت	ساخت و نفوذ بدافزارها برای سرقت رمزهای عبور	آگاهی مستمر از سیستم و تغییرات شبکه، آموزش برای استفاده از رمزهای عبور
عمومی / روانشناختی	جعل هویت و ترغیب	کارمندان را همواره از طریق برنامه‌های آموزشی مستمر آگاه نگه دارید
ساختمان	سرقت اسناد مهم و حساس	اسناد محرمانه را علامت گذاری کنید و آنها را در جایی امن و محفوظ نگه دارید

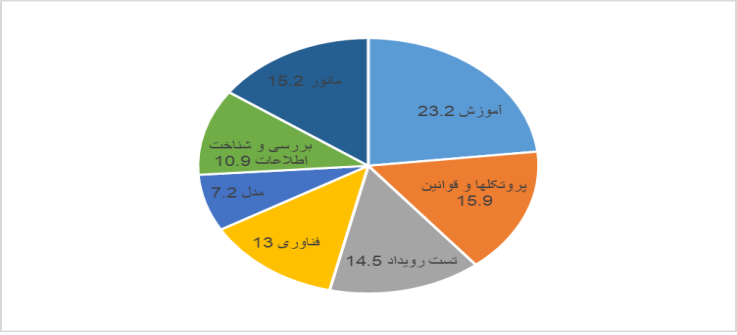
با مروری بر روش‌های بالا می‌توان بیان داشت سازمان‌ها خطرات امنیتی خود را با موارد زیر می‌توانند کاهش دهند:

- آموزش به کارکنان: آموزش کارکنان در پروتکل‌های امنیتی مرتبط با موقعیت آنها. (به عنوان مثال، اگر هویت یک فرد قابل تأیید نباشد، باید به کارکنان آموزش داده شود تا مودبانه امتناع کنند.)
- چارچوب استاندارد: ایجاد چارچوب‌های اعتماد در سطح کارمند/ پرسنل (به عنوان مثال، مشخص کردن و آموزش پرسنل در زمان/ کجا/چرا/چگونه اطلاعات حساس باید مدیریت شوند)
- بررسی دقیق اطلاعات: شناسایی اطلاعات حساس و ارزیابی قرار گرفتن در معرض مهندسی اجتماعی و خرابی در سیستم‌های امنیتی (ساختمان، سیستم کامپیوتری و غیره)
- پروتکل‌های امنیتی: ایجاد پروتکل‌ها، سیاست‌ها و رویه‌های امنیتی برای مدیریت اطلاعات حساس.
- تست رویداد: انجام آزمایش‌های دوره‌ای و اعلام نشده چارچوب امنیتی.
- شبیه‌سازی/مانور: جلوگیری از مهندسی اجتماعی و دیگر ترفندها یا تله‌های متقلبانه با القای مقاومت در برابر تلاش‌های متقاعدسازی از طریق قرار گرفتن در معرض تلاش‌های مشابه یا مرتبط.
- بررسی: مرور مراحل بالا به طور منظم: هیچ راه حلی برای یکپارچگی اطلاعات کامل نیست.
- مدیریت پسماند: استفاده از سرویس مدیریت پسماند با کلید محدود و توام با نظارت.

با توجه به نتایج حاصله در بالا، در قسمت بعدی پژوهش از روش دلفی و استفاده از آرای صاحبنظران که یک رویکرد تحقیقاتی است، برای بدست آوردن متغیرهای موثر و اولویت بندی آنها استفاده شده و قسمتی از فرایند اجرای تحقیق، به مصاحبه و تکمیل پرسشنامه توسط خبرگان اختصاص یافت.

