فریب‌های سایبری و کلاه‌برداری‌های آنلاین

تهدیدات پنهان در رسانه‌های اجتماعی همراه با هوش مصنوعی،
ارائه تکنیک‌ها و راهکارهای امنیتی

مولف :

مهندس حمیدرضا صالحین

نشر دانشگاهی فرهمند

نام کتاب: فریب‌های سایبری و کلاه‌برداری‌های آنلاین
تهدیدات پنهان در رسانه‌های اجتماعی همراه با هوش مصنوعی، ارائه تکنیک‌ها و راهکارهای امنیتی
نویسنده : مهندس حمیدرضا صالحین
ویراستاران : علیرضا صالحین/ امیر زینی / نیلوفر زینی/ علیرضا محسنی فخر / پویا آرزومند امیدی لنگرودی / شهرام یوسفی / علیرضا فرهمندزادگان
سال چاپ: ۱۴۰۳
نوبت چاپ: اول
شمارگان: ۱۰۰
بها: ۲۸۰۰۰۰۰ ریال
شابک: ۳-۰۸-۴۹۸۰-۶۲۲-۹۷۸

نشانی: تهران، خیابان انقلاب، روبروی در اصلی دانشگاه، پاساژ فروزنده، طبقه اول، واحد ۴۱۹
تلفن: ۶۶۴۱۰۶۸۸-۶۶۹۶۸۶۱۴

تقدیم‌نامه:

با کمال تقدیر و تشکر، تقدیم به مادر و پدر عزیزم.

مهندس حمیدرضا صالحین
پاییز ۱۴۰۳

مقدمه نویسنده

در دنیای دیجیتال امروز، رسپانه‌های اجتماعی به‌طور چشمگیری شیوه ارتباط، گفتگو و به اشتراک‌گذاری زندگی ما را تغییر داده‌اند. با این‌حال، همزمان با این پیشرفت، افزایش نگران‌کننده‌ای در کلاهبرداری‌های آنلاین دیده می‌شود؛ به‌ویژه زمانی که کلاهبرداران به سرعت خود را با همان پلتفرم‌هایی که برای نزدیک‌تر کردن مردم طراحی شده بودند، تطبیق داده و از آن‌ها سوءاستفاده می‌کنند.

کتاب حاضر در پاسخ به یکی از بزرگترین چالش‌های فضای دیجیتال امروز، یعنی کلاهبرداری‌های سایبری و آنلاین، تدوین شده است. در عصری که فناوری با سرعتی سرسام‌آور در حال پیشرفت است و کاربران به‌طور گسترده‌تری از پلتفرم‌های آنلاین و رسانه‌های اجتماعی استفاده می‌کنند، خطرات و تهدیداتی جدید و پیچیده‌تر نیز به‌وجود آمده است. جامعه ایران که به‌سرعت در حال رشد دیجیتال و استفاده از این پلتفرم‌ها است، به آگاهی و آموزش صحیح درباره این تهدیدات نیاز مبرم دارد. این کتاب با هدف ارائه‌ی راهکارهای عملی و نوآورانه برای مقابله با این تهدیدات، به‌ویژه در زمینه‌ی کلاه‌برداری‌های آنلاین و امنیت سایبری، نگاشته شده است.

تحول فناوری و نیاز به امنیت بیشتر: با افزایش استفاده از پلتفرم‌هایی نظیر دیوار، شیپور، باما، ایسام و ترب، همزمان با افزایش رشد اینترنت در ایران، فضای جدیدی برای کاربران به وجود آمده است که متأسفانه به‌طور همزمان فرصت‌هایی را برای کلاه‌برداران نیز فراهم کرده است. کلاه‌برداری‌هایی نظیر جعل هویت، فیشینگ، و سکزتورتینگ به دلیل ماهیت ناشناس بودن در فضای مجازی و گستردگی کاربران، بسیار رایج شده‌اند. یکی از مهم‌ترین اهداف این کتاب، آشنایی کاربران ایرانی با روش‌های جدید کلاه‌برداری سایبری و ارائه‌ی توصیه‌هایی برای پیشگیری از این تهدیدات است. برای مثال، در فصل‌های مربوط به پلتفرم‌های ایرانی مانند دیوار و شیپور، به‌طور ویژه به روش‌های کلاه‌برداری مرتبط با این پلتفرم‌ها پرداخته شده است و نکات کاربردی برای حفظ امنیت کاربران ارائه شده است.

نوآوری‌ها و چالش‌های تکنولوژیک: یکی از موضوعات نوین این کتاب، پرداختن به تأثیر فناوری‌های جدید نظیر هوش مصنوعی، دیپ‌فیک و ابزارهای پیشرفته‌ی هک است. این فناوری‌ها، که از یک‌سو برای تسهیل زندگی و بهبود تجربه‌ی کاربری طراحی شده‌اند، به ابزاری قدرتمند برای کلاه‌برداران تبدیل شده‌اند. فصل‌های مربوط به دیپ‌فیک و تماس‌های ویدیویی

جعلی نشان‌دهنده‌ی تهدیدات جدیدی هستند که کاربران آنلاین با آن‌ها روبه‌رو هستند. این مسائل به‌خصوص در زمینه‌ی کلاه‌برداری‌های عاشقانه و سکزتورتینگ بسیار پررنگ هستند؛ زیرا کلاه‌برداران با استفاده از فناوری‌های جدید قادر به ایجاد ویدیوهای جعلی بسیار واقعی هستند که تشخیص آن‌ها حتی برای کاربران حرفه‌ای نیز دشوار است.

