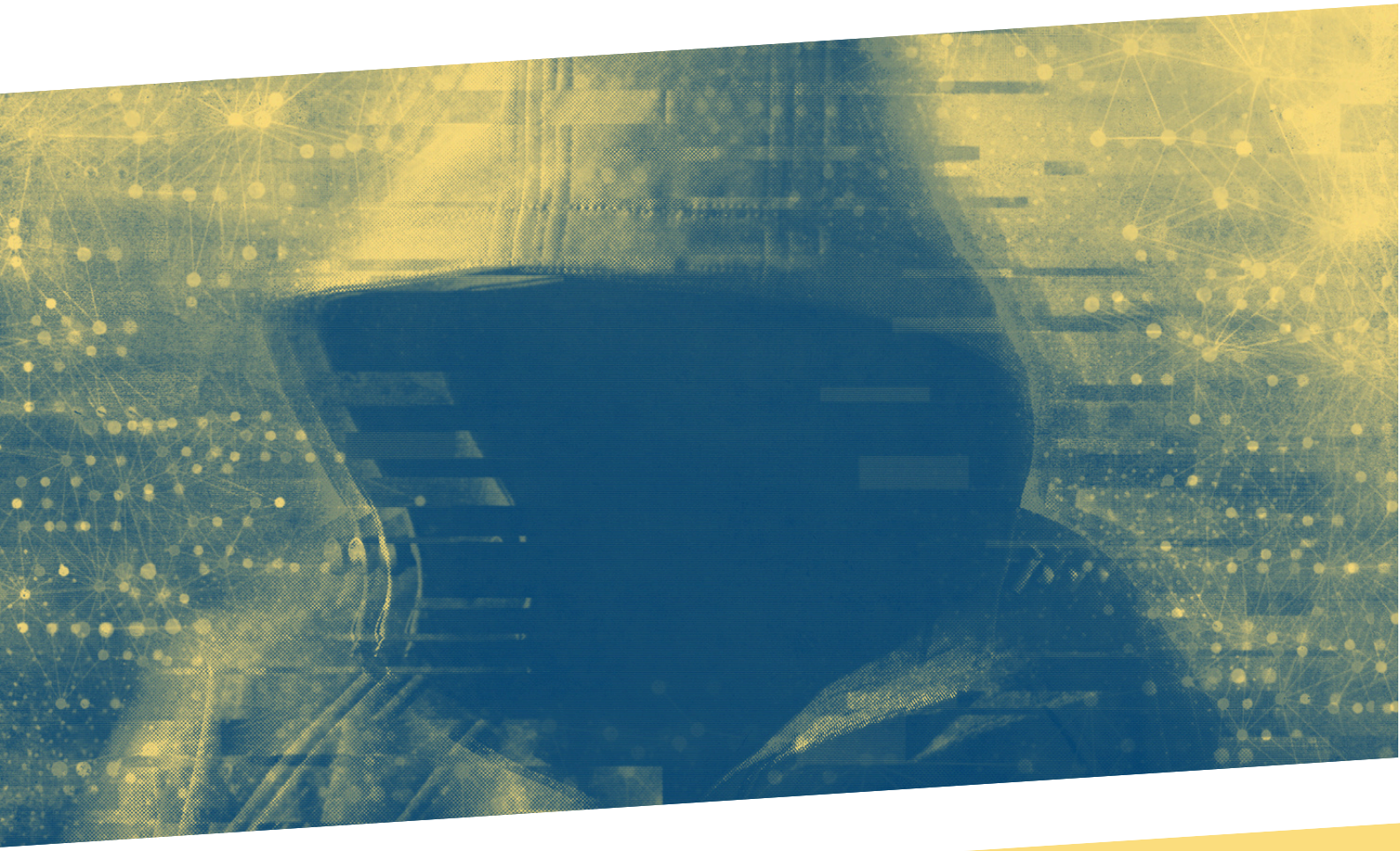
IA E GIOVANI CONSUMATORI
Educazione e Diritti a Portata di Click

U.Di.Con.
UNIONE per la DIFESA dei CONSUMATORI
Lazio



I rischi poco evidenti dell'IA: truffe più comuni e sistemi automatizzati

Strumenti e diritti per un uso sicuro dell' IA

REGIONE LAZIO

Iniziativa finanziata dal fondo Regione Lazio per i consumatori – anno 2024

Indice

Introduzione

L'intelligenza artificiale sta trasformando molti aspetti della nostra quotidianità, ma il suo utilizzo presenta anche nuove sfide per i consumatori. I criminali informatici sfruttano l'IA per rendere più sofisticate truffe come il phishing avanzato, i deepfake vocali e le frodi negli investimenti online, rendendo più difficile distinguere il vero dal falso.

