چهارمین کنفرانس
دانشجویان مهندسی کامپیوتر و فناوری اطلاعات و ارتباطات
4th Conference on
Computer Engineering, Information Technology and Communications Students

مهندسی اجتماعی: از هک ذهن انسان و نقش هوش مصنوعی در فریب سایبری

محمدجواد مجدمی ۱، عیسی جعفری ۲

۱-دانشجوی مهندسی کامپیوتر، نرم افزار، دانشگاه ملی مهارت، دانشکده پسران شهید چمران اهواز، اهواز، ایران
mohammadmjm9@gmail.com
۲-کارشناسی ارشد مدیریت فناوری اطلاعات، اهواز، ایران
jafari.e@scu.ac.ir

چکیده

در دنیای امروز، هوش مصنوعی به‌سرعت در حال پیشرفت و توسعه است و در پی آن، استفاده‌های نادرست از آن نیز بیشتر می‌شود. با پیشرفت هوش مصنوعی، بستری فراهم می‌شود که هکرها و نفوذگران با استفاده از تکنیک‌های مهندسی اجتماعی و استفاده از ابزارهای هوش مصنوعی، بتوانند، حملات پیچیده‌تر و باورپذیرتر و شخصی‌سازی‌شده‌تری طراحی کنند. ما در این مقاله با ارائه مثال‌هایی، به مبحث مهندسی اجتماعی و هک ذهن انسان، و همچنین تأثیر روزافزون هوش مصنوعی بر مهندسی اجتماعی و امنیت سایبری می‌پردازیم و آن را بررسی می‌کنیم. تکنیک‌های مهندسی اجتماعی و در ادامه ابزارهای مهندسی اجتماعی مبتنی بر هوش مصنوعی را شرح می‌دهیم و بررسی می‌کنیم.

هدف این مقاله آشنایی با مهندسی اجتماعی و تأثیر هوش مصنوعی بر آن، و شناختی عمیق‌تر از ماهیت و عملکرد مهندسی اجتماعی سنتی و مدرن است، و بررسی این که چگونه پیشرفت هوش مصنوعی می‌تواند تهدیدی جدی و درعین‌حال فرصتی برای دفاع هوشمندانه‌تر در برابر حملات مهندسی اجتماعی باشد. در پایان هم به راه‌حل‌هایی برای دفاع در برابر حملات مهندسی اجتماعی و مهندسی اجتماعی مبتنی بر هوش مصنوعی می‌پردازیم.

کلمات کلیدی: مهندسی اجتماعی، هکر، نفوذ، امنیت سایبری، هک، ذهن انسان، هوش مصنوعی.

۱. مقدمه

در عصر امروز که روزبه‌روز بیشتر به سمت دیجیتالی‌شدن می‌رود، مهندسی اجتماعی به‌عنوان یکی از پیچیده‌ترین و مؤثرترین روش‌های حمله سایبری شناخته می‌شود که بر خلاف روش‌های سنتی که هکرها به کار می‌گرفتند، روی ذهن انسان‌ها کار می‌کند و بجای نفوذ در کامپیوترها و سیستم‌ها به ذهن انسان‌ها نفوذ می‌کند و آنها را فریب می‌دهد. این نوع حملات که یک نوع از دست‌کاری روانی محسوب می‌شوند، بر اصول اصلی رفتار انسانی مانند اقتدار، ترس‌ها و یا تأیید اجتماعی افراد تکیه می‌کنند تا افراد را به افشای اطلاعات محرمانه یا انجام اعمال موردنیاز مهاجم یا هکر، مجبور کنند. [1] برای دفاع در برابر حمله‌های سایبری مهندسی اجتماعی لازم است که درک عمیق‌تری نسبت به این موضوع داشته باشیم که این حملات سایبری از چه جنبه‌هایی از شناخت انسان سوءاستفاده می‌کنند، چرا انسان‌ها در معرض این نوع حملات قرار می‌گیرند و چگونه می‌توانیم آسیب های آنها را به حداقل برسانیم یا حداقل کاهش دهیم.

با ورود هوش مصنوعی به حوزه مهندسی اجتماعی، و تأثیر هوش مصنوعی مولد همچون Chat GPT بر این حوزه، این فناوری، باعث خودکارسازی وظایف مختلف روزمره، شده است. این خودکارسازی وظایف توسط عوامل هوش مصنوعی که نرم‌افزارهای جداگانه‌ای هستند و برای انجام وظایف و اقدامات مختلف طراحی شده‌اند، انجام می‌شود که مشاغل در صنایع مختلف در حال پذیرش این ابزارهای مبتنی بر هوش مصنوعی هستند.[2]

بااین‌وجود، ظهور مدل‌های هوش مصنوعی منجر به ظهور حملات سایبری جدیدی شده است که به‌عنوان حملات مبتنی بر هوش مصنوعی شناخته می‌شوند و با خودکارسازی و طراحی حملات قابل باورپذیرتر و شخصی‌سازی‌شده‌تر به هکرها و مهندسان اجتماعی کمک می‌کنند که بتوانند حملات مبتنی بر مهندسی اجتماعی بهتر و حساب‌شده‌تر و کامل‌تری داشته باشند. با افزایش روزبه‌روز داده‌های شخصی در محیط سایبری و پیچیده‌تر شدن ابزارهای هوش مصنوعی، هکرها و مهندسان اجتماعی، می‌توانند حملات مبتنی بر مهندسی اجتماعی راحت‌تر و فریبکارانه‌تری داشته باشند و همچنین افرادی که دارای علم کمتر و تجربهٔ کمتری در حوزه مهندسی اجتماعی هستند نیز می‌توانند حملات مبتنی بر مهندسی اجتماعی را طراحی کنند.[2]

این مقاله به بررسی مهندسی اجتماعی و ابزارهای آن، و ظهور و نقش هوش مصنوعی در این حوزه و فریب سایبری و راهکارهای دفاعی برای مقابله با آن، می‌پردازد.

۲. مفهوم هک ذهن انسان

مفهوم هک ذهن انسان در مهندسی اجتماعی، به تلاش هکرها و نفوذگران برای استفاده از ضعف‌های روان‌شناختی و نداشتن علم کافی انسان‌ها برای افشای اطلاعات حساس و محرمانه و انجام کارهای مخرب، اشاره دارد. در این روش هکرها به‌جای نفوذ به سیستم‌های فنی که به زمان و هزینهٔ زیادی نیاز دارند، و همچنین با عناصر امنیتی پیچیده‌ای محافظت می‌شوند و نفوذ به آنها بسیار دشوار است، ذهن انسان‌ها را هدف قرار می‌دهند. زیرا انسان‌ها همیشه در دسترس هستند و می‌توانند به هکرها و نفوذگران در مدت‌زمان کمتری اطلاعات محرمانه بیشتری ارائه دهند. هکرها دریافتند که هک‌کردن ذهن انسان‌های امروزی خیلی آسان‌تر از هک‌کردن سیستم‌های یک سازمان است، به همین