فصل‌های ابتدایی کتاب به مرور تاریخچه‌ی کلاه‌برداری‌های سایبری پرداخته و نشان می‌دهند که چگونه از ابتدای اینترنت، این تهدیدات وجود داشته و هم‌زمان با پیشرفت فناوری، روش‌های کلاه‌برداری نیز پیچیده‌تر و تخصصی‌تر شده‌اند. این کتاب با ارائه راهکارهای عملی برای هر نوع کلاه‌برداری، تلاش کرده است تا به کاربران ایرانی ابزاری برای حفاظت از خود در برابر این تهدیدات ارائه دهد.

نیاز جامعه ایران به آگاهی بیشتر: از ویژگی‌های برجسته این کتاب، تمرکز بر نیاز جامعه ایرانی به آموزش و آگاهی در زمینه تهدیدات سایبری است. به‌ویژه با توجه به افزایش استفاده از پلتفرم‌های آنلاین برای خرید و فروش محصولات و خدمات، جامعه ایرانی نیازمند درک بهتر از روش‌های کلاه‌برداری و نحوه‌ی مقابله با آن‌هاست. فصل‌های مربوط به روش‌های مرسوم کلاه‌برداری در بازارچه‌های آنلاین، مثل دیوار و شیپور، به‌طور ویژه به مسائل رایج در این پلتفرم‌ها پرداخته و با ذکر مثال‌های واقعی، راهکارهایی برای پیشگیری از این تهدیدات ارائه داده است.

علاوه بر این، فصول کتاب به موضوعات روان‌شناختی مرتبط با کلاه‌برداری‌های عاطفی و سکزتورتینگ نیز پرداخته‌اند. در جامعه‌ای که حفظ آبرو و حریم شخصی اهمیت ویژه‌ای دارد، این نوع کلاه‌برداری‌ها می‌توانند عواقب عاطفی و مالی جدی برای قربانیان به‌دنبال داشته باشند. این کتاب با ارائه توصیه‌هایی برای تشخیص این نوع کلاه‌برداری‌ها و ارائه راهکارهایی برای بازیابی و مقابله، به کاربران کمک می‌کند تا از خود و عزیزانشان در برابر این تهدیدات محافظت کنند.

منابع و مطالعات علمی: این کتاب با استفاده از منابع علمی معتبر و گزارش‌های رسمی پلیس فتا و مراکز بین‌المللی نظیر Kaspersky وMcAfee ، به‌طور جامع به تحلیل و بررسی تهدیدات سایبری پرداخته است. هر فصل از کتاب بر اساس مطالعات روز و تجربیات واقعی نوشته شده و به کاربران کمک می‌کند تا با استفاده از ابزارهای امنیتی، تنظیمات سیستم‌های عامل مختلف، و راهکارهای عملی در مقابل این تهدیدات ایمن شوند.

این کتاب به بررسی این بخش تاریک از فضای دیجیتال پرداخته و سازوکارها و راهبردهایی را که کلاهبرداران برای فریب کاربران ناآگاه به کار می‌گیرند، روشن می‌کند. این کتاب به روش‌های متنوعی اشاره می‌کند که طی آن‌ها رسانه‌های اجتماعی به‌طور ناخواسته به بستری برای فریب، سوءاستفاده و سرقت تبدیل شده‌اند. همچنین، نقاط ضعف این پلتفرم‌ها – شامل شکاف‌های موجود در حریم خصوصی، امنیت و نظارت – که به کلاهبرداران اجازه داده است تا به فعالیت خود ادامه دهند، آشکار می‌کند و به روش‌های مختلفی که کلاهبرداران برای جمع‌آوری داده‌ها، ایجاد هویت‌های جعلی و اجرای طرح‌های پیچیده استفاده می‌کنند، می‌پردازد؛ طرح‌هایی که اغلب پیامدهای مالی و احساسی سنگینی برای قربانیان به همراه دارند.

در طول این کتاب، خوانندگان به درک عمیق‌تری از چگونگی سوءاستفاده کلاهبرداران از رسانه‌های اجتماعی دست خواهند یافت. خواه از طریق لینک‌های فیشینگ، پروفایل‌های جعلی یا حتی روش‌های پیشرفته‌تری مانند دیپ‌فیک و کلاهبرداری‌های مبتنی بر هوش مصنوعی. تاکتیک‌های کلاهبرداران بسیار متنوع هستند، اما همگی یک وجه مشترک دارند: بهره‌برداری از اعتماد کاربران.

تلاش گردیده تا با ارائه اطلاعات دقیق و کاربردی، به کسب‌وکارها کمک می‌کند تا با اعتمادبه‌نفس بیشتری در بازار جهانی فعالیت کنند و از حقوق و منافع خود محافظت کنند. امیدوارم که این کتاب برای شما، خواننده گرامی، مفید و مؤثر واقع شود و بتواند نقشی مؤثر در افزایش آگاهی و توانمندی شما در مقابله با جعل ایفا نماید.

