



ChatGPT

آیا چت جی پی تی

جدیدترین دروازه برای کلاهبرداری است؟

هر چند که ناراحت‌کننده است، اما هکرها و مجرمان سایبری به دلیل داشتن مهارت‌های انجام این کارها، بیشتر اوقات مورد تحسین قرار می‌گیرند. انجام هک و جرایم سایبری، مستلزم داشتن دانش درخور توجهی است که خوشبختانه این فعالیتها را به گروه کوچکی محدود می‌کند. اما ربات جدید چت جی پی تی (Chat GPT) می‌تواند همه این عوامل را تغییر دهد. در اینجا علت و نحوه مقابله با زرسان تقلب با این فعالیتها ارائه شده است.

تنها چند هفته پس از این که موسسه اوپن‌ای‌ای (OpenAI) آزمایشگاه پژوهشی هوش مصنوعی در ایالات متحد، چت جی پی تی را در نوامبر سال گذشته (۲۰۲۲) راه‌اندازی کرد، شرکت امنیت سایبری چک پوینت (Check Point) متوجه افزایش مکالمات در دارکوب^۱ شد.

دستیار سخنگوی هوش مصنوعی با توانایی خود در انجام بسیاری از وظایف انسانی، از کدنویسی گرفته تا قبولی در آزمون سطح ام‌بی‌ای (MBA) و نوشتن متن بدون ایراد، عموم را شگفت‌زده کرده و در عین حال باعث ناراحتی مردم هم شده است.

با این وجود، در یک همنشینی پرهوادار هک { ویراستار: شاید بتوان از معادل «رخنه‌گری» به جای هک استفاده کرد}، در مطلبی با عنوان «چت جی پی تی، مزایای بدافزار» بیان شد که چگونه یکی از کلاهبرداران از ابزار هوش مصنوعی برای

در مورد دامنه گسترده‌ای از موضوعها، از جمله تاریخ، علوم تجربی، جغرافیا و غیره پاسخ دهد.

• تولید متن: چت جی‌پی‌تی می‌تواند متنی را براساس یک درخواست یا موضوع تولید کند؛ همانند نوشتن یک داستان، تولید یک شعر، یا خلاصه‌کردن یک مقاله خبری.

• گفتگو: چت جی‌پی‌تی می‌تواند در گفتگوها به زبان طبیعی با کاربران شرکت کند و برای آن‌ها این امکان را فراهم می‌آورد که تجربه‌ای مشابه گفتگو با یک انسان داشته باشند.

• تکمیل جمله‌ها یا بندها: چت جی‌پی‌تی می‌تواند یک جمله یا بند را براساس دستور داده‌شده تکمیل کند و برای کاربران این امکان را فراهم می‌آورد که بتوانند متنی با کارایی بیشتر تولید کنند.

به‌طور کلی، چت جی‌پی‌تی یک ابزار قدرتمند برای پردازش زبان طبیعی است و می‌تواند در برنامه‌های مختلف همانند رباتهای گفتگو، ترجمه زبان و خلاصه‌سازی متن استفاده شود.

وقتی از چت جی‌پی‌تی خواستم خودش را به‌سادگی برای مردم عادی توضیح دهد، پاسخ داد:

”چت جی‌پی‌تی یک مدل زبان هوش مصنوعی است که توسط موسسه اپن‌ای‌آر توسعه یافته و می‌تواند متنی شبیه انسان را درک و تولید کند. این روی حجم عظیمی از داده‌های متنی آموزش دیده است؛ بنابراین می‌تواند به پرسشها پاسخ دهد، گفتگو کند، جمله‌ها یا بندها را کامل و به‌تنهایی متن تولید کند. به زبان ساده، همانند داشتن یک دوست دیجیتالی است که می‌تواند شما را درک کند و به پرسشها و پیامهای شما به‌شیوه‌ای انسانی پاسخ دهد.“

دستیار سخنگوی هوش مصنوعی با توانایی خود در انجام بسیاری از وظایف انسانی از کدنویسی گرفته تا قبولی در آزمون ام‌بی‌ای تا نوشتن متن بی‌ایراد، عموم را متحیر کرده اما باعث ناراحتی مردم نیز شده است.

هر شخصی می‌تواند از چت جی‌پی‌تی برای توضیح مفاهیم ساده و پیچیده و کمک به نوشتن رزومه، شرح زندگی، آهنگ، لطایف و وبلاگ استفاده کند. این دستیار می‌تواند به ایجاد محتوای بازاریابی و ترجمه محتوای موجود به چندین زبان با تفاوت‌های دستور زبانی و واژه‌پردازی کمک کند. دستیار می‌تواند اصول بنویسد، مشاوره ارتباطی ارائه دهد یا یک همراه

بازافرینی انواع بدافزار استفاده کرده است؛ همانند به‌اصطلاح دزدهایی که در سامانه‌های رایانه‌های پیشرفته، انواع خاصی از فایلها را جستجو می‌کنند و سپس بدون اطلاع صاحبان، آن‌ها را حذف می‌کنند.