دلیل است که یک متخصص مهندسی اجتماعی می‌تواند در عرض یک ساعت به‌اندازه ۱۰۰ ساعت تلاش یک تیم هکری برای نفوذ به سیستم‌های محافظت شده یک سازمان اطلاعات جمع‌آوری کند. همین موضوع باعث افزایش تعداد حملات مهندسی اجتماعی شده است و نفوذگران ترجیح می‌دهند که بیشتر روی ذهن انسان‌ها کار کنند.[3]

۳. روانشناسی تاریک

روان‌شناسی تاریک (سیاه) یکی از زیرشاخه‌های علم روان‌شناسی است که ذهن افراد را دست‌کاری می‌کند، آنها را برای اهداف خودفریب می‌دهد و افراد را متقاعد یا اجبار می‌کند که به خود یا دیگران و یا یک سازمان آسیب برساند. روان‌شناسی تاریک جنبه‌های تاریک‌تر طبیعت انسان‌مانند مهندسی افکار، کنترل ذهن و متقاعدسازی را در بر می‌گیرد. این حوزه از علم روان‌شناسی می‌تواند بسیار جذاب، اما درعین‌حال نگران‌کننده و خطرناک باشد. به‌طورکلی، روان‌شناسی تاریک به‌عنوان سوءاستفاده و دست‌کاری روان‌شناختی یا عاطفی شناخته شود. دست‌کاری روان‌شناختی نوعی تأثیر اجتماعی است که هدف آن تغییر رفتار یا برداشت دیگری ازطریق روش‌های غیرمستقیم، فریب‌آمیز یا پنهان است. دست‌کاری کنندگان با بهره‌برداری از آسیب‌پذیری و ضعف‌های افراد، می‌توانند به طور نامحسوس آن‌ها را به کارهایی تشویق کنند که در حالت معمول انجام نمی‌دهند. افرادی که دست به این کار می‌زنند، با درک نحوه تفکر و احساس افراد به‌راحتی می‌توانند ذهن افراد را دست‌کاری کنند تا کاری را انجام دهند که آن‌ها می‌خواهند. از رویکرد مذکور می‌توان برای هر هدفی استفاده کرد؛ از مجبور کردن فرد برای خرید محصولی که به آن نیازی ندارد تا متقاعدکردن او برای ارتکاب جرم و افشای اطلاعات حساس و محرمانه یک سازمان، یا انجام کارهای مخرب. مهندسین اجتماعی و هکرها، از این زیر شاخه روان‌شناسی برای رسیدن به اهدافشان استفاده می‌کنند.[4]

۴. مفهوم مهندسی اجتماعی

مهندسی اجتماعی (Social Engineering) یک تکنیک مجرمانه است که در آن هکرها می‌توانند به طور غیرمستقیم و با استفاده از تأثیرگذاری بر روی احساسات، روان‌شناسی و رفتار افراد، اطلاعات محرمانه و شخصی را به دست آورند، دسترسی به سیستم‌ها و منابع محدود را به دست آورند یا فعالیت‌های غیرقانونی را انجام دهد. در واقع، مهندسی اجتماعی از ضعف‌ها و نقاط ضعف روانی و اجتماعی افراد برای رسیدن به اهداف خود استفاده می‌کند.
روش‌های مهندسی اجتماعی شامل تکنیک‌ها و فنون مختلفی است که استفاده از آن‌ها می‌تواند شامل تهدیدات کذب، مراحل تست نفوذ (penetration testing) یا هرگونه فعالیت مجرمانه‌ای باشد که به‌منظور دسترسی به شبکه‌های سازمانی انجام می‌شود. این روش‌ها و تکنیک‌ها می‌توانند شامل تقلید هویت، تکنیک‌های مهندسی اجتماعی، استفاده از تکنیک‌های جعلی، استفاده از هوش مصنوعی و چت‌بات‌ها و تلاش برای متقاعدکردن و فریب‌دادن افراد به‌منظور ارائه اطلاعات محرمانه، کلمات عبور یا دسترسی به سیستم‌ها باشند. اهداف مهندسی اجتماعی نیز می‌تواند شامل دستیابی به اطلاعات حساس، سرقت هویت، دسترسی غیرمجاز به سیستم‌ها و شبکه‌ها، به‌دست‌آوردن رمزهای عبور، انجام تقلب مالی، فریب‌دادن افراد برای انجام کارهای مجرمانه یا بهره‌برداری از اعتماد و هویت افراد باشد.[5]

۵. مثال های مهندسی اجتماعی

مثال‌های زیادی دراین‌رابطه وجود دارد، و هکران و نفوذگران و مهندسان اجتماعی با استفاده از تکنیک‌های متنوعی از مهندسی اجتماعی، دست به فریب‌دادن و سو استفاده از افراد می‌زنند. به‌عنوان‌مثال: فردی با نزدیک‌شدن به شما از شما می‌خواهد یک فلش آلوده را به سیستم‌های یک سازمان وصل کنید، یا اینکه با تماس‌گرفتن به فرد قربانی و

پخش گردن صدای گریهٔ بچه، از احساسات فرد سو استفاده می‌کند و با تکنیک‌هایی به اطلاعات آن فرد دسترسی پیدا می‌کند. همچنین مهندسان اجتماعی با فرستادن لینک‌ها و پیام‌های آلوده (فیشینگ) سعی می‌کنند اطلاعات افراد را سرقت کنند و آن‌ها را فریب دهند.

نائوکی هیروشیما که یک کاربر عادی توییتر بود، قربانی مهندسی اجتماعی شد، به این‌گونه که فرد مهاجم برای به‌دست‌آوردن نام کاربری توییتر او که آیدی خاصی داشت و تک حرفی بود (N@) به خدمات مشتری پی پال زنگ‌زده و وانمود می‌کند به اینکه کارمند بخش دیگر این شرکت است، اطلاعات مربوط به چهار رقم آخر کارت اعتباری نائوکی را از آن‌ها می‌گیرد. بعد با شرکت ثبت دامنه و میزبانی وب GoDaddy تماس می‌گیرد که وب‌سایت نائوکی در آنجا میزبانی می‌شد. این هکر با داشتن چهار عدد کارت اعتباری، از GoDaddy می‌خواهد رمز عبور وب‌سایت نائوکی را ریست کند. حالا هکر این قدرت را داشت تا تمام اطلاعات وب‌سایت نائوکی را پاک کند و این تهدید کافی بود تا نائوکی حاضر شود نام کاربری خود را در اختیار هکر قرار دهد.[6]

۶. تاریخچه مهندسی اجتماعی

پیدایش حوزه مهندسی اجتماعی را می‌توان، از داستان‌ها و وقایع تاریخی فهمید. وقایعی مثل جنگ تروآ در یونان که یونانیان به مدت ۱۰ سال پشت دروازه های شهر تروجان در جنگ متوقف مانده بودند. و نمیتوانستند پیشروی کنند، جنگجویی با نام اودیسه، نقشه ای ریخت که سربازان یک اسب چوبی غول پیکری بسازند و درون آن مخفی شوند و با فریب دادن تروجان ها با آن اسب چوبی وارد شهر شوند. به دلیل نقشه مبتنی بر مهندسی اجتماعی اودیسه، یونانی‌ها در جنگی که فکر میکردند شکست خوردند، پیروز شدند. همچنین در دهه ۱۹۲۰ میلادی دولت شوروی کمپینی را راه انداخت، که در آن رفتار ها و آرزو های شهروندان شوروی تغییر میکرد، و قوانین و چهارچوب های قدیمی امپراتوری روسیه جایش را به فرهنگ جدید شوروی، و توسعه انسان جدید شوروی داد و کمیسر ها را به ماموران مهندسی اجتماعی، تبدیل کرد.