از جناب آقای علیرضا فرهمند زادگان و نشر دانشگاهی فرهمند دررابطه با همکاری در راستای به‌وجودآمدن و چاپ این اثر که با بنده همکاری داشتند، و همچنین مهندس علیرضا صالحین که بر روی مرحله‌به‌مرحله کتاب نظارت داشتند هم کمال تشکر و سپاسگزاری را دارم.

مهندس حمیدرضا صالحین، پاییز ۱۴۰۳

فهرست کتاب

فصل اول : سیر تحول کلاهبرداری‌ها در رسانه‌های اجتماعی

این کتاب نه تنها به روشن‌سازی این خطرات می‌پردازد، بلکه به خوانندگان ابزارها و دانشی ارائه می‌دهد تا بتوانند با امنیت بیشتری در این فضای پر از تله رسانه‌های اجتماعی حرکت کنند. فصل‌های بعدی کتاب، راهنمای جامعی برای شناخت جهان همیشه در حال تغییر کلاهبرداری‌های رسانه‌های اجتماعی ارائه می‌دهد، و با تشویق به هوشیاری و ارائه راهبردهای پیشگیرانه، به دنبال ایجاد امید و آگاهی در خوانندگان است. این اثر، فراخوانی است برای محافظت فردی و یادآوری اهمیت سواد دیجیتال در دنیایی که با وجود اتصال بیشتر، آسیب‌پذیرتر از همیشه است.

این رسانه‌ها که در ابتدا به‌منظور ایجاد ارتباطات شخصی و تعاملات اجتماعی ساده طراحی شده بودند، به تدریج به محیطی پیچیده و گسترده برای فعالیت‌های تجاری، حرفه‌ای و شخصی تبدیل شدند. اما همزمان با گسترش دسترسی و نفوذ این پلتفرم‌ها، گروه‌های مخرب نیز به فکر سوءاستفاده از این فضا افتادند. در ابتدا، کلاهبرداری‌های مرتبط با رسانه‌های اجتماعی بسیار ابتدایی و محدود به موارد ساده‌ای مانند هک کردن حساب‌های شخصی و ارسال پیام‌های اسپم یا لینک‌های فیشینگ به دوستان بودند.

این کلاهبرداری‌های اولیه معمولاً بدون هدف‌گذاری دقیق و با تکیه بر ناآگاهی کاربران از تهدیدات اینترنتی انجام می‌شدند. با این حال، با گذشت زمان و گسترش نفوذ رسانه‌های اجتماعی، کلاهبرداران نیز به روش‌های پیشرفته‌تر و پیچیده‌تری روی آوردند. به این ترتیب، رسانه‌های اجتماعی به یکی از اهداف اصلی کلاهبرداران تبدیل شدند، چرا که حجم بالای اطلاعات شخصی کاربران و فرصت‌های بی‌پایان برای تقلب، بستری مناسب برای فعالیت‌های کلاهبرداری فراهم کرد.

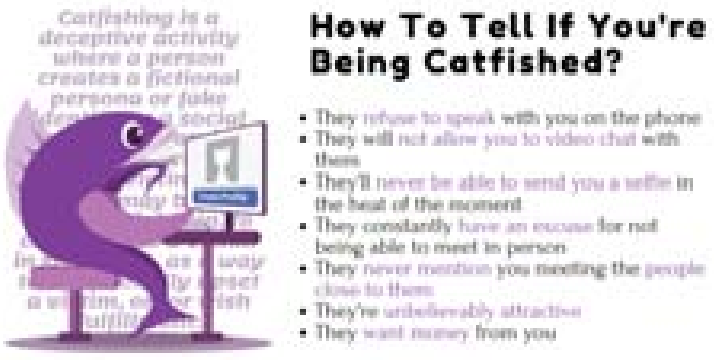
در این کتاب به بررسی راه‌ها و روش‌هایی پرداخته می‌شود که کلاهبرداران برای بهره‌برداری از این فضا استفاده می‌کنند، از جمله ایجاد پروفایل‌های جعلی، ارسال لینک‌های مخرب، و حتی استفاده از فناوری‌های پیشرفته مانند دیپ‌فیک‌ها و هوش مصنوعی برای فریب کاربران. هدف این کتاب، ارائه شناخت عمیق‌تر از این تهدیدات و همچنین آموزش راه‌های مقابله با آن‌هاست.

ظهور کلاهبرداری‌های پیچیده: دهه ۲۰۱۰ و بعد از آن

با ادغام شبکه‌های اجتماعی با خدمات دیجیتال دیگر، مانند بازارهای آنلاین، درگاه‌های پرداخت و شبکه‌های تبلیغاتی، نوع و ماهیت کلاهبرداری‌ها دستخوش تغییرات اساسی شد. دهه ۲۰۱۰ شاهد رشد و توسعه کلاهبرداری‌های هدفمند و پیچیده‌ای بود که از نقاط ضعف زیرساختی رسانه‌های اجتماعی بهره‌برداری می‌کردند. کلاهبرداران به‌سرعت با استفاده از روش‌هایی که با توسعه خود شبکه‌های اجتماعی همگام بود، به فریب کاربران پرداختند؛ از ساخت پروفایل‌های جعلی و فریب به‌وسیله "کت فیش" گرفته تا تصاحب حساب‌های کاربران و راه‌اندازی کمپین‌های پیچیده فیشینگ.