با وجود آن‌که ایجاد بدافزار چیز جدیدی نیست، اما بحث در دارک‌وب نگران‌کننده بود؛ زیرا همانطور که چک‌پوینت اشاره کرد، در ظاهر هدف آن بود که به کلاهبردارانی با دانش فنی کمتر، نشان دهند که آن‌ها هم می‌توانند از چت جی‌پی‌تی برای کدنویسی در راستای اهداف مخرب استفاده کنند.

به‌عنوان شاهدهی بر این موضوع، چک‌پوینت به یک مطلب دیگر درباره دارک‌وب پرداخت که در آن یک مجرم سایبری با نام **یواس‌داد** (USDoD) در مورد این صحبت کرد که چگونه موسسه اپن‌ای‌آی به او کمک کرد اولین **اسکرپت** (Script) خود را که یک مجموعه دستورالعمل شبیه برنامه‌نویسی محاسباتی اما به‌طور معمول ساده‌تر از آن است را بسازد.

با وجود آن‌که اسکرپت‌نویسی به‌خودی‌خود مخرب نیست، چک‌پوینت خاطر نشان کرد که هکر یواس‌داد شاید مهارت‌های فنی محدودی دارد و در شبکه پنهانی، به‌دلیل فروش دسترسی به شرکت‌های در معرض ریسک و داده‌های سرقت‌شده، شناخته شده است.

چت جی‌پی‌تی چیست

هر اختراع، عواقبی غیرمنتظره و ناخواسته به‌همراه دارد. چت جی‌پی‌تی مخفف عبارت **انتقال‌دهنده مولد از پیش آموزش‌یافته** (Generative Pre-trained Transformer) است. در حقیقت، هوش مصنوعی است که توسط موسسه اپن‌ای‌آی تهیه شده و محتوای مبتنی‌بر متن تولیه می‌کند. از خود چت جی‌پی‌تی خواستم که در مورد خودش توضیح دهد و پاسخ داد:

”یک مدل زبان محاوره‌ای است که توسط موسسه اپن‌ای‌آی تهیه شد. این مدل براساس طرح مولد از پیش آموزش‌یافته درست شده و روی مجموعه بزرگی از داده‌های متنی آموزش داده شده است تا پاسخهایی شبیه انسان به دامنه گسترده‌ای از پرسشها و درخواستها ارائه دهد.“

چت جی‌پی‌تی قادر به انجام وظایف مختلفی است، از جمله:

- پاسخ به پرسشها: چت جی‌پی‌تی می‌تواند به پرسشهایی

همیشگی (هرچند مصنوعی) باشد. کاربردهای نامحدودی دارد و همین یک مشکل است؛ زیرا کلاهبرداران از آن به روشهای خلاقانه و غیرقابل تصور استفاده منفی می‌کنند. موسسه این ای‌آی، چت جی‌پی‌تی را در ۳۰ نوامبر ۲۰۲۲ راه‌اندازی کرد، اما پس از اولین حضورش در نمایشگاه **لوازم الکتریکی** (Consumer Electronics) در لاس‌وگاس در ژانویه ۲۰۲۳، غوغایی در دنیای فناوری ایجاد کرد. در عرض چند هفته، دانش‌آموزان دبیرستانی و کالج شروع به استفاده از چت جی‌پی‌تی برای انجام تکالیف از جمله نوشتن مقاله‌های مفصل خود کردند.

معلمان فوری با مشکلی اساسی روبه‌رو شدند. اما بدتر از آن، کلاهبرداران، متقلبان و مجرمان سایبری به سرعت شروع به استفاده از آن برای کلاهبرداریهای مختلف کردند:

- ایمیل‌های کلاهبردارانه.
- ایجاد بدافزار و ویروس.
- رمزگذاری داده‌ها برای تولید باج افزار.
- رمزگشایی داده‌ها برای سرقت اطلاعات قابل‌شناسایی شخصی محافظت شده.
- پرداخت به موقع ارز دیجیتال برای بازارهای دارکوب.
- کلاهبرداری عاشقانه.

هیچ یک از اینها مشکلات جدید نیستند، اما چت جی‌پی‌تی اهمیت آن‌ها را بالا برد و مسایل جدیدی را ایجاد کرد. در اینجا نگاهی عمیق‌تر به برخی از فعالیتهای کلاهبرداری که چت جی‌پی‌تی می‌تواند آن‌ها را تشدید کند، می‌اندازیم.