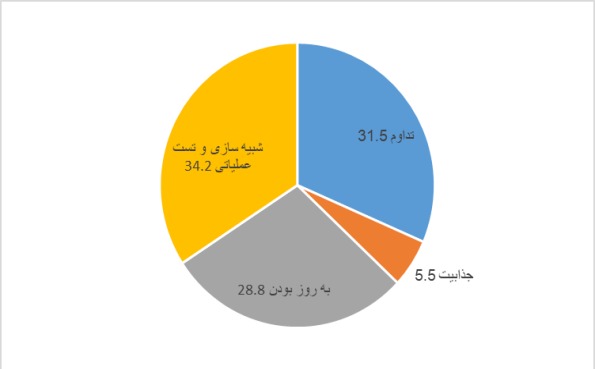
روش دلفی یکی از روش‌های پیش بینی و تصمیم‌گیری گروهی است که در آن برای دستیابی به توافق پیرامون مساله مورد بررسی، از دیدگاه خبرگان استفاده می‌شود. این روش، یک فرایند چند مرحله‌ای ساختار یافته برای جمع آوری و تجمیع دانش از گروهی از متخصصان برای حل یک مشکل (مسأله) با استفاده از مجموعه‌ای از پرسشنامه‌ها که با باز خورد کنترل شده منتشر شده‌اند، است [۳۹]. دلفی بر این اصل استوار است که پیش‌بینی‌ها (یا تصمیم‌گیری‌ها) توسط یک گروه ساختاریافته از افراد (خبرگان انتخاب شده)، دقیق‌تر از گروه‌های بدون ساختار است [۴۰]. این روش برای «شناسایی» و «غربال» مهم‌ترین شاخص‌های تصمیم‌گیری قابل استفاده است. دلفی همچنین می‌تواند برای کمک به دستیابی به اجماع کارشناسان و توسعه دستورالعمل‌های حرفه‌ای استفاده شود [۴۱]. بر همین اساس در این پژوهش، از روش دلفی جهت تعیین اهمیت و اولویت عوامل موثر در پدافند مهندسی اجتماعی استفاده شده است. از این رو، بر مبنای روش دلفی، با پانزده نفر از خبرگان، مسئولین و اساتیدی که در حوزه‌های پدافند غیرعامل و امنیت صاحب نظر و فعال بودند، مصاحبه شده و در سه دور پرسشنامه مربوط جهت اولویت بندی عوامل موثر بر پدافند مهندسی اجتماعی توسط این افراد تکمیل شد.

بر اساس روش فوق، در مرحله اول از خبرگان پرسش شونده خواسته شد که با توجه به شاخص‌هایی چون میزانِ تأثیر، زمانِ تأثیر، هزینه و قابلیت اجرا نسبت به تعیین اولویت و اهمیت هر یک از عوامل مطرح در پدافند مهندسی اجتماعی اعم از آموزش، پروتکل‌ها و قوانین، تست رویداد، فناوری، مدل، بررسی اطلاعات و مانور پرداخته شود که نتایج این مرحله در شکل ۵ به نمایش درآمده است. بر این مبنا و بر اساس نتیجه حاصل از نظرات خبرگان، در بین عوامل موثر در پدافند مهندسی اجتماعی، موثرترین عامل را می‌باید بحث آموزش دانست. بعد از آموزش و با فاصله‌ای قابل توجه، به ترتیب پروتکل‌ها و قوانین، تست رویداد، بررسی و شناخت اطلاعات، فناوری و در نهایت مدل قرار می‌گیرند. اختلاف قابل توجهی که آموزش با عوامل بعدی دارد، تاکید موکدی بر اهمیت فوق‌العاده آن در پدافند مهندسی اجتماعی می‌باشد.



شکل (۵): نمودار تأثیر و اهمیت عوامل موثر بر پدافند مهندسی اجتماعی (برحسب درصد)

با توجه به مشخص شدن آموزش به عنوان موثرترین عامل در پدافند مهندسی اجتماعی، در مرحله بعد و جهت تعیین اولویت عوامل موثر در آموزش و مشخص شدن میزان اهمیت آنها، چهار عامل موثر در آموزش اعم از تداوم آموزش، شبیه سازی و تست عملیاتی، به روز بودن و جذابیت مورد پرسش از خبرگان قرار گرفتند که نتایج آن در شکل (۶) نمایش داده شده است.



شکل (۶): نمودار مقایسه عوامل موثر در آموزش (بر حسب درصد)

بر اساس نتایج حاصل از نظر خبرگان و همانطور که در شکل (۶) مشخص است عامل شبیه سازی و تست عملیاتی آموزش، به عنوان مهم‌ترین و تأثیرگذارترین عامل در آموزش بوده و پس از آن تداوم آموزش و به روز بودن آن، در مراتب بعدی تأثیر و اهمیت قرار می‌گیرند.