توضیحاتی در مورد کت فیش:

کَتفیش)Catfishing) نوعی کلاهبرداری آنلاین است که در آن فردی با استفاده از هویت‌های جعلی و پروفایل‌های دروغین در شبکه‌های اجتماعی یا وب‌سایت‌های دوستیابی، تلاش می‌کند دیگران را فریب دهد. این افراد با ساختن شخصیت‌های غیرواقعی و ارائه اطلاعات نادرست درباره خود، سعی می‌کنند تا با قربانیان ارتباط برقرار کنند و از اعتماد آن‌ها سوءاستفاده نمایند. هدف این نوع کلاهبرداری می‌تواند مالی، عاطفی، یا حتی برای سرگرمی باشد.

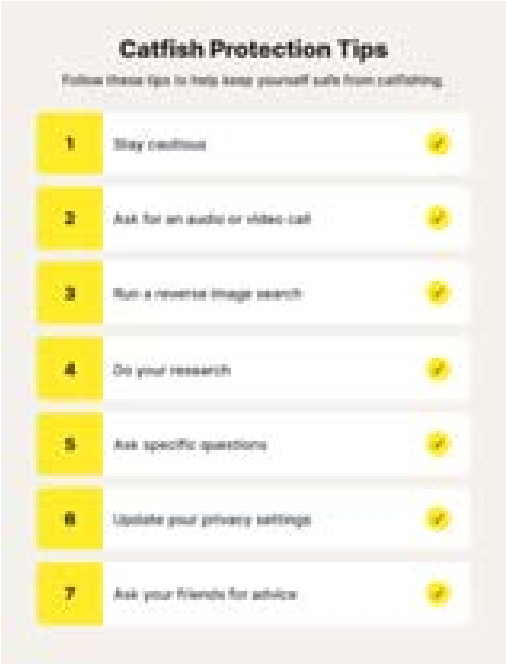


در کتفیش، فرد کلاهبردار معمولاً از تصاویر و اطلاعات ساختگی برای جلب توجه و اعتماد قربانی استفاده می‌کند. این افراد ممکن است خود را به عنوان شخصی جذاب و مورد اعتماد معرفی کنند تا بتوانند رابطه‌ای آنلاین با قربانی برقرار کنند. پس از اینکه اعتماد قربانی جلب

شد، کلاهبردار ممکن است از آن‌ها درخواست پول، اطلاعات شخصی یا حتی عکس‌ها و ویدیوهای خصوصی کند. در برخی مواقع، هدف کلاهبردار فقط دستکاری احساسات و وقت‌تلفی قربانی است، اما در بسیاری از موارد، این نوع فریب منجر به آسیب‌های جدی مالی و روانی می‌شود.

یکی از ویژگی‌های مهم کتفیش این است که قربانی‌ها معمولاً از هویت واقعی فرد مقابل خبر ندارند و ممکن است تا مدت‌ها در یک رابطه آنلاین با فردی که وجود خارجی ندارد، باقی بمانند. این نوع کلاهبرداری به طور معمول از طریق پیام‌های مستقیم در شبکه‌های اجتماعی، سایت‌های دوستیابی، یا حتی از طریق ایمیل انجام می‌شود.

برای جلوگیری از گرفتار شدن در دام کتفیش، باید هنگام برقراری ارتباطات آنلاین بسیار محتاط بود. به‌ویژه زمانی که طرف مقابل درخواست‌هایی مانند ارسال پول یا ارائه اطلاعات شخصی دارد، باید هوشیار بود. همچنین بهتر است قبل از اعتماد کامل به کسی که فقط از طریق فضای مجازی با او آشنا شده‌اید، تحقیقاتی در مورد هویت واقعی او انجام دهید و مطمئن شوید که شخص مقابل واقعی است.



در این دوران، روش جدیدی از کلاهبرداری با نام «مهندسی اجتماعی» به‌شدت رشد کرد. در این روش، کلاهبرداران با فریب و جلب اعتماد کاربران، آن‌ها را به ارائه اطلاعات شخصی خود وادار می‌کردند. معمولاً این کار با تقلید از هویت‌های معتبر و مورد اعتماد، مانند دوستان یا سازمان‌های شناخته‌شده انجام می‌شد. ویژگی‌های ذاتی شبکه‌های اجتماعی، مانند درخواست دوستی، دنبال کردن و ارسال پیام‌های خصوصی، زمینه‌ساز ایجاد اعتماد کاذب بود. کلاهبرداران به‌سادگی می‌توانستند پروفایل‌های جعلی بسازند، حساب‌ها را شبیه‌سازی کنند و هویت افراد یا سازمان‌ها را جعل نمایند، در حالی‌که خطر شناسایی بسیار پایین بود. این عوامل باعث شد که رسانه‌های اجتماعی به بستری جذاب برای انواع کلاهبرداران، از مجرمان خرده‌پا گرفته تا شبکه‌های سازمان‌یافته جنایی، تبدیل شود.