بعدها در دهه ۹۰ میلادی کوین میتنیک (Kevin Mitnick) لقب پدر مهندسی اجتماعی گرفت. چون او، بعد از سالها تلاش و بکارگیری حقه ها و ترفند هایی برای بدست آوردن اطلاعات، و دستکاری روانی و فریب دادن افراد، موفق شد مهندسی اجتماعی را در دنیای امنیت سایبری به شهرت برساند. او با اینکه فقط ۱۳ سال داشت می‌توانست، از سیستم حمل و نقل اتوبوس های لوس آنجلس با حقه های مهندسی اجتماعی به طور رایگان استفاده کند. میتنیک بعدها موفق شد که به شبکه‌های شرکت دیجیتال اکوپیمنت و شرکت مخابراتی پسیفیک بلز دسترسی غیرمجاز پیدا کند.

و همچنین یک‌چرخه مرحله‌ای مهندسی اجتماعی را طراحی کرد که به چرخه Kevin Mitnick معروف است.
این مراحل شامل:۱-انجام تحقیقات۲-اعتمادسازی۳-بهره برداری از روابط برای کسب اطلاعات ازطریق مکالمات، رفتارها و یا فناوری۴-استفاده از اطلاعات جمع آوری شده برای مقاصد بدخواهانه است.[6,7,8]

۷. انواع تکنیک ها و حملات مهندسی اجتماعی

مهندسان اجتماعی از تکنیک‌ها و حملات مختلفی برای پیشبرد اهدافشان استفاده می‌کنند، و بسته به شرایط و موقعیت‌ها به یک‌شکل خاص عمل می‌کنند. انواع حملات و تکنیک‌ها به شرح زیر است:

بهانه سازی Pretexting

مهاجم و هکر با ساختن یک نقشه و یک سناریوی ساختگی و از قبل طراحی شده سعی می‌کند که قربانی را فریب دهد و به اطلاعاتش دسترسی پیدا کند یا او را مجبور به انجام کاری کند. مثل تغییر هویت خود در قامت یک پلیس یا کارمند پشتیبانی یا مأمور آمارگیری.

طعمه گذاری Baiting

مهاجم با دادن یک پیشنهاد وسوسه‌انگیز و جذاب، مثل وای‌فای رایگان یا ارائهٔ یک برنامهٔ پولی به‌صورت رایگان، قربانی را به دام می‌اندازد و اقدام به سرقت اطلاعات او می‌کند یا از او باج می‌گیرد.

دنباله روی فیزیکی Tailgating

هکر یا مهاجم، با دنبال‌کردن افراد مجاز، سعی می‌کند که وارد محیط‌های غیرمجاز شود. او با فریب یا تهدید کارکنان یک سازمان یا مجموعه اقدام به نفوذ در آن مجموعه یا سازمان می‌کند.

فریب یا نظرسنجی Quizzing

مهاجم با پوشش یک دانشجو یا محقق، با ارائه‌دادن یک نظرسنجی یا پرسش‌نامه، اطلاعات مهم را از کاربر دریافت می‌کند.

نرم افزار ترساننده Scareware

هکر یا نفوذگر، افراد را به خرید یک آنتی‌ویروس جعلی که خودشان طراحی کردند، ترغیب می‌کند. به ادعای اینکه سیستم آنها آلوده است و قربانی پس از نصب آن نرم‌افزار، سیستمش آلوده شده و در اختیار هکر، قرار می‌گیرد.

فیشینگ Phishing

در این نوع حملات، نفوذگر، با ارسال پیام‌ها یا ایمیل‌هایی با ارائهٔ لینک‌ها و بدافزارهای مخرب تحت عنوان سازمان یا ارگان‌های معروف و دولتی، اقدام به آلوده‌کردن قربانی و سرقت اطلاعات افراد می‌کند که خود این نوع از حملات، دارای زیرمجموعه‌هایی به شرح زیر است:

فیشینگ ایمیلی Email Phishing

نفوذگر، اقدام به ارسال ایمیل‌هایی جعلی می‌کند که انگار از سوی مراجع قانونی یا سازمان‌های دولتی است و افراد را وادار به افشای اطلاعات می‌کند، یا با قراردادن لینک مخرب یا بدافزار، سیستم قربانی را آلوده می‌کند.

فیشینگ هدفمند Spear Phishing

این نوع فیشینگ، مشابه فیشینگ ایمیلی است، با این تفاوت که ایمیل برای یک شخص یا سازمان مشخص و از پیش تعیین شده شخصی‌سازی و طراحی شده است.

فیشینگ پیامکی Smishing

مهاجم با ارسال پیامک‌های جعلی برای فرد قربانی، اقدام به آلوده‌کردن سیستم فرد و ترغیب او به کلیک بر روی لینک‌های مخرب می‌کند، و سعی می‌کند که به اطلاعات فرد دسترسی پیدا کند.

فیشینگ نهنگی Whaling

این نوع فیشینگ، نمونه‌ای از فیشینگ هدفمند است، اما با این تفاوت که برای افراد با جایگاه بالا، مثل مدیرعامل یک شرکت، طراحی می‌شود. هکرها و مهندسان اجتماعی معمولاً در این نوع فیشینگ، افراد را به افشای اطلاعات سازمانی یا انجام تراکنش‌های مالی بزرگ ترغیب می‌کنند.

فارمینگ Pharming

هکر، فرد قربانی را برای پرداخت و یا واردکردن اطلاعات دیگر، به یک وب‌سایت جعلی هدایت می‌کند و فرد با واردکردن اطلاعات خود در آن سایت، اطلاعات وارد شده را در اختیار آن هکر و نفوذگر می‌گذارد. مثل صفحه‌های وب جعلی بانک‌ها، ارگان‌های دولتی و....

فیشینگ صوتی Vishing

مهاجم در این روش، با برقراری تماس تلفنی در قالب یک مجری تلویزیونی به بهانهٔ برنده‌شدن فرد در یک قرعه‌کشی یا کارمند یک بانک یا ارگان دولتی، سعی می‌کند که قربانی را فریب داده و اطلاعات او را به سرقت ببرد.