Parallelamente, l'uso crescente di chatbot e assistenti virtuali nei servizi clienti e nel supporto legale può complicare la risoluzione di problemi, limitando il contatto umano e riducendo la possibilità di contestare decisioni automatizzate.

Questa guida ti aiuterà a riconoscere i rischi legati all'IA e ai sistemi automatizzati, fornendoti strumenti pratici per proteggerti e far valere i tuoi diritti di consumatore.

IA e cybercriminalità

Sebbene l'intelligenza artificiale rappresenti uno strumento di innovazione, può facilmente diventare un'arma potente nelle mani dei criminali informatici. Oggi, le truffe digitali sono diventate sempre più sofisticate e difficili da riconoscere grazie all'IA avanzata. Tra queste troviamo ad esempio le truffe realizzate con i deepfake, una tecnologia basata sull'intelligenza artificiale che consente di creare contenuti audiovisivi in modo estremamente realistico, sostituendo volti, voci o movimenti con quelli di altre persone. Il deepfake vocale, quello che riproduce fedelmente la voce di una persona, dal tono all'inflessione, e che viene creato attraverso algoritmi di apprendimento automatico che analizzano campioni audio da messaggi vocali o video sui social, è attualmente il sistema più utilizzato per scopi fraudolenti. Le truffe telefoniche ne sono un esempio e vengono utilizzate con lo scopo di ingannare le persone e sottrarre loro denaro o dati sensibili.

Anche il phishing, tipologia di truffa che può portare al furto di informazioni private e di denaro e che si concretizza attraverso l'invio di messaggi di posta elettronica ingannevoli, è diventato sempre più sofisticato grazie all'uso dell'intelligenza artificiale. Se un tempo, queste mail erano maggiormente riconoscibili per errori grammaticali, traduzioni approssimative, loghi poco definiti, oggi l'IA permette di creare messaggi perfettamente scritti e personalizzati, capaci di imitare lo stile comunicativo di aziende affidabili. In questo modo, anche le truffe di phishing diventano più autentiche e particolarmente difficili da riconoscere, esponendo gli utenti a un maggiore rischio di essere ingannati e di condividere, senza volerlo, dati sensibili o informazioni personali.

E ancora, sempre più diffuso il falso trading online. Si tratta di una truffa finanziaria attraverso la quale si promettono alla vittima elevati guadagni grazie all'uso di algoritmi avanzati di intelligenza artificiale. La truffa inizia con un contatto attraverso telefonate, social network o siti di incontri, dove la vittima viene persuasa a fornire i propri dati personali. Un truffatore, spacciandosi per un broker esperto, la convince a effettuare un primo investimento di piccola entità, promettendo guadagni elevati. In breve tempo, la vittima viene indotta a investire somme maggiori, credendo che il proprio capitale stia crescendo rapidamente. Nella fase finale, quando tenta di prelevare il denaro, le viene richiesto di pagare presunti "costi di sblocco". A quel punto, però, i fondi risultano irrecuperabili e la piattaforma scompare nel nulla.

Segnali di truffe basate su IA

Chiamate sospette da familiari o conoscenti

Potrebbe capitare di ricevere una telefonata da un parente stretto che, con tono preoccupato, chiede aiuto immediato. Questo potrebbe essere il caso di un deepfake vocale, un file audio realizzato con un campione della voce estratto da un messaggio vocale o da un video sui social.

A cosa bisogna fare attenzione?

Al tono della voce preoccupato e affrettato, al ritmo della voce che potrebbe risultare robotico o meccanico, alle parole che potrebbero suonare tagliate o enfatizzate in modo innaturale;

Alla richiesta di invio di denaro, in particolare alla richiesta di effettuare il pagamento su un IBAN diverso dal solito o di utilizzare metodi di pagamento alternativi come criptovalute o buoni regalo, oppure di usare servizi non tracciabili come le carte prepagate.

All'insistenza del richiedente di effettuare l'operazione immediatamente.

All'incapacità dell'interlocutore di rispondere a domande specifiche e alla ripetizione di frasi in modo innaturale.

E come difendersi?