رشد کلاهبرداری‌های بازار و مالی

با گسترش پلتفرم‌هایی مانند فیس‌بوک و اینستاگرام و افزودن قابلیت‌هایی که به کاربران اجازه خرید و فروش کالاها را می‌داد، کلاهبرداری‌های مرتبط با بازار نیز به سرعت افزایش یافت.

کلاهبرداران با ساخت پروفایل‌های جعلی، اقدام به فروش کالاهای تقلبی یا غیرموجود می‌کردند و خریداران ناآگاه را با پیشنهادات جذاب و قیمت‌های پایین فریب می‌دادند. این نوع کلاهبرداری‌ها از رشد سریع تجارت الکترونیک و اجتماعی بهره‌برداری می‌کردند؛ فضایی که کاربران دیگر تنها برای ارتباطات اجتماعی از آن استفاده نمی‌کردند، بلکه به‌عنوان بازاری برای خرید و فروش محصولات و خدمات نیز به کار می‌بردند.

در کنار این، کلاهبرداری‌های مالی نیز رشد چشمگیری داشت. با ظهور سیستم‌های پرداخت دیجیتال و محبوبیت روزافزون ارزهای دیجیتال، کلاهبرداران از آگاهی محدود کاربران در مورد این فناوری‌های جدید سوءاستفاده کردند. طرح‌های پونزی، هرمی و فرصت‌های سرمایه‌گذاری کاذب به‌ویژه در پلتفرم‌هایی نظیر فیس‌بوک و توییتر (X) به وفور دیده شد. کلاهبرداران با معرفی خود به‌عنوان سرمایه‌گذاران موفق یا مشاوران مالی، فرصت‌های «یک بار در زندگی» را به کاربران ارائه می‌دادند و وعده بازدهی‌های سریع و غیرواقعی می‌دادند. بسیاری از کاربران، تحت تأثیر این تبلیغات و اعتمادی که به این پلتفرم‌ها داشتند، گرفتار این طرح‌های کلاهبرداری شدند.

رسانه‌های اجتماعی و سرقت هویت

یکی از تحولات مهم در زمینه کلاهبرداری‌های رسانه‌های اجتماعی، افزایش استفاده از این پلتفرم‌ها برای سرقت هویت بود. کاربران به‌طور داوطلبانه بخش‌های مختلفی از زندگی شخصی خود را به‌صورت آنلاین به اشتراک می‌گذاشتند؛ از عکس‌ها و به‌روزرسانی وضعیت گرفته تا موقعیت‌های مکانی و اطلاعات شغلی. این امر به کلاهبرداران کمک کرد تا به‌راحتی به اطلاعات شخصی کاربران دسترسی پیدا کنند و از آن‌ها برای کلاهبرداری‌های بعدی بهره‌برداری کنند. سرقت هویت یکی از چالش‌های جدی در این فضا شد و به کلاهبرداران این امکان را داد که بدون اطلاع کاربران از اطلاعات شخصی آن‌ها برای اهداف مختلفی استفاده کنند.

کلاهبرداران در بسیاری از موارد اقدام به شبیه‌سازی پروفایل‌های واقعی یا ایجاد حساب‌های جعلی می‌کنند که به‌طور دقیق از کاربران واقعی تقلید می‌کنند. این حساب‌های جعلی به‌گونه‌ای طراحی شده‌اند که بتوانند با دوستان و خانواده قربانی ارتباط برقرار کنند. هدف اصلی این کلاهبرداری‌ها معمولاً درخواست پول تحت بهانه‌های جعلی یا ارسال لینک‌های مخرب برای انتشار بدافزار است. استفاده از رسانه‌های اجتماعی به‌عنوان ابزاری برای سرقت هویت چنان گسترده شده که در حال حاضر یکی از مهم‌ترین دلایل کلاهبرداری‌های آنلاین در سطح جهان به‌شمار می‌رود.

ویژگی‌های متصل و پیوسته شبکه‌های اجتماعی به این معناست که وقتی اطلاعات یک کاربر در یک پلتفرم به سرقت می‌رود، احتمال سرایت این نقض امنیتی به سایر پلتفرم‌ها نیز بسیار زیاد است. به‌عنوان مثال، کلاهبرداری که به حساب فیس‌بوک فردی دسترسی پیدا کند، به‌راحتی می‌تواند از اطلاعات جمع‌آوری‌شده برای دسترسی به ایمیل، حساب بانکی یا سایر حساب‌های شبکه‌های اجتماعی او استفاده کند. این آسیب‌پذیری میان‌پلتفرمی، رسانه‌های اجتماعی را به بستری مناسب برای سرقت هویت و انجام کلاهبرداری‌های گسترده‌تر تبدیل کرده است.

کلاهبرداری‌های فیشینگ و جعل هویت

فیشینگ، یکی از قدیمی‌ترین و پرکاربردترین روش‌های کلاهبرداری آنلاین، با ظهور شبکه‌های اجتماعی شکل‌های پیچیده‌تر و مؤثرتری به خود گرفته است. در گذشته، فیشینگ به ارسال ایمیل‌هایی شبیه به پیام‌های نهادهای معتبر مانند بانک‌ها یا سازمان‌های دولتی محدود بود. اما با گسترش شبکه‌های اجتماعی، کلاهبرداران توانسته‌اند هویت نزدیکان یا همکاران قربانی را جعل کنند و فریب را به سطح جدیدی برسانند.