فیشینگ در شبکه‌های اجتماعی Social-Media Phishing

در این روش هکر یا نفوذگر، از فضای مجازی و اپلیکیشن‌هایی مثل: توییتر، واتس‌اپ، تلگرام، اینستاگرام و... برای فریب‌دادن افراد و جمع‌کردن اطلاعات استفاده می‌کند که امروزه با گسترده‌تر شدن این فضا و بیشترشدن کاربران، استفاده از این روش توسط مهندسان اجتماعی بیشتر می‌شود.[9]

۸. هوش مصنوعی چیست؟

هوش مصنوعی، تکنولوژی است که به انسان‌ها کمک می‌کند که کارهای روزمره خود را سریع‌تر و راحت‌تر انجام دهند. هوش مصنوعی، قدرت یادگیری، خلاقیت، حل مسئله، تصمیم‌گیری و همچنین خودمختار بودن انسان را شبیه‌سازی می‌کند و روزبه‌روز نیز پیشرفته‌تر می‌شود و خود را ارتقا می‌دهد.[10] دستگاه ها و ربات های دارای فناوری هوش مصنوعی می‌توانند، محیط دور خود را اسکن کنند، اشیا را ببینند و تشخیص دهند. می‌توانند زبان انسان هارا درک کنند و آن را تشخیص دهند و از تجربیات آنها استفاده کنند. می‌توانند مستقل باشند و بدون دخالت انسان عمل کنند(به عنوان مثال: خودرو های خودران).همچنین می‌توانند در انجام امور، به متخصصان کمک کنند و توصیه های لازم را به آن ها بدهند. در سال ۲۰۲۴ بیشتر محققان بر روی فناوری جدیدی به اسم هوش مصنوعی مولد(gen ai)

تحقیق می‌کنند. هوش مصنوعی مولد می‌تواند محتوای جدیدی در قالب متن، تصویر، ویدئو و سایر محتواهای دیگر را تولید کند و آیندهٔ مهندسی اجتماعی را نیز تحت‌تأثیر خود قرار دهد. ما برای فهمیدن و شناخت کامل هوش مصنوعی مولد ابتدا باید تکنولوژی‌هایی را که ابزارهای هوش مصنوعی مولد بر اساس آن‌ها ساخته شده‌اند را یاد بگیریم و درک کنیم که آن تکنولوژی‌ها و فناوری‌ها عبارت‌اند از: یادگیری ماشین (ML) و یادگیری عمیق. [10]

۹.تاریخچه هوش مصنوعی

تاریخچه هوش مصنوعی به یونان باستان با ایده ماشینی که فکر می‌کند برمی‌گردد. ولی از زمان به‌وجودآمدن تکنولوژی و محاسبات الکترونیکی و کامپیوترها، اتفاقات و پیشرفت‌های مهم در تکامل هوش مصنوعی به این شرح است. [10]

در سال ۱۹۵۰ آلن تورینگ، کسی که به خاطر شکستن دستگاه انیگما آلمانی ها در زمان جنگ جهانی دوم به وسیله دستگاهی که ساخت مشهور است، کتابی با اسم (ماشین آلات محاسباتی و هوش) را منتشر می‌کند و این سوال را می‌پرسد که آیا ماشین ها می‌توانند فکر کنند؟

در سال ۱۹۵۶ جان مک کارتی، اصطلاح (هوش مصنوعی) را برای اولین بار در اولین کنفرانس هوش مصنوعی در کالج دارتموث به وجود آورد و در همان سال آلن نیوئل، جی. سی. شاو و هربرت سایمون اولین برنامه هوش مصنوعی را با نام نظریه پرداز منطقی، پدید آوردند.

به این ترتیب، طی سال‌ها و دهه‌ها هوش مصنوعی پیشرفته‌تر و پیشرفته‌تر می‌شد. کامپیوترهای مبتنی بر شبکه‌های عصبی پدید آمدند، و محققان فعال در این حوزه، روزبه‌روز به چیزهای جدیدی دست پیدا می‌کردند و هوش مصنوعی را گسترش می‌دادند. تا به امروز و در سال ۲۰۲۲ که مدل‌های زبانی بزرگ یا LMM ها مانند Chat GPT ساخت شرکت Open Ai بوجود آمدند و گسترش پیدا کردند، و انقلابی در فناوری هوش مصنوعی مولد ایجاد کردند. و تا کنون که سال ۲۰۲۵ است، در حال ارتقا پیدا کردن و پیشرفته تر شدن و پیچیده تر شدن هستند. [10]

۱۰. مهندسی اجتماعی مبتنی بر هوش مصنوعی

ظهور هوش مصنوعی و ابزارهای پیشرفته متن‌باز هوش مصنوعی مولد، در زندگی انسان‌ها به‌ویژه در مباحث امنیت سایبری مشخص است و این می‌تواند زندگی انسان‌ها را تحت‌تأثیر قرار دهد و به هکرها و مهندسان اجتماعی کمک کند که با استفاده از این قابلیت‌ها، حملات مهندسی اجتماعی پیچیده‌تری توسعه دهند. هکرها با استفاده از این ابزارها می‌توانند حملات مهندسی اجتماعی خود را خودکارسازی کنند، می‌توانند متن‌های شخصی‌سازی‌شده‌تر و تأثیرگذارتری تولید کنند، محتوای ویدئویی فیک و تصاویر جعلی تولید کنند و صدای اشخاص معروف را جعل کنند و چیزهای دیگر که همهٔ اینها با استفاده از ابزارها و مدل‌های زبانی بزرگی مانند GPT-4 برای شرکت Open Ai و دیپ‌فیک‌ها امکان‌پذیر شده است.

روش‌های سنتی مهندسی اجتماعی، به‌شدت به دخالت‌های انسانی متکی بودند و دارای نواقص و خطاهایی بودند. اما اکنون و با نقش هوش مصنوعی، هکرها می‌توانند این حملات مهندسی اجتماعی را بادقت و مقیاس بالاتری انجام دهند و این حملات را شخصی‌سازی‌شده‌تر و به‌صورت خودکار توسط هوش مصنوعی انجام دهند و احساسات، اعتماد و درک افراد را به بازی بگیرند و تهدیدات سایبری را افزایش دهند. [9,11,12]

برخی از قابلیت های هوش مصنوعی در زمینه مهندسی اجتماعی

با پیشرفت فناوری هوش مصنوعی، کارهای انسان راحت‌تر و سریع‌تر انجام می‌شود و همچنین در به‌وجودآمدن برخی از هزینه‌ها صرفه‌جویی می‌شود. اما بااین‌حال نقش هوش مصنوعی در مهندسی اجتماعی و فریب سایبری نیز روزبه‌روز افزایش پیدا می‌کند. حملات مهندسی اجتماعی مبتنی بر هوش مصنوعی به سه بخش تقسیم می‌شود:

۱-تولید محتوای واقعگرایانه

۲-هدفگیری پیشرفته و شخصی سازی

۳-زیر ساخت حمله خودکار. [9]

هوش مصنوعی هرچقدر برای انسان‌ها مفید باشد، به همان اندازه آثار مخربی به همراه دارد که نمونه‌اش کمک به مهندسان اجتماعی است که بتوانند حملات دقیق‌تر و حساب‌شده‌تری طراحی کنند. در ادامه با برخی از قابلیت‌های هوش مصنوعی در زمینه مهندسی اجتماعی آشنا می‌شویم:

هوش مصنوعی مولد

هوش مصنوعی مولد بر اساس الگوریتم‌هایی که به‌وسیلهٔ آن‌ها تولید شده است، می‌تواند محتواهای بسیار واقعی و متقاعدکننده‌ای مانند: متن، ویدئو، تصویر و... برای حملات مهندسی اجتماعی تولید کند. این محتواها هم نیز به‌وسیلهٔ الگوهای داده‌ای که آموخته است و همچنین به‌صورت روزانه می‌آموزد، تولید می‌کند.