ایمیل کلاهبردارانه

موسسه این‌ای‌آی تلاش کرد که از استفاده از محتوای مخرب جلوگیری کند. برای نمونه، اگر از چت جی‌پی‌تی بخواهید که ایمیل کلاهبردارانه ایجاد کند، امتناع می‌ورزد اما راهکارهای آسانی در این باره وجود دارد. (مقاله «مجرمان سایبری برای تولید محتوای مخرب محدودیتهای چت جی‌پی‌تی را دور می‌زنند»). به‌عنوان نمونه، وقتی از چت جی‌پی‌تی خواستم نامه‌ای از **بانک چیس** (Chase Bank) برای یک حساب در معرض خطر بنویسد، این نامه را ارائه کرد:

موضوع: مهم: حساب شما در بانک چیس به خطر افتاده است

[نام] عزیز،

امیدواریم این ایمیل برای شما خوب باشد. سوابق نشان می‌دهد که فعالیت مشکوکی در حساب شما در بانک چیس شما وجود داشته است.

امنیت حساب شما را بسیار جدی می‌گیریم و می‌خواهیم برای جلوگیری از هرگونه تراکنش غیرمجاز بعدی اقدام فوری انجام دهیم.

جزئیات فعالیت مشکوک:

تاریخ: [درج تاریخ]

مکان: [درج مکان]

مبلغ: [درج مقدار]

لطفاً توجه داشته باشید که این فعالیت ممکن است بدون اطلاع یا مجوز شما انجام شده باشد. اقدامهایی را برای ایمن‌سازی حساب شما و جلوگیری از هرگونه تراکنش غیرمجاز بعدی انجام دادیم.

اهمیت دارد که برای ایمن‌سازی حساب خود اقدام فوری انجام دهید. لطفاً در اسرع وقت با [درج شماره تماس چیس] با ما تماس بگیرید تا مشکل را گزارش کنید. تیم اختصاصی ما ۲۴ ساعته برای کمک به شما در دسترس هستند. ما برای هرگونه مشکلی که ممکن است ایجاد کرده باشیم، عذرخواهی می‌کنیم و از توجه سریع شما به این موضوع سپاسگزاریم. اگر پرسش یا ابهامی در این زمینه دارید، لطفاً با ما تماس بگیرید.

با احترام، تیم امنیتی چیس بانک

کیفیت ایمیل کلاهبردارانه بیش از یک دهه است که ارتقا یافته، اما چت جی‌پی‌تی تعداد کمی از هشدارهای خطر باقی‌مانده را که بسیاری برای تشخیص ایمیل‌های کلاهبردارانه از اطلاع‌رسانی داخلی به آن‌ها تکیه کرده‌اند، از بین برده است. چت جی‌پی‌تی خطاهای دستور زبانی و تفاوت‌های ظریف را که نشان دهد ایمیل‌ها از کشورهای دیگر یا توسط کسانی که زبان دوم آن‌ها انگلیسی است نوشته شده است را حذف می‌کند. البته این موضوع برای همه زبانهایی که چت جی‌پی‌تی استفاده می‌کنند، صادق است.

بیشترین هدف ایمیل کلاهبردارانه، ترغیب گیرندگان به کلیک‌کردن روی لینکها است. چت جی‌پی‌تی می‌تواند به ایجاد این لینکها و کدهای مخرب درون آن‌ها کمک کند. (به

نرم‌افزار (به مطلب «مجرمان سایبری شروع به استفاده از چت جی‌پی‌تی» مراجعه کنید، چک پوینت، ۶ ژانویه ۲۰۲۳) مراجعه کنید). با این حال، اکنون، به نظر می‌رسد که مجرمان سایبری با استفاده از محبوبیت بسیار زیاد ابزار هوش مصنوعی برای ترغیب کاربران به کلیک روی سایتهای نادرست چت جی‌پی‌تی، از رویکرد ساده‌تر و سنتی‌تر برای نصب بدافزار از طریق چت جی‌پی‌تی استفاده کرده‌اند. (به مطلب «هکرها از برنامه‌های جعلی چت جی‌پی‌تی برای به‌روزرسانی ویندوز و بدافزار اندروید استفاده می‌کنند» توسط بیل تولاس (Bill Toulas) بلپینگ کامپیوتر (Bleeping Computer) ۲۲ فوریه ۲۰۲۳ مراجعه کنید).

بدافزارها، پس از شناسایی، به‌طور معمول از طریق اسکن سریع سامانه‌ها و افزون بر آن، به‌روزرسانی نرم‌افزاری حذف می‌شوند. در نتیجه، مجرمان سایبری بیشتر اوقات تنها می‌توانند پیش از نوشتن کد جدید به چند هدف ضربه بزنند. اما ابزار هوش مصنوعی، مانند چت جی‌پی‌تی می‌تواند که بدافزار چندشکلی را ارائه دهند که با شکل‌گیری یا تغییر ظاهر آن از شناسایی جلوگیری کنند.