کلاهبرداری رایجی که امروزه در شبکه‌های اجتماعی اتفاق می‌افتد، شامل هک کردن حساب کاربری فردی است که پس از آن کلاهبردار پیام‌هایی را به دوستان و مخاطبان قربانی ارسال می‌کند. این پیام‌ها معمولاً درخواست کمک مالی یا ارائه اطلاعات شخصی دارند. از آنجایی که

این پیام‌ها ظاهراً از سوی فردی می‌آید که قربانی او را می‌شناسد و به او اعتماد دارد، احتمال فریب خوردن بسیار بالاست. علاوه بر این، با افزایش استفاده از دستگاه‌های تلفن همراه برای دسترسی به شبکه‌های اجتماعی، کاربران بیشتر در معرض حملات فیشینگ قرار می‌گیرند. رابط کاربری کوچک‌تر دستگاه‌های موبایل، ممکن است نشانه‌های هشداردهنده‌ای که معمولاً در کلاهبرداری‌های فیشینگ وجود دارد را پنهان کند و در نتیجه احتمال فریب کاربران بیشتر شود.

عصر کلاهبرداری‌های مبتنی بر هوش مصنوعی و دیپ‌فیک‌ها

آشنایی مختصر با دیپ فیک:

دیپ‌فیک (Deepfake) یکی از فناوری‌های پیشرفته و نوظهور است که با استفاده از هوش مصنوعی و یادگیری ماشین، ویدیوها و تصاویر جعلی تولید می‌کند که به‌طرز شگفت‌انگیزی واقعی به نظر می‌رسند. این فناوری قادر است چهره و صدای افراد را با دقتی بالا تغییر دهد و آن‌ها را در ویدیوهایی که هرگز در واقعیت اتفاق نیفتاده‌اند، نشان دهد. به این ترتیب، ممکن است ویدیویی منتشر شود که در آن فردی مشهور، سیاستمدار یا حتی یک شخص عادی، به‌نظر می‌رسد که در حال انجام کاری است که هرگز انجام نداده است.

کاربردهای دیپ‌فیک متنوع است و می‌تواند هم در زمینه‌های مثبت و هم در حوزه‌های منفی مورد استفاده قرار گیرد. از موارد مثبت می‌توان به صنعت فیلم‌سازی و تلویزیون اشاره کرد که از این فناوری برای بازسازی چهره بازیگران قدیمی یا جوان‌سازی آن‌ها استفاده می‌شود. همچنین در تبلیغات و تولید محتوای آموزشی نیز دیپ‌فیک‌ها می‌توانند ابزارهای مفیدی باشند. اما از سوی دیگر، دیپ‌فیک‌ها در دست افراد نادرست به ابزاری برای کلاهبرداری، جعل هویت و تخریب شهرت دیگران تبدیل شده‌اند.

خطرات دیپ‌فیک زمانی جدی‌تر می‌شود که تشخیص جعلی بودن این ویدیوها بسیار دشوار است. ویدیوهای دیپ‌فیک به‌قدری با دقت و مهارت ساخته می‌شوند که تشخیص آن‌ها از ویدیوهای واقعی برای افراد عادی تقریباً غیرممکن است. این موضوع به کلاهبرداران اجازه می‌دهد تا از دیپ‌فیک‌ها برای فریب افراد، باج‌گیری یا انتشار اطلاعات نادرست استفاده کنند. به‌عنوان مثال، ممکن است ویدیوی جعلی از یک سیاستمدار ساخته شود که در آن سخنانی می‌گوید که هرگز نگفته است. چنین ویدیوهایی می‌توانند به شدت بر افکار عمومی تأثیر بگذارند و پیامدهای اجتماعی و سیاسی گسترده‌ای داشته باشند.

در مقابل، تلاش‌هایی برای مقابله با این تهدیدها در حال انجام است. متخصصان فناوری به‌دنبال توسعه ابزارهایی هستند که قادر به شناسایی ویدیوهای دیپ‌فیک باشند. همچنین، برخی کشورها در حال تصویب قوانین جدید برای محدود کردن استفاده غیرقانونی از این فناوری هستند. با این حال، سرعت پیشرفت دیپ‌فیک و پیچیدگی آن چالش‌های بزرگی را در این مسیر به وجود آورده است.

دیپ‌فیک در عین حال که می‌تواند در حوزه‌هایی مانند سینما و آموزش، نوآوری و خلاقیت به همراه داشته باشد، در صورت استفاده نادرست می‌تواند به ابزاری خطرناک تبدیل شود که به امنیت و اعتماد عمومی آسیب برساند. بنابراین، نیاز است که نه تنها از لحاظ فناوری، بلکه از نظر قانونی نیز به شکل جدی‌تری بر استفاده از این فناوری نظارت شود تا از آسیب‌های احتمالی آن جلوگیری شود.

در تصاویر زیر نمونه هایی از دیپ فیک را می توانید مشاهده کنید.