پردازش زبان طبیعی(NLP)

همان‌طور که از نامش پیداست، برای درک و تولید رفتار و حالات و زبان انسانی بکار می‌رود. در حملات مهندسی اجتماعی نیز، می‌تواند ایمیل‌ها و پیام‌های مختلف را تجزیه‌وتحلیل کند، پیام‌ها و ایمیل‌های متقاعدکننده تولید کند و حتی می‌تواند، رفتار و سبک نوشتاری قربانی را تقلید کند.

تقلید و جعل صوتی و چهره

با این قابلیت و تکنیک، هکرها از تکنیک یادگیری عمیق و دیپ‌فیک‌ها برای جعل صدا یا چهره اشخاص مختلف برای فریب فرد قربانی از طریق تماس‌های تلفنی و ویدئو های جعلی در فضای سایبری استفاده می‌کنند.

تحلیل رفتار

هوش مصنوعی قادر است تا الگوهای رفتاری و سبک نوشتاری افراد را در فضای سایبری، تحلیل کند و به واسطه آن اطلاعاتی درباره عادات، علایق، نقاط ضعف و رفتار افراد به دست آورد و از این اطلاعات برای حملات مهندسی اجتماعی حساب‌شده‌تر استفاده کند.

تشخیص احساسات

مهندسان اجتماعی و هکرها باقابلیت‌های هوش مصنوعی می‌توانند، احساسات افراد را در شبکه‌های اجتماعی مثلاً پست‌ها و گروه‌ها، یا ایمیل‌ها استخراج کنند و آن را تحلیل کنند. این فرایند به مهندسان اجتماعی کمک می‌کند که حملات خود را زمان‌بندی و تنظیم محتوای مؤثرتری داشته‌باشند.

جست و جوی خودکار اطلاعات

نفوذگران، با استفاده ربات‌های مبتنی بر هوش مصنوعی می‌توانند، داده‌ها و اطلاعات زیادی را از شبکه‌های اجتماعی، پایگاه‌های داده‌ای اینترنتی و... دریافت کنند و بر اساس آن‌ها حملات خود را طراحی کنند.

چت بات های هوشمند

هکرها با استفاده از قابلیت‌های هوش مصنوعی، چت‌بات‌های هوشمندی طراحی می‌کنند که قادر است مکالمات طبیعی و متقاعدکننده‌ای را با افراد قربانی برقرار کند و اطلاعات حساس و شخصی آن‌ها را دریافت نماید.

حملات فیشینگ مبتنی بر هوش مصنوعی

مهندسان اجتماعی با استفاده از هوش مصنوعی، حملات فیشینگ واقعی‌تر و مؤثرتری را برای افراد قربانی طراحی می‌کنند. به‌گونه‌ای که متقاعدکننده باشد و جوری واقعی باشد که قربانی را ترغیب کند که روی لینک یا فایل‌های آلوده کلیک کند.

تحلیل هوش مصنوعی

منظور از تحلیل هوش مصنوعی، کاربرد تکنیک‌های یادگیری ماشین و تحلیل داده‌ها برای پردازش و تفسیر داده‌ها است که در حملات مهندسی اجتماعی به هکرها و نفوذگران کمک می‌کند که اهدافشان را پیدا کنند و رفتار قربانی‌هایشان را تشخیص دهند، و بتوانند نقاط ضعف و مواردی را که باعث آسیب‌پذیری قربانی می‌شود را ارزیابی کرده و شناسایی کنند.

استخراج اطلاعات توسط هوش مصنوعی

استخراج اطلاعات توسط هوش مصنوعی و ابزارهای خودکار که بیشتر بر پایه یادگیری ماشین است، هکرها را قادر می‌سازد که در حملات مهندسی اجتماعی، از منابع آنلاین و پروفایل‌های شبکه‌های اجتماعی و پایگاه‌داده‌های عمومی اطلاعات مهم و موردنیازشان را استخراج کنند و پروفایل‌های دقیقی از قربانی‌هایشان ایجاد کنند.

اتوماسیون یا خودکارسازی هوش مصنوعی

مهندسان اجتماعی با این قابلیت هوش مصنوعی، حملات خود را خودکارسازی می‌کنند. به‌گونه‌ای که به‌صورت کاملاً خودکار، حملات خود را به قربانی آغاز می‌کنند و ارتباط خود را با آن‌ها حفظ می‌کنند و تضمین می‌کنند و همچنین احتمال شناسایی شدن توسط قربانی را کاهش می‌دهند.

ارزیابی هوش مصنوعی

هوش مصنوعی با استفاده از الگوریتم‌ها و فناوری‌های خود، به مهندسان اجتماعی کمک می‌کند که حملات خودشان را ارزیابی و تحلیل بکنند. ارزیابی حملات، توسط هوش مصنوعی باعث می‌شود که حساب‌های به خطر افتاده یا نشت داده‌ها، پایش شود و اثربخشی حملات مورد بررسی قرار گیرد و مهندسان اجتماعی بتوانند از این طریق، حملات خود را بهبود بخشند و بهتر کنند. [9]

پرامپت اینجکشن

پرامپت اینجکشن (prompt injection) نوعی حمله سایبری است که هکرها به مدل‌های زبانی بزرگ نظیر Chat GPT می‌کنند. آن‌ها با این تکنیک دستیارهای هوش مصنوعی را وادار می‌کنند که اطلاعاتی را به آنها بدهد که نباید داده شود. به‌عنوان یک مثال واقعی، کوین لیو، دانشجوی دانشگاه استنفورد، با واردکردن این دستور و استفاده از تکنیک پرامپت اینجکشن، بینگ چت مایکروسافت را وادار به افشای برنامه‌نویسی خود کرد. مهندسان اجتماعی با این تکنیک و با سو استفاده از دستیارهای هوش مصنوعی می‌توانند به اهداف خود برسند و حملات مهندسی اجتماعی خود را با استفاده از هوش مصنوعی طراحی کنند. [13]

ایجنت یا عامل های هوشمند

عامل‌های هوشمند، نوعی عامل هستند که می‌توانند، وظایف خاص و قابل‌پیش‌بینی و تکراری را انجام دهند و توان یادگیری نیز داشته باشند. هکرها و مهندسان اجتماعی با استفاده از عامل‌های هوشمند در فضای سایبری می‌توانند حملات مهندسی اجتماعی خود را خودکارسازی کنند. [14]

۱۱. ابزار های مهندسی اجتماعی مبتنی بر هوش مصنوعی

مهندسان اجتماعی و هکرها از گذشته تا کنون، تکنیک‌ها و روش‌های مختلفی را برای نفوذ و همچنین فریب افراد و قربانی‌هایشان به کار می‌برند. با ظهور هوش مصنوعی و نقش آن در فضای سایبری و مهندسی اجتماعی، هکرها نیز می‌توانند حملات مهندسی اجتماعی قوی‌تر و حساب‌شده‌تری طراحی کنند. این می‌تواند تهدید بزرگی برای افراد و فضای سایبری باشد. امروزه هکرها و مهندسان اجتماعی، برای طراحی حملات خود از ابزارهای مهندسی اجتماعی مبتنی بر هوش مصنوعی مختلفی استفاده می‌کنند که در ادامه با برخی از آن‌ها آشنا می‌شویم.