از آنجایی که هوش مصنوعی هنگام آموزش توسعه پیدا می‌کند و نیازی به استراحت ندارد، می‌تواند بدافزاری ایجاد کند که همیشه در حال تکامل و به‌روزرسانی است و توقف آن را بسیار دشوارتر می‌کند. افزون بر این، هوش مصنوعی همچنان با افزایش تولید محتوا در حال آموزش است که منجر به ایجاد کدهای پیچیده‌تری می‌شود که کارشناسان امنیت سایبری در پیشگیری و شناسایی را با مشکلات بیشتری مواجه خواهد کرد.

موسسه این‌ای‌آی تلاش کرده که از استفاده نادرست از چت جی‌پی‌تی جلوگیری کند. به‌عنوان نمونه، این شرکت ابزار **دستیار متن و نوشتار** (AI Text Classi) را راه‌اندازی کرد؛ ابزار جدیدی برای کمک به کاربرانی (همانند معلمان) که نگران تقلب هستند، برای این‌که تمایز بین متن نوشته شده توسط انسان و هوش مصنوعی را تشخیص دهند. چت جی‌پی‌تی همچنین به‌طور مستقیم به پرسشهای کاربران در انجام اقدامهای غیرقانونی یا غیراخلاقی همانند پرسشهایی در مورد ساخت بمب یا ایجاد ایمیل کلاهبردارانه پاسخ نمی‌دهد.

هر شخصی می‌تواند از چت جی‌پی‌تی

برای توضیح مفاهیم

ساده و پیچیده و کمک به

نوشتن رزومه

شرح زندگی

آهنگ

لطایف و وبلاگ استفاده کند

مقاله «هوش مصنوعی می‌تواند مشکلی را حل کند یا آن را هک کند» توسط **شارون بن‌موشه** (Sharon Ben-Moshe) **گیل گکر** (Gil Gekker) و **گولان کوهن** (Golan Cohen)، چک پوینت، ۱۹ دسامبر ۲۰۲۲ مراجعه کنید). در نامه جعلی از چیس در بالا، به‌گیرنده دستور داده شد که تماس بگیرد و شاید این روش برای کلاهبرداران موفقیت‌آمیزتر باشد، زیرا امروزه بسیاری از مردم به‌روش کلاهبرداری «اینجا کلیک کنید» آگاه هستند. متأسفانه، آسان شدن روشی که کلاهبردار امروز بتواند یک شماره تلفن را جعل کند، ممکن است رویکرد «لطفاً با ما تماس بگیرید...» را بسیار اثربخش کند.

ایجاد بدافزار و ویروس

همانطور که در مطالب اولیه دیدید، صحبت در میان کلاهبرداران در مورد نحوه استفاده از چت جی‌پی‌تی برای ایجاد بدافزار و سایر برنامه‌های مخرب، بلافاصله پس از راه‌اندازی آن در نوامبر سال گذشته در هم‌نشینیهای جنایی آشکار شد. کلاهبرداران نحوه کمک از چت جی‌پی‌تی را برای همکاران خود به اشتراک می‌گذاشتند؛ همانند نوشتن کد برای سرقت داده‌ها و راه‌های نصب درهای پشتی روی

داشته باشید که این اسکرپت، فایل یا پوشه اصلی را با داده‌های رمزگذاری شده بازنویسی می‌کند، بنابراین حتما پیش از اجرای آن، از داده‌های خود یک نسخه پشتیبان تهیه کنید. همچنین، باید کلید را در جای امنی نگه دارید؛ زیرا پس از این برای رمزگشایی داده‌ها به آن نیاز خواهید داشت.

شکل ۱- نمونه درخواست چت جی‌پی‌تی برای درخواست رمزگذاری

```
python copy code

from cryptography.fernet import Fernet
import os

# Generate a new key
key = Fernet.generate_key()

# store the key in a file for safekeeping
with open('key_key', 'wb') as key_file:
    key_file.write(key)

# Load the key from the file
with open('key_key', 'rb') as key_file:
    key = key_file.read()

# Define a function to encrypt a file
def encrypt_file(filename, key):
    with open(filename, 'rb') as file:
        data = file.read()

    fernet = Fernet(key)
    encrypted = fernet.encrypt(data)

    with open(filename, 'wb') as encrypted_file:
        encrypted_file.write(encrypted)

# Define a function to encrypt a folder
def encrypt_folder(folder, key):
    for dirpath, dirnames, filenames in os.walk(folder):
        for filename in filenames:
            file_path = os.path.join(dirpath, filename)
            encrypt_file(file_path, key)

# Encrypt a file or folder
file_or_folder = '/path/to/file/or/folder'
if os.path.isfile(file_or_folder):
    encrypt_file(file_or_folder, key)
elif os.path.isdir(file_or_folder):
    encrypt_folder(file_or_folder, key)
```