ORIGINAL
DEEPFAKE
FAKE

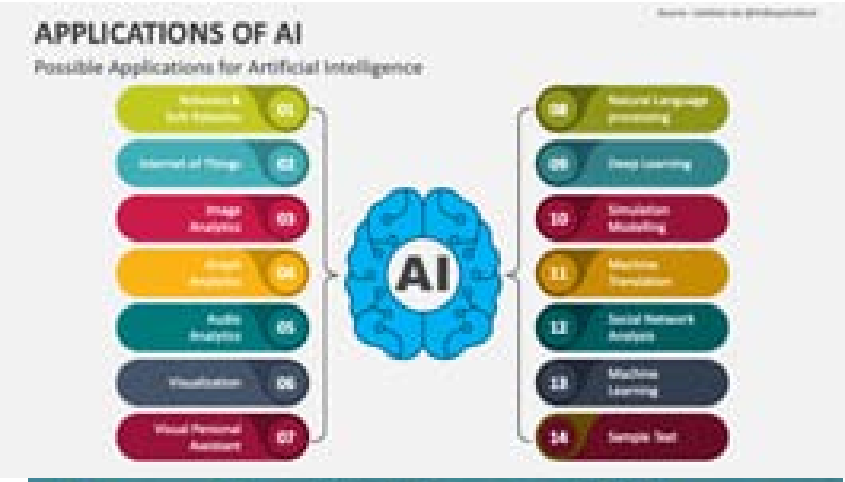
آشنایی مختصر با هوش مصنوعی:

هوش مصنوعی (AI) در واقع به مجموعه‌ای از تکنیک‌ها و الگوریتم‌هایی گفته می‌شود که به ماشین‌ها امکان می‌دهد وظایفی را انجام دهند که پیش‌تر به طور انحصاری توسط انسان‌ها انجام می‌شد. این وظایف شامل یادگیری، تصمیم‌گیری، حل مسائل و حتی تشخیص الگوها هستند. به بیان ساده، هوش مصنوعی می‌تواند ماشین‌ها را قادر سازد که مانند انسان فکر کنند و عمل کنند.

یکی از رایج‌ترین انواع هوش مصنوعی که امروزه در بسیاری از محصولات و خدمات دیجیتال مشاهده می‌شود، هوش مصنوعی محدود است. این نوع هوش مصنوعی تنها قادر است وظایف خاص و مشخصی را انجام دهد و خارج از این چارچوب توانایی عمل ندارد. برای مثال، دستیارهای صوتی مانند سیری یا الکسا، و همچنین سیستم‌های تشخیص چهره که در گوشی‌های هوشمند مورد استفاده قرار می‌گیرند، از هوش مصنوعی محدود بهره می‌برند. این سیستم‌ها توانایی یادگیری یا تصمیم‌گیری خارج از محدوده تعیین‌شده خود را ندارند.

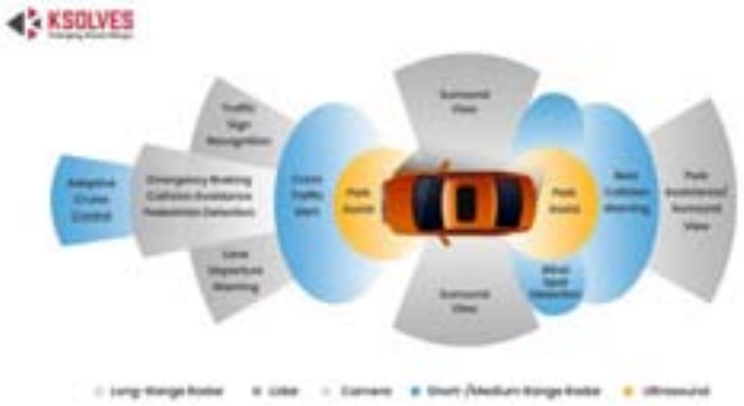
نوع دیگری از هوش مصنوعی که هنوز در مرحله پژوهش و توسعه است، هوش مصنوعی عمومی است. این نوع از هوش مصنوعی توانایی دارد در هر زمینه‌ای که انسان‌ها قادر به انجام آن هستند، عمل کند. یعنی می‌تواند به صورت خودکار از تجربیات گذشته یاد بگیرد و در مواجهه

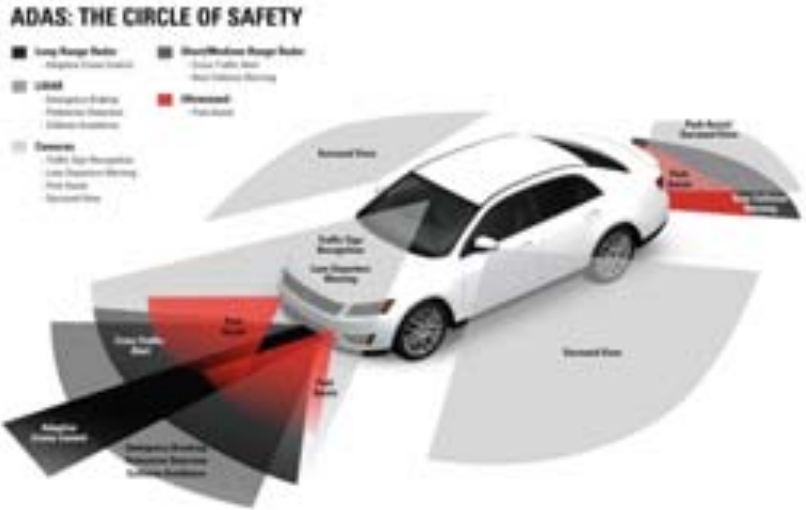
با مسائل جدید، راه‌حل‌هایی ارائه دهد. برخلاف هوش مصنوعی محدود، هوش مصنوعی عمومی به صورت بالقوه می‌تواند به تنهایی به حل مسائل پیچیده بپردازد و تصمیمات هوشمندانه‌ای بگیرد.