ابزار n8n

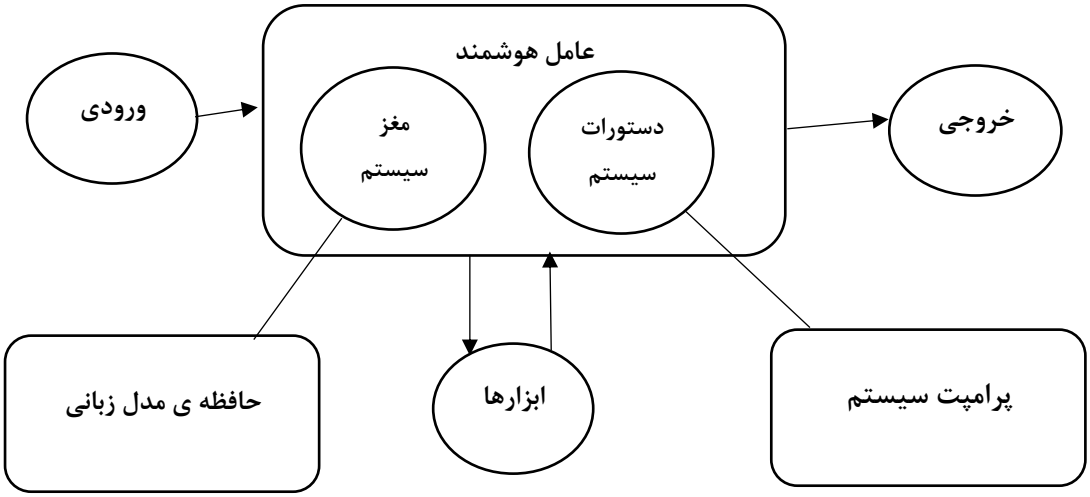
یک ابزار و پلتفرم متن‌باز است که در سال ۲۰۱۹ توسط یان اوبرهاوزر در برلین ساخته شد. این ابزار به افراد کمک می‌کند که بدون دانش کد نویسی برای خود، عامل های هوشمند طراحی کنند. که به واسطه آن بتوانند کار ها و وظایف تکراری خود را خودکارسازی کنند.

این ابزار متن‌باز است و به لطف متن‌باز بودن، خود کاربران می‌توانند بر اساس نیازهای خودشان آن را شخصی‌سازی کنند. یکی دیگر از ویژگی‌های این ابزار پشتیبانی از بیش از ۳۵۰ برنامه مختلف است که به کاربران امکان می‌دهد که از سرویس‌هایی نظیر Slack,Google sheets,Trello و کلی سرویس دیگر استفاده کنند و آن‌ها را بدون نیاز به کدنویسی به یکدیگر وصل کنند.

ابزار n8n با استفاده از نودها یا گره‌ها کار می‌کند، به این صورت که می‌تواند با استفاده از نودها گردش کارهایی را ایجاد کند که چندین سایت، پایگاه‌داده، سرویس ابری، ابزار و یا برنامه با هم ترکیب شوند. هر نود می‌تواند کاری؛

مانند ارسال فایل یا ایمیل، خواندن پیام‌ها و یا ویرایش یک فایل را انجام دهد که این فرایند می‌تواند به‌صورت مجزا یا با هم انجام شود. [15]
برای نصب و استفاده از این ابزار می‌توان به سایتش مراجعه کرد یا از طریق Docker ، npm آن را نصب کرد یا مستقیماً روی سرور نصب و راه‌اندازی کرد. [15]

هکرها و مهندسان اجتماعی، با این ابزار می‌توانند، عامل‌های هوشمندی طراحی کنند (بدون هیچ‌گونه دانش برنامه‌نویسی) که خودش به‌صورت خودکار با استفاده از هوش مصنوعی (انتخاب دستیار هوش مصنوعی یا ابزارهای آن به انتخاب خود هکر است) حملات فیشینگ را انجام دهند.
به‌عنوان‌مثال، هکرها با استفاده از الگوهایی، عامل هوشمندی طراحی می‌کنند به‌گونه‌ای که هکر پرامپت خودش را مبنی بر حملات فیشینگ در یک چت‌بات به‌عنوان ورودی بنویسد و عامل با استفاده از آن پرامپت، به‌صورت خودکار حملات فیشینگ را آغاز کند. شکل ۱



شکل ۱ : نمای یک عامل هوشمند برای ساخت آن توسط ابزار n8n

ابزار FraudGPT

یکی دیگر از ابزارهای هوش مصنوعی است که بدون داشتن محدودیت است و به مهندسان اجتماعی و هکرها کمک می‌کند که ایمیل‌های فیشینگ و وب‌سایت‌های بسیار واقعی و متقاعدکننده‌ای را طراحی و تولید کنند. این ابزار و دستیار هوش مصنوعی بدون هیچ‌گونه محدودیتی است و هر درخواستی که از او شود را پاسخ می‌دهد که می‌تواند باعث شود که افراد کم‌تجربه نیز دست به حملات مهندسی اجتماعی بزنند. این ابزار توسط یک تیم تحقیقاتی به اسم Netenrich در ژوئیه سال ۲۰۲۳ در کانال‌های تلگرامی دارک‌وب کشف شد. [16]
هکرها برای استفاده از ابزار FraudGPT با پرداخت اشتراک ماهانه ۲۰۰ دلار و یا اشتراک سالانه ۱۷۰۰ دلار می‌توانند به مجموعه ای عظیم از قابلیت های آن مانند: ایجاد ایمیل های فیشینگ و مهندسی اجتماعی، ساخت بد افزار ها، ساخت اکسپلویت ها، کشف آسیب پذیری ها و ارائه تکنیک های هک دسترسی داشته باشند.[17]

ابزار WormGPT

همانند ابزار FraudGPT است که بر پایه مدل زبان GPTJ است که در سال ۲۰۲۱ طراحی شد. این ابزار به طور خاص برای اهداف شرورانه ساخته شده و به هکرها و مهندسان اجتماعی کمک می‌کند که حملات خود را توسعه دهند و ایمیل های BEC تولید کنند.[18]