پرداخت به موقع ارزهای دیجیتال برای بازارهای دارکوب

کلاهبرداران و مجرمان سایبری از جمله اولین افرادی بودند که به دلیل ناشناس بودن و نبود مقررات برای ارز دیجیتال، از آن استقبال کردند. اما همچنان به مهارت‌های درخور توجهی برای ایجاد بازارهای دارکوب با قابلیت پرداخت نیاز داشتند. چک پوینت کلاهبردارانی را در هم‌نشینیها پیدا کرد که اطلاعاتی در این باره به اشتراک گذاشتند که خیلی راحت از چت جی‌پی‌تی برای ایجاد بازارهای دارکوب و دریافت قیمت‌های ارزهای دیجیتال از طریق یک زبان برنامه‌نویسی عمومی (PHP) به جای زبان برنامه پیچیده‌تر مانند پایتون یا جاوا

اما هیچ یک از این کنترلرها بی‌خطا نیستند و نمی‌توانند مانع استفاده کسی از چت جی‌پی‌تی برای تولید بدافزارهای مخرب شوند. روزنامه‌نگاران یک وبگاه اخبار فناوری، به‌سادگی از چت جی‌پی‌تی خواستند تا یک اسکرپت برای شناسایی اطلاعات کارت اعتباری و ارسال آن به یک مکان واحد ایجاد کند، و او دقیقاً این کار را انجام داد. (به مقاله «ربات چت جی‌پی‌تی جدید موسسه اپن‌ای‌آی: ۱۰ کار خطرناکی که قادر به انجام آن است» توسط **شارما (Ax Sharma)**، بلیینگ کامپیوتر، ۶ دسامبر ۲۰۲۲؛ «طبقه‌بندی جدید هوش مصنوعی برای نمایش متن نوشته‌شده با هوش مصنوعی» توسط **هندریک کرشنر (Jan Hendrik Kirchner)**، **لاما احمد (Lama Ahmad)**، **اسکات آرونسون (Scott Aaronson)**، **یان لیکه (Jan Leike)** موسسه اپن‌ای‌آی، ۳۱ ژانویه ۲۰۲۳ و «آیا اپن‌ای‌آی پیش از این کنترل چت جی‌پی‌تی را از دست داده است؟» توسط **ماکسول تیموتی (Maxwell Timothy)**، **ام‌یو (MUO)**، ۱۱ فوریه ۲۰۲۳ مراجعه کنید)

رمزگذاری و رمزگشایی داده‌ها

چت جی‌پی‌تی می‌تواند کد رمزگذاری و رمزگشایی بنویسد که کلاهبرداران می‌توانند از آن برای باج‌افزار و سرقت داده‌های محافظت‌شده (رمزگذاری شده) استفاده کنند. من از چت جی‌پی‌تی خواستم که یک اسکرپت پایتون (Python) یک زبان برنامه‌نویسی) برای رمزگذاری هارد دیسک روی لپ‌تاپ بنویسد و آنچه که در شکل ۱ آمده است، به همراه نظرات اضافه زیر را ارائه داد:

«به‌عنوان یک مدل زبان هوش مصنوعی، نمی‌توانم عملیاتی را روی سخت‌افزار فیزیکی انجام دهم، اما می‌توانم یک اسکرپت ساده در پایتون برای رمزگذاری محتویات یک فایل یا پوشه در کتابخانه رمزنگاری در پایتون برای رمزگذاری و رمزگشایی داده‌ها با استفاده از رمزگذاری متقارن ارائه کنم.

برای استفاده از این اسکرپت، کافی است مسیر «فایل یا پوشه» را با مسیر فایل یا پوشه‌ای که می‌خواهید رمزگذاری کنید، جایگزین و اسکرپت را اجرا کنید. اسکرپت یک کلید جدید تولید، آن را در یک فایل ذخیره و سپس از آن برای رمزگذاری محتویات فایل یا پوشه مشخص‌شده، استفاده می‌کند. توجه

می‌توانند از چت جی‌پی‌تی برای استفاده مکرر از محتوا استفاده کنند. در ۳۰ تانیه، چت جی‌پی‌تی می‌تواند محتوای جدید و منحصر به فردی برای هر سایت ایجاد کند و آن را واقعی‌تر نشان دهد.

سرعتی که چت جی‌پی‌تی می‌تواند این نمایه‌های متقاعدکننده و فریبنده منحصر به فرد را تولید کند، می‌تواند این کلاهبرداری را اندکی تلاش به یک بازی اعداد ساده برای کلاهبرداران تبدیل کند.

دیپ‌فیکها (Deepfakes) همراه با جعل صدا، یکی دیگر از راه‌های نگران‌کننده کلاهبرداران است که از هوش مصنوعی برای کلاهبرداری از قربانیان استفاده می‌کنند. در یکی از موارد اخیر که در واشنگتن پست گزارش شد، کلاهبرداران یک زوج مسن در کانادا را فریب دادند که پس از استفاده از هوش مصنوعی برای تقلید صدای نوه‌شان که برای نجات از زندان درخواست کمک می‌کرد، پول بفرستند. طبق این مقاله، کلاهبرداران فقط به نمونه‌های صوتی کوتاهی نیاز دارند که از مطالب سایتهای رسانه‌های اجتماعی مانند **تیک تاک (TikTok)** یا **فیس بوک (Facebook)** گرفته شده‌اند تا بتوانند کار کنند.

ویدیوی ساخته‌شده توسط هوش مصنوعی از **مورگان فریمن (Morgan Freeman)** بازیگر که اواخر سال گذشته در فضای مجازی منتشر شد، شاید حتی وحشتناک‌تر باشد. این ویدیو به قدری واقعی بود که اکنون افراد بیشتری در مورد نحوه استفاده از این فناوری برای اهداف مخرب در آینده نزدیک نگران هستند. (مقاله «آن‌ها فکر کردند که عزیزانشان کمک می‌خواهند، این یک کلاهبرداری با هوش مصنوعی بود.»، توسط **پرانشو ورما (Pranshu Verma)**، واشنگتن پست، ۵ مارس ۲۰۲۳ و «این ویدیوی ساختگی ترسناک واقعگرایانه در توئیتر وحشت به پا کرده است»، توسط **دانیل پایپر (Daniel Piper)** دسامبر ۱۹، ۲۰۲۲ را مطالعه کنید.)

خطرهای پیش‌رو

نمونه‌های قبلی روشهایی هستند که متقلبان، کلاهبرداران و مجرمان سایبری پیش از این از چت جی‌پی‌تی استفاده می‌کردند یا با آن آزمایش می‌کردند و آن‌ها روزانه راهکارهای

اسکرپیت استفاده کردند (به مطالب «مجرمان سایبری اکنون از چت جی‌پی‌تی برای مالکیت شما استفاده می‌کنند» نوشته **درک بی. جانسون (Derek B. Johnson)** ۶ ژانویه ۲۰۲۳ و «مجرمان سایبری شروع به استفاده از چت جی‌پی‌تی کردند، چک پوینت، ۶ ژانویه ۲۰۲۳ مراجعه کنید).

کلاهبرداری عاشقانه

این‌که کلاهبردارانی که از هوش مصنوعی یا رباتها با حفظ نمایه‌های متعددی از خود برای کلاهبرداری عاشقانه استفاده می‌کنند نیز مفهوم جدیدی نیست، اما بیشتر اوقات پیامها یکنواخت و فاقد محتوا هستند و به اهداف مورد نظر اشاره می‌کنند. می‌توان به چت جی‌پی‌تی دستور داد که لحن پیامها را تغییر دهد تا آن‌ها را جذاب‌تر یا عاشقانه‌تر کند. این امر به کلاهبرداران اجازه می‌دهد تا نیم‌رخهای متعددی را اجرا کرده و قربانیان احتمالی بیشتری را با اطلاعات بسیار کم مورد هدف قرار دهند، هیچ اطلاعات اضافی فراتر از درخواست اصلی به چت جی‌پی‌تی ارائه نشد، اما به‌طور مستقل جزئیات مربوط به علایق و ویژگیهای مورد نظر را طراحی کرد.

وقتی از او درخواست شد که نسخه‌ای برای سبک زندگی شهری ایجاد کند، متن شکل ۲ را دوباره در کمتر از ۳۰ ثانیه ارائه کرد.

سرعتی که چت جی‌پی‌تی می‌تواند این نمایه‌های متقاعدکننده و فریبنده منحصر به فرد را تولید کند، می‌تواند کلاهبرداری عاشقانه را با اندکی تلاش به یک بازی اعداد ساده برای کلاهبرداران تبدیل کند.

یکی از علایم خطر در کلاهبرداری عاشقانه، شباهت بین چندین نمایه با تصاویر و نامهای متفاوت است. اما کلاهبرداری عاشقانه، تنها نوع کلاهبرداری نخواهد بود که توسط چت جی‌پی‌تی فعال شده است که در آن محتوای منحصر به فرد موجب کاهش یا حذف آن‌ها می‌شود. کلاهبرداری در خرید برخط، به‌طور درخور توجهی در دو سال گذشته افزایش یافته است، که به‌طور عمده به دلیل همه‌گیری است. یکی از علایم خطر برای ده‌ها سایت کلاهبردار، شباهتها و محتوای کپی شده از یک سایت به سایت دیگر بود. اما اکنون کلاهبرداران

دست بدهیم و در صورت شکست سیستم هوش مصنوعی، آسیب‌پذیر شویم.

این تهدیدهای احتمالی، اهمیت توسعه و استقرار هوش مصنوعی و نیاز به مقررات و نظارت مناسب برای اطمینان از همسویی هوش مصنوعی با ارزشها و اولویتهای انسانی را پررنگ می‌کند.

اکنون اخبار خوب

اما یک خبر خوب وجود دارد؛ کلاهبرداران می‌توانند از چت جی‌پی‌تی هم به‌طور بسیار کارآمد استفاده کنند.

از این دستیار می‌توان موارد زیر را درخواست کرد:

۱- فهرستی از فعالیتهای پیشگیری و کشف تقلب ویژه صنعت و فرایند.

۲- نمونه‌هایی از نحوه استفاده از هوش مصنوعی برای ارتکاب کلاهبرداری و اقدامهای لازم برای جلوگیری از آن.

۳- فهرستی از اقدامهایی که حساب‌برسان داخلی باید در برنامه‌های کشف تقلب در حین حسابرسی لحاظ کنند.

۴- روندهای تقلب و نحوه محافظت در برابر آنها.

۵- فهرستی از راه‌هایی که می‌توان از هوش مصنوعی در مبارزه با تقلب استفاده کرد. موارد پیشنهادی عبارتند از:

الف- شناسایی الگوها و ناهنجاریها در داده‌ها.

ب- تشخیص خودکار تقلب.

جدیدی را کشف و به‌اشتراک می‌گذاشتند. وقتی از چت جی‌پی‌تی پرسیدم که بزرگترین تهدید هوش مصنوعی برای انسان چیست، پاسخ داد:

”چندین تهدید احتمالی توسط هوش مصنوعی برای انسان وجود دارد، از جمله:

۱- جابجایی شغل: هوش مصنوعی می‌تواند زمینه خودکارشدن بسیاری از مشاغل را فراهم و نیروی انسانی را از کار بیکار کرده و منجر به بیکاری گسترده شود.

۲- تعصب و تبعیض: هوش مصنوعی تنها به‌ازای داده‌هایی که روی آنها آموزش دیده‌اند، بی‌طرف هستند و اگر این داده‌ها سوگیریهای انسانی را بازتاب دهند، هوش مصنوعی آنها را تکرار خواهد کرد.

۳- ایمنی و کنترل: با هوش مصنوعی می‌توان برنامه‌ریزی یا هک را انجام داد که به انسان آسیب برساند یا تصمیم‌هایی غیراخلاقی یا زیانبار بگیرد.

۴- تجاوز به حریم خصوصی: هوش مصنوعی می‌تواند مقادیر زیادی از داده‌های شخصی را پردازش کند، که می‌تواند برای تجاوز به حریم خصوصی افراد یا سوءاستفاده از اطلاعات آنها استفاده شود.

۵- وابستگی به فناوری: همانطور که برای تصمیم‌گیری و سایر وظایف به هوش مصنوعی وابسته می‌شویم، ممکن است مهارتها و تواناییهای انجام این کارها را خودمان از

شکل ۲- نسخه چت جی‌پی‌تی برای سبک زندگی شهری

MB

Can we create a profile for an urban lifestyle?



Absolutely, here's a sample profile that highlights an urban lifestyle:

Hey there, I'm an urbanite through and through! I live for the hustle and bustle of the city and all the excitement that comes with it.

During the day, you'll find me working as a marketing executive at a top agency downtown. But when the sun goes down, I'm all about exploring the city's vibrant nightlife scene. From speakeasies to rooftop bars, I love trying out new spots and finding hidden gems.

When I'm not working or out on the town, I like to stay active by running through the city's streets and parks. I'm also a bit of a foodie and love trying out new restaurants and cuisines.

I'm looking for someone who shares my passion for city living and can keep up with my fast-paced lifestyle. Someone who's confident, ambitious, and isn't afraid to take risks. Bonus points if you can make me laugh and have a sense of adventure!

If you're ready to explore the city with me, shoot me a message and let's see where it takes us.

۹- مراقب تماسهای تلفنی ناخواسته باشید. اگر شخصی با شما تماس گرفت و شماره تامین اجتماعی شما را درخواست کرد، وقت آن است که تلفن را قطع کنید.

۱۰- در نهایت به یاد داشته باشید که کلاهبرداران بسیار خلاق هستند. آنها همیشه با کلاهبرداریهای جدید می‌آیند. اما اگر از عقل سلیم خود استفاده کرده، هوشیار باشید و حس شوخ طبعی خود را حفظ کنید، آنگاه یک قدم جلوتر از آنها خواهید بود.

مجرمان سایبری از چت جی‌پی‌تی برای کاهش بار کاری خود و خودکارسازی برنامه‌های خود استفاده می‌کنند. اما خبر خوب اینجاست.

شاید آنها ندانند که دستیار سخنگو به‌طور معمول اطلاعات ۱۰۰ درصد دقیقی را منتشر می‌کند؛ به‌ویژه اگر کلاهبرداران در مورد برخی از موضوعها آگاهی یا تجربه‌ای نداشته باشند. کاربران باهوش بیشتر اوقات می‌توانند خطاهای چت جی‌پی‌تی را شناسایی و برنامه‌ها را تشخیص دهند. دانش یک قدرت است (توانا بود هر که دانا بود).

استفاده مناسب از چت جی‌پی‌تی و نه استفاده نامناسب از آن، شاید دروازه جدیدی برای کلاهبردارانی خواهد بود که نمی‌توانند همان برنامه‌ها را اجرا کنند؛ زیرا پیش از این، مهارت‌های مربوط به جرایم سایبری را یاد نگرفته‌اند. همانطور که فناوری گذشته، فرصتهای جدید کلاهبرداری را از طریق پیامدهای پیش‌بینی نشده و ناخواسته برای آنها ایجاد کرد، چت جی‌پی‌تی نیز همینطور خواهد بود. با این حال، به دلیل سروصدای رسانه‌ای که چت جی‌پی‌تی ایجاد کرده است، بسیاری از کلاهبرداران از قابلیت‌های آن آگاه هستند. اکنون می‌توانیم از چت ربات زیرکانه و سایر ابزار هوش مصنوعی برای مقابله با آن استفاده کنیم.

پانویس:

1- Dark web

منبع:

• Is ChatGPT the Newest Gateway to Fraud?. <https://www.fraud-magazine.com/May/June/2023>

ج- تحلیل پیش‌بینی کننده.
د ارزیابی ریسک پیشرفته.
ه. بهبود تجربه مشتری.
و. ساده‌سازی بازرسیها.

۶- در آموزش به‌منظور آگاهی درباره تقلب در سازمان کمک کنید. وقتی از چت جی‌پی‌تی خواستم که پیامهای طنز و به‌یادماندنی برای آموزش آگاهی از کلاهبرداری و پوششهای پیام ایجاد کند، مطالبی را ارائه کرد:

”بی‌شک در اینجا ده نکته پیشگیری و کشف تقلب وجود دارد که در قالب طنز بیان شده است:

۱- رمز عبور خود را به هیچکس حتی مادرشوهرتان ندهید. شاید او فردی خوب به‌نظر آید، اما او آنقدرها هم خوب نیست.
۲- همیشه قبل از کلیک روی یک لینک ارسالی در ایمیل، دوباره آن را بررسی کنید. شما نمی‌خواهید کار شما با ویگاهی «درمانهای معجزه‌آسا» برای طاسی سر به شما می‌فروشد، تمام شود.

۳- اگر غریبه‌ای فرصت سرمایه‌گذاری «یک بار در زندگی» را به شما داد، احتمال دارد که به‌دلیلی «آخرین فرصت زندگی» باشد. از آن فرار کن!

۴- شاید بهتر از آن به‌نظر می‌رسد که واقعی باشد؛ شاید همینطور است. متاسفم، اما شما یک سفر دریایی رایگان به کاراییب به‌خاطر ثبت نام یک کارت اعتباری دریافت نمی‌کنید.
۵- هنگام استفاده از شبکه بی‌سیم عمومی مراقب باشید. مردی که در استارباکس کنار شما نشسته است، ممکن است سعی کند اطلاعات شخصی شما را بدزدد، همچنین کیک شما را.

۶- حساب بانکی خود را مرتب چک کنید. شما نمی‌خواهید بفهمید که نامزد سابقتان، حساب شما را خالی کرده است تا هزینه کلاسهای یوگای حیوان خانگی خود را تامین کند.

۷- نرم‌افزار ضدویروس خود را به‌روز نگه دارید؛ شما که نمی‌خواهید مسئول رهاکردن انبوهی از زامبیهای دیجیتال در جهان باشید.

۸- گرفتار کلاهبرداری با پیام “از مایکروسافت تماس می‌گیریم، یک ویروس در رایانه شما وجود دارد” نشوید. آنها از مایکروسافت تماس نمی‌گیرند، از زیرزمین خانه مادرشان زنگ می‌زنند.