کاربردهای هوش مصنوعی بسیار گسترده‌اند و در زمینه‌های مختلفی از جمله پزشکی، صنعت، حمل‌ونقل و خدمات مالی دیده می‌شوند. در پزشکی، هوش مصنوعی در تشخیص سریع‌تر و دقیق‌تر بیماری‌ها کمک می‌کند و می‌تواند تحلیل‌های پیچیده‌ای روی داده‌های پزشکی انجام دهد. در صنعت، هوش مصنوعی به بهینه‌سازی فرآیندهای تولید و پیش‌بینی نیازهای آینده کمک

می‌کند. همچنین در حمل‌ونقل، خودروهای خودران که از هوش مصنوعی استفاده می‌کنند، بدون نیاز به راننده مسیر خود را پیدا کرده و تصمیمات لازم برای جلوگیری از تصادفات را اتخاذ می‌کنند.





ا وجود تمام مزایای هوش مصنوعی، نگرانی‌هایی نیز پیرامون آن وجود دارد. یکی از این نگرانی‌ها، از دست رفتن فرصت‌های شغلی برای انسان‌هاست. با گسترش سیستم‌های خودکار، احتمالاً نیاز به نیروی کار انسانی در برخی حوزه‌ها کاهش یابد. همچنین، بحث حریم خصوصی

و امنیت داده‌ها نیز یکی دیگر از دغدغه‌هاست، چرا که هوش مصنوعی برای یادگیری و تصمیم‌گیری نیازمند دسترسی به حجم زیادی از داده‌های شخصی است.

هوش مصنوعی به سرعت در حال پیشرفت است و در آینده نزدیک احتمالاً تغییرات چشمگیری در صنایع مختلف ایجاد خواهد کرد. با توسعه بیشتر این فناوری، می‌توانیم شاهد اتوماسیون بیشتر در بسیاری از زمینه‌ها باشیم، از جمله در حوزه‌های تولید، پزشکی، حمل‌ونقل و حتی آموزش.

با پیشرفت فناوری، کلاهبرداران نیز به ابزارهای پیشرفته‌تری دسترسی پیدا کرده‌اند که کار آن‌ها را بسیار ساده‌تر کرده است. یکی از این ابزارها، هوش مصنوعی (AI) است که امکان‌های جدیدی را برای کلاهبرداری در شبکه‌های اجتماعی فراهم کرده است. با استفاده از هوش مصنوعی، کلاهبرداران می‌توانند صداهایی بسیار شبیه به صدای افراد واقعی تولید کنند. این صداهای مصنوعی به‌قدری دقیق هستند که قربانیان به راحتی فریب می‌خورند و تصور می‌کنند با دوست یا فرد معتبری در حال مکالمه هستند.

از سوی دیگر، فناوری دیپ‌فیک به کلاهبرداران این امکان را داده است تا ویدیوهایی بسازند که به نظر کاملاً واقعی هستند، اما در حقیقت هیچ‌یک از وقایعی که در آن‌ها نمایش داده می‌شود، اتفاق نیفتاده است. این ویدیوهای جعلی می‌توانند از افراد مشهور، سیاستمداران یا حتی دوستان و آشنایان قربانی ساخته شوند و برای اخاذی، باج‌گیری یا تغییر افکار عمومی مورد استفاده قرار گیرند. به‌عنوان مثال، کلاهبرداران ممکن است ویدیویی جعلی از یک سیاستمدار بسازند که در آن او در حال بیان سخنانی است که هرگز نگفته است. چنین ویدیوهایی می‌توانند تأثیرات بسیار مخربی داشته باشند.

هرچند استفاده از کلاهبرداری‌های مبتنی بر هوش مصنوعی و دیپ‌فیک‌ها هنوز به‌طور گسترده صورت نمی‌گیرد، اما این فناوری‌ها پتانسیل زیادی برای ایجاد خسارت‌های بزرگ دارند. با گسترش و دسترسی آسان‌تر به این فناوری‌ها، انتظار می‌رود که این ابزارها به‌سرعت به یکی از روش‌های اصلی کلاهبرداری در فضای مجازی تبدیل شوند.

جهانی‌شدن کلاهبرداری‌های شبکه‌های اجتماعی

یکی از ویژگی‌های بارز کلاهبرداری‌های مرتبط با رسانه‌های اجتماعی، جهانی بودن آن‌ها است. شبکه‌های اجتماعی همچون فیس‌بوک، اینستاگرام و توییتر، کاربران را از سراسر جهان به هم متصل می‌کنند، و این به کلاهبرداران این فرصت را می‌دهد که به‌صورت همزمان، قربانیانی از کشورهای مختلف را مورد هدف قرار دهند.