ابزار OSINT

OSINT مخفف عبارت Open Source Intelligence است که به معنی اطلاعات یا هوش منبع‌باز است. مهندسان اجتماعی و هکرها با استفاده از این ابزار می‌توانند از طریق اینترنت، شبکه‌های اجتماعی، وب‌سایت‌ها و پایگاه‌های داده‌ای عمومی که برای عموم آزاد است، اطلاعات موردنیازشان را برای پیداکردن قربانی‌شان و توسعه حملات مهندسی اجتماعی استخراج کنند. همچنین این ابزار می‌تواند برای اهداف مفید هم استفاده شود به صورتی که می‌تواند به سازمان‌ها و افراد کمک کند که اطلاعاتی را که ممکن است از نظر امنیتی به ضررشان باشد را پیدا کنند و جلوی حملات مهندسی اجتماعی آینده را بگیرند. [19]

دیپ فیک ها یا جعل عمیق

تکنولوژی جعل عمیق یا دیپ‌فیک می‌تواند بسیار خطرناک باشد. زیرا هکرها و مهندسان اجتماعی می‌توانند با استفاده از ابزارهای دیپ‌فیک حملات واقعی‌تری را ترتیب دهند. می‌توانند صدا یا چهره افراد را جعل کنند و به‌وسیله آنها دست به اقدامات خرابکارانه یا فریب قربانی‌هایشان بزنند یا از آن‌ها سو استفاده کنند. ابزارهایی وجود دارد که مهندسان اجتماعی می‌توانند از آن‌ها برای اهداف خود استفاده کنند مانند: هوش مصنوعی شرکت Bland Ai که می‌تواند صدای افراد را باهوش مصنوعی جعل کند و تماس‌های تلفنی واقع‌گرایانه ایجاد کند.
یا ابزار DeepFaceLab که به افراد یا هکرها این امکان را می‌دهد که چهره هارا در ویدئو ها عوض کنند. [20]

۱۲. راهکارها و ابزار های دفاعی برای مقابله با مهندسی اجتماعی مبتنی بر هوش مصنوعی

با پیشرفته‌تر شدن فناوری هوش مصنوعی و گسترده‌تر شدن فضای سایبری، مجرمان سایبری و مهندسان اجتماعی نیز روزبه‌روز بیشتر می‌شوند و حملات بیشتر و گسترده‌تری را انجام می‌دهند. ازاین‌رو افراد باید اقدامات دفاعی را در برابر این حملات در نظر بگیرند که در ادامه به آن‌ها می‌پردازیم.

آموزش عمومی

با برگزارکردن دوره‌ها و برنامه‌های آموزشی گسترده توسط سازمان‌ها یا ارگان‌ها دررابطه با مهندسی اجتماعی و آشناکردن افراد با هوش مصنوعی و مهندسی اجتماعی، تا حد زیادی می‌توان جلوی این حملات را گرفت. افراد با آگاه شدن دراین‌رابطه متوجه می‌شوند که در این شرایط خاص چه اقداماتی را باید انجام دهند.

محافظت کردن از اطلاعات شخصی خود

ما می‌توانیم با رعایت‌کردن نکات امنیتی، به‌عنوان‌مثال ندادن اطلاعات شخصی‌مان به افراد غریبه یا به اشتراک نگذاشتن اطلاعات و علایقمان در فضای مجازی مثل اینستاگرام و تلگرام و باز نکردن ایمیل‌ها و پیام‌های مشکوک، تا حد زیادی از حملات مهندسی اجتماعی در امان بمانیم.

۱۲-۳. ابزار Intel FakeCatcher

این ابزار می‌تواند ویدئو هایی را که توسط دیپ‌فیک‌ها ساخته شده است و جعلی است را تشخیص دهد. ساخت شرکت اینتل است و به گفته شرکت اینتل قادر است که تا ۹۶ درصد ویدیو های جعلی را شناسایی کند و این کار را با فناوری های خاص و بررسی نشانه های طبیعی موجود در ویدیو ها، نظیر گردش خون انجام می‌دهد.
این فناوری و ابزار به افراد و سازمان‌ها کمک می‌کند که ویدئو های جعلی ساخته شده توسط دیپ‌فیک هارا شناسایی کند. [21]

ابزار CrowdStrike Falcon AI

سرویس هوش مصنوعی CrowdStrike Falcon AI یک پلتفرم و ابزار مبتنی بر هوش مصنوعی است که تهدیدات و حملات فضای سایبری و دیجیتال را شناسایی کرده و با آن‌ها مقابله می‌کند. این سامانه و ابزار توسط CrowdStrike ساخته شده و به دلیل استفاده از فناوری‌های ابری و تحلیل پیشرفته در زمان واقعی موردتوجه شرکت‌ها و سازمان‌های بزرگ قرار گرفته است.
این ابزار امکاناتی مثل، تشخیص تهدیدات، ارائه اقدامات مقابله با حملات سایبری و مهندسی اجتماعی و تحلیل رفتارهای مشکوک را دارد و از الگوریتم‌های یادگیری ماشین و تحلیل رفتاری استفاده می‌کند. استفاده از این ابزار و پلتفرم به افراد و سازمان‌ها این امکان را می‌دهد که تهدیدات موجود در فضای سایبری را شناسایی کنند و بتوانند با آن‌ها مقابله کنند و زمان واکنش خودشان را به حملات سایبری و مهندسی اجتماعی کاهش دهند. افراد و سازمان‌ها می‌توانند، پس از ارزیابی نسخه آزمایشی این ابزار و پلتفرم با پرداخت اشتراک‌های سالیانه و قراردادها، به این ابزار و پلتفرم دسترسی داشته باشند. [22]

ابزار virustotal

این ابزار به افراد و سازمان‌ها کمک می‌کند که با آپلود لینک‌ها و برنامه‌های ناشناخته در این ابزار، خطرات و تهدیدات آن را تشخیص دهند. افراد با این ابزار می‌توانند وب‌سایت‌های جعلی و بدافزارها را شناسایی کنند و جلوی حملات سایبری و مهندسی اجتماعی را تا حد زیادی بگیرند.

استفاده از دستیار های هوش مصنوعی

هوش مصنوعی همان‌طور که با پیشرفت خود تهدیداتی را نیز به وجود می‌آورد، همچنین می‌تواند به افراد و سازمان‌ها کمک کند که حملات مهندسی اجتماعی و سایبری را شناسایی کنند. دستیارهای هوش مصنوعی با ارائه‌کردن اقدامات امنیتی و ارائه آموزش‌های لازم و به روز می‌تواند افراد و سازمان هارا برای حملات مهندسی اجتماعی و سایبری آماده کند و باعث شود که این حملات کاهش پیدا کند.

۱۳. نتیجه گیری

مهندسی اجتماعی، به‌عنوان هنر فریب ذهن انسان نشان می‌دهد که هکرها فقط به سیستم‌های فنی نفوذ نمی‌کنند؛ بلکه با نفوذ کردن به ذهن افراد یک سازمان و فریب‌دادن آن‌ها و سو استفاده‌کردن از آنها می‌توانند به اهداف خود برسند.