بر این مبنا و با توجه به نتایج حاصل از نظر خبرگان که در دو شکل (۵) و (۶) نمایش داده شده است، می‌توان بیان داشت که آموزش موثرترین عامل و رکن اصلی موفقیت در پدافند حملات مهندسی اجتماعی بوده و در خود آموزش نیز، شبیه سازی و تست عملیاتی و تداوم آموزش را می‌باید به عنوان مهم‌ترین و موثرترین عوامل موثر در آموزش، جهت داشتن آموزشی موثر، و بالتبع آن داشتن دفاع موفق در برابر حملات مهندسی اجتماعی محسوب نمود.

۴- نتیجه گیری

مهندسی اجتماعی مفهومی است که بر پایه ویژگی‌های روانشناختی انسان و آسیب‌پذیری‌های انسانی مبتنی بر آن استوار است. این مشخصه مهم، حملات مهندسی اجتماعی را از ویژگی‌های خاصی برخوردار می‌سازد و بدیهی است پدافند در برابر این حملات دقت و ظرافت‌های خاص خود را می‌طلبد. هر سازمان و مجموعه‌ای حتی اگر به لحاظ فناورانه از سطوح بالایی برخوردار باشد، اما کماکان وجود انسان در آن به عنوان حلقه ضعفی در حلقه پدافندی آن محسوب می‌شود که می‌باید همواره به آن توجه نمود. در این پژوهش روش‌های مختلفی جهت پدافند حملات مهندسی اجتماعی ارائه شد که در میان همه موارد انسان محورانه‌ای که هر سازمانی به آن می‌باید توجه نماید، حوزه آموزش نیروی انسانی را می‌توان محور تمامی این موارد نامید. در این میان دو اصل آموزش مبنی بر تداوم آموزش، و گرفتن بازخورد و تثبیت و اثربخشی آموزش از طریق تداوم و عملیاتی نمودن آموزش را می‌توان ارکان اساسی آن دانست که تمامی سازمان‌ها موارد و روش‌های پدافندی ارائه شده در این پژوهش را با تأکید بر این اصول می‌باید مورد توجه قرار دهند. رفتار کارکنان می‌تواند تأثیر زیادی بر امنیت اطلاعات در سازمان‌ها داشته باشد. آموزش موثر شکل دهنده الگوهای رفتاری در هر سازمانی بوده و مجموعه الگوهای رفتاری، فرهنگ امنیت اطلاعات را در سازمان شکل می‌دهد و بدیهی است که حصول چنین شرایطی می‌تواند پدافند موثر در برابر مهندسی اجتماعی و حفاظت اطلاعات از هر نوع را موفق سازد. البته باید توجه داشت که فرهنگ امنیت اطلاعات باید به طور مداوم بهبود یابد و این فرایندی بی پایان است که آموزش حرف اول آن است.

۵- مراجع

[1] L. Janczewski, “Social engineering based-attacks Model & New Zealand perspective”, Computer science & information technology, 2010.
[2] B. Oosterloo, “Managing social engineering risk”, Atos consulting, p. 27, 2008.
[3] A. A. Taghipour, A. Mashayekhi, and P. Ahmadi Dehrashid, “Assessing Citizen’s Attitudes Toward Security in Cyberspace with a Passive Defense Approach”, Scientific Journal of Passive Defense, no. 52, Winter 2023. (In Persian)
[4] S. Heikkinen, “Social engineering in the world of emerging communication technologies”, Tampere university of technology, 2007.
[5] RSA, “Social engineering & cyber attacks”, RSA, 2011
[6] N. Pavkovic and L. Perkov, “Social engineering toolkit- A systematic approach to social engineering”, Ruder boskovic institute, 2011.
[7] R. Brody, W. Brizzee, and L. Cano, “Flying under the radar: social engineering”, International journal of accounting & information management, 2012.
[8] B. Oosterloo, “Managing social engineering risk”, Atos consulting, p. 18, 2008.
[9] R. Cialdini, “Influence”, G. Ghasem zadeh, Tehran: Hoormazd, 7 ed., 2022. (In Persian)
[10] R. J. Anderson, “Security engineering: a guide to building dependable distributed systems” (2 ed.), Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, p. 17, 2008.
[11] Security Through Education, “Social Engineering Defined”, Security Through Education, https://www.social-engineer.org/framework/general-discussion/social-engineering-defined.
[12] George Washington university, “Social engineering – GW Information Security”, www.gwu.edu, George Washington university, Washington D.C., 2020.
[13] B. Kirdemir, “Hostile Influence and Emerging Cognitive Threats in Cyberspace”, Centre for Economics and Foreign Policy Studies, 2019.
[14] I. Austen, “On EBay, E-Mail Phishers Find a Well-Stocked Pond”, The New York Times, ISSN 0362-4331, 7 March 2005.
[15] K. Steinmetz, F. Holt, and J. Thomas, “Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations”, Social Science Computer Review: 5 August