Se ricevi una chiamata inaspettata con una richiesta di aiuto particolarmente urgente, non prendere decisioni affrettate;

Se ricevi chiamate da un presunto operatore bancario che richiede dati sensibili come il numero della carta di credito o la password, potrebbe trattarsi di una truffa. Nessun istituto di credito richiede queste informazioni telefonicamente. Interrompi la chiamata e contatta direttamente l'ente attraverso i propri canali ufficiali;

Non fidarsi della richiesta di inviare urgentemente denaro;

Provare a identificare la persona che pensi stia chiamando attraverso altre modalità, ad esempio attraverso una videochiamata o un messaggio;

Non rispondere ai numeri sconosciuti o alle chiamate internazionali, sarebbe opportuno cercarli online prima di richiamare;

Utilizzare strumenti per identificare chiamate sospette come le app per il blocco degli spam e bloccare i numeri sospetti.

Email di phishing create con IA, come difendersi?

Nonostante oggi sia più complicato riconoscere le mail di phishing grazie all'uso dell'intelligenza artificiale generativa in grado di crearle perfettamente scritte e personalizzate, non mancano modi per proteggersi da questa tipologia di truffa:

Fare attenzione a richieste inusuali, come richiesta di dati sensibili (es. richiesta password del conto corrente bancario);

Fare attenzioni a richieste urgenti, come l'aggiornamento delle password o di dati in generale o risoluzione di un problema immediato;

Non cliccare sui link presenti nel corpo della mail. Il rischio è quello di installare sul dispositivo un malware che potrebbe impadronirsi dei dati personali;

Verificare sempre l'indirizzo del mittente e confrontarlo con quello ufficiale.

Falso trading online, come riconoscerlo?

Le truffe legate al trading online sfruttano tecniche di manipolazione psicologica e strumenti di intelligenza artificiale per apparire credibili. Per evitare di cadere in questi inganni, è fondamentale riconoscere alcuni segnali d'allarme:

Promesse di guadagni elevati e sicuri

Nessun investimento è privo di rischi. Se una piattaforma garantisce profitti elevati e costanti, è probabile che si tratti di una truffa.

Siti e broker non regolamentati

Verifica sempre che la piattaforma sia registrata presso autorità finanziarie ufficiali, come la CONSOB in Italia. Diffida dei siti con nomi simili a quelli di istituzioni affidabili.

Pressioni per investire velocemente

I truffatori usano spesso tecniche di urgenza, come "offerte esclusive" o "posti limitati", per spingere le vittime a depositare denaro senza riflettere. Rendimenti fasulli mostrati sulla piattaforma - In molti casi, i truffatori manipolano i dati sulla dashboard dell'utente, facendo apparire falsi guadagni per convincere la vittima a investire di più.

Difficoltà a prelevare i fondi

Se una piattaforma impone costi di sblocco, ritardi ingiustificati o chiede ulteriori pagamenti per il ritiro dei fondi, è un chiaro segnale di truffa.

Recensioni negative e segnalazioni online

Prima di investire, cerca opinioni su forum finanziari affidabili o siti di tutela dei consumatori. Se una piattaforma ha molte segnalazioni di frode, evita di usarla.

Rischi dell'IA nei servizi automatizzati

L'uso sempre più frequente di chatbot e assistenti virtuali per la gestione del servizio clienti sta trasformando il modo in cui i consumatori si relazionano con le aziende e le istituzioni. Sebbene questi strumenti permettano di gestire richieste semplici in modo rapido e di ricevere risposte immediate, dall'altro presentano limiti significativi che possono compromettere l'accesso a un'assistenza adeguata. Uno dei rischi principali è la mancanza di comprensione delle richieste più complicate. Nel caso in cui un consumatore avesse un problema più complesso, come una contestazione bancaria o la richiesta di una modifica contrattuale, le chatbot, operando su modelli predefiniti basati su parole chiave, potrebbero non fornire risposte esaustive, non indirizzare il consumatore verso la giusta soluzione e, di conseguenza, non offrire un reale supporto. E ancora, molte aziende strutturano il proprio servizio clienti al fine di limitare il contatto diretto con un consulente, spingendo all'uso di sistemi automatizzati. La mancanza di un contatto umano, con un operatore reale, potrebbe impedire la risoluzione di problemi più urgenti o semplicemente di fare valere i propri diritti di consumatore e, in settori come la sanità, finanza e assistenza legale, dove è necessaria un'assistenza personalizzata, potrebbe rappresentare una criticità. Le chatbot non sono sistemi infallibili, potrebbero commettere errori provocando gravi conseguenze