با پیشرفت روزافزون هوش مصنوعی و پررنگ‌تر شدن آن در زندگی ما، با اینکه زندگی ما را راحت‌تر کرده و برای ما مفید است؛ اما به واسطه آن تهدیدات فضای سایبری نیز بیشتر می‌شود. زیرا همیشه افرادی سودجو و مخرب هستند که از هوش مصنوعی برای اهداف مخرب و مجرمانه خود استفاده می‌کنند. ازاین‌رو باید آماده باشیم و راهکارهای دفاعی و آموزش‌های امنیتی لازم را جدی بگیریم و از آن‌ها استفاده بکنیم. ما در این مقاله، با مهندسی اجتماعی و تکنیک‌های آن آشنا شدیم و نقش هوش مصنوعی را در مهندسی اجتماعی بررسی کردیم و راهکارهایی را برای دفاع در برابر این حملات پیشنهاد دادیم. با پیشرفت هوش مصنوعی و ابزارهای مبتنی بر آن لازم است که تحقیقات بیشتری دراین‌خصوص انجام شود که بتوانیم از رخ‌دادن حملات مهندسی اجتماعی مبتنی بر هوش مصنوعی پیشرفته‌تری جلوگیری کنیم و از تهدیدات جدیدتر موجود در فضای سایبری پیشگیری کنیم. حملات مهندسی اجتماعی، می‌تواند برای هر شخصی و با هر شغل و جایگاهی رخ دهد، ازاین‌رو لازم است که تمام افراد با این موضوع آشنایی لازم را داشته باشند و راهکارهای دفاعی در برابر این نوع حملات را بدانند.

ما در این مقاله سعی کردیم که با معرفی تکنیک‌های مهندسی اجتماعی و آشناکردن افراد با ابزارهای مهندسی اجتماعی مبتنی بر هوش مصنوعی، افراد را آگاه‌تر کنیم. افراد و سازمان‌ها با دانستن و آشناشدن با این نوع تکنیک‌ها و ابزارها می‌توانند که در برابر حملات مهندسی اجتماعی آماده‌تر شوند و با آگاهی بیشتری با این نوع حملات مواجهه شوند. حملات مهندسی اجتماعی می‌تواند برای هر فردی در جامعه رخ دهد. مانند: معلمان، دانشجویان، مدیران و کارکنان سازمان‌ها، حتی کودکان و هر شخص دیگری که در این جامعه حضور دارد. همین موضوع باعث مهم بودن این مسئله می‌شود که باید بیشتر به آن پرداخته شود و مورد تحقیق و بررسی بیشتری قرار بگیرد و راهکارهای دفاعی نیز در رابطه با آن پیشنهاد شود.

مراجع

1.Cognisys. (202۴, August 22). Exploring the psychology of social engineering attacks. Cognisys. https://cognisys.co.uk/blog/social-engineering-attacks/

2. weforum. (25 oct 2024). AI could empower and proliferate social engineering cyberattacks. https://www.weforum.org/stories/2024/10/ai-agents-in-cybersecurity-the-augmented-risks-we-all-need-to-know-about/

*3.*Dr. Ozkaya*. E. (April 2018). Learn Social Engineering. UK. Packt Publishng Ltd.*

۴.صفدری. مریم. (۱۴۰۲). روانشناسی تاریک چیست؟ هرآنچه باید بدانید. https://www.zoomit.ir/health-medical/410144-dark-psychology-and-manipulation/

۵.sophosfirewall . (۱۴۰۲). مهندسی اجتماعی، تکنیک‌های مهندسی اجتماعی چیست؟. https://sophosfirewall.ir/social-engineering/

۶.شیخی.مرجان.(۱۴۰۰). مهندسی اجتماعی چیست ؛ وقتی به جای سیستم‌ها، انسان‌ها هک می‌شوند!. https://www.zoomit.ir/security/374861-social-engineering-complete-guide/

7. Kort. Michael G. (17 April 2019) [1985]. "Into the Fire: The Civil War". The Soviet Colossus: History and Aftermath (8 ed.). New York: Routledge (published 2019).

8. Francois Mouton, Mercia M. Malan, Louise Leenen, H.S. Venter; " Social Engineering Attack Framework " , Defence Peace Safety & Security, Council for Industrial and Scientific Research Pretoria, South Africa, 9, 2014.

9. Schmitt, M, & Flechais, I. (2023). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. https://arxiv.org/abs/2310.13715

10. Stryker, C, & Kavlakoglu, E. (9 August 2024). What is artificial intelligence (AI)?

https://www.ibm.com/think/topics/artificial-intelligence

11.S. Neupane, I.A. Fernandez, S. Mittal, S. Rahimi, Impacts and Risk of Generative AI Technology on Cyber Defense, (2023). http://arxiv.org/abs/2306.13033.

۱۲. afratec.ir (۲۲ مهر ۱۴۰۲). نقش هوش مصنوعی در حملات مهندسی اجتماعی

https://afratec.ir/ai-roles-in-cyber-attacks/

۱۳. Kosinski, M, & Forrest, A. (26 March 2024). What is a prompt injection attack?

https://www.ibm.com/think/topics/prompt-injection

۱۴.faradars. (۱ اردیبهشت ۱۴۰۴). عامل هوشمند چیست؟ – مفاهیم هوش مصنوعی به زبان ساده

https://blog.faradars.org/عامل-هوشمند-چیست/

۱۵.شریفی. نسرین. (۲۵ اسفند ۱۴۰۳). n8nچیست؟ مقدمه‌ای بر یک ابزار اتوماسیون گردش کار

https://liara.ir/blog/n8n-%DA%86%DB%8C%D8%B3%D8%AA/

16. E. K. Sing. (Sep. 22, 2023). "With generative AI, businesses need to rewrite the phishing rulebook," 2023. https://identityweek.net/with-generative-ai-businesses-need-to-rewrite-the-phishing-rulebook/

17. L. Columbus. (August 14, 2023). "How FraudGPT presages the future of weaponized AI," 2023. https://venturebeat.com/security/how-fraudgpt-presages-the-future-of-weaponized-ai/

18. D. RILEY. (Sep. 26, 2023). "Cybercriminals are using custom 'WormGPT' for business email compromise attacks," 2023. https://siliconangle.com/2023/07/13/slashnext-warns-cybercriminals-using-custom-wormgpt-business-email-compromise-attacks/

19. Nobili. M. (1 Sep 2023). Review OSINT tool for social engineering. https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2023.1169636/full

20. Olney. M. (March 31 2025). What is deepfake social engineering and how can businesses defend against it?. https://insights.integrity360.com/what-is-deepfake-social-engineering-and-how-can-businesses-defend-against-it

21. Clayton. J. (22 July 2023). Intel's deepfake detector tested on real and fake videos

https://www.bbc.com/news/technology-66267961

۲۲. مردانه زاده. حجت. (۱ اردیبهشت ۱۴۰۴). معرفی سرویس هوش مصنوعی + CrowdStrike Falcon AI قابلیت ها و کاربردها.

https://www.afzoneha.com/what-is-crowdstrike-falcon-ai-and-introduction/