2022, doi:10.1177/08944393221117501, ISSN 0894-4393, S2CID 251420893, 2022.
[16] FireEye, “The Real Dangers of Spear-Phishing Attacks”, FireEye Inc, 2016.
[17] F. Davani, “The story of HP pretexting scandal with discussion” is available at Davani, Faraz (14 August 2011), "HP Pretexting Scandal by Faraz Davani”, 2011.
[18] Federal Trade Commission, “Pretexting: Your Personal Information Revealed”, Federal Trade Commission, 2022.
[19] J. Fagone, "The Serial Swatter", The New York Times, 24 November 2015.
[20] Invincea, “Chinese Espionage Campaign Compromises Forbes.com to Target US Defense, Financial Services Companies in Watering Hole Style Attack”, invincea.com, 10 February 2015.
[21] W. Conklin, A. Greg, C. Cothren, R. Davis, and D. Williams, “Principles of Computer Security”, Fourth Edition (Official Comptia Guide), New York: McGraw-Hill Education, pp. 193–194, ISBN 978-0071835978, 2015.
[22] D. Raywood, “#BHUSA Dropped USB Experiment Detailed”, info security, 4 August 2016.
[23] J. Leyden, “Office workers give away passwords”, 18 April 2003.
[24] BBC, “Passwords revealed by sweet deal”, BBC News, 20 April 2014.
[25] F. Mouton, M. Malan, and H. S. Venter, “Social engineering from a normative ethics perspective”, University of petroria, 2013.
[26] A. Podhradsky and C. Casy, “Xbox 360 hoaxes, social engineering and gamer tag exploits”, 2013.
[27] R. Cressey and M. Nayfeh, “Cyber capabilities in the middle east”, Booz Allen Hamilton Inc, 2012.
[28] R. Chapman and C. Hannigan, (n.d.), “Social engineering networks”, 2014.
[29] Trend Micro, “How social engineering works. Trend Micro”, www.trendmicro.com, 2012.
[30] M. Bada and J. Nurse, “The social and psychological impact of cyberattacks”, Academic press, 2019.
[31] T. Bakhshi, M. Papadaki, and S. Furnell, “Social engineering: assessing vulnerabilities in practice”, Information management & computer security, 2009.
[32] T. Thornburgh, “Social engineering: The Dark Art”, Kennesaw state university, 2012.
[33] A. Chantler, “Social engineering & crime prevention in cyberspace”, 2006.
[34] Enisa, “Social engineering: The weakest link”, Enisa Inc, 2008.
[35] B. Oosterloo, “Managing social engineering risk”, Atos consulting, p. 53, 2008.
[36] J. Treglia and M. Delia, “Cyber Security Inoculation”, Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, 3–4 June, 2017.
[37] B. Oosterloo, “Managing social engineering risk”, Atos consulting, p. 60, 2008.
[38] Verizon, “Data breach investigation”, Verizon Inc, 2012.
[39] M. Adler and E. Ziglio, “Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health”, Jessica Kingsley Publishers, p. 12, 1996.
[40] G. Rowe and G. Right, “Expert Opinions in Forecasting. Role of the Delphi Technique”, Principles of Forecasting: A Handbook of Researchers and Practitioners. International Series in Operations Research & Management Science, Vol. 30, Boston: Kluwer Academic Publishers, pp: 125–144, 2001.
[41] E. Taylor, “We Agree, Don't We? The Delphi Method for Health Environments Research”, HERD, 13 (1), pp: 11–23, 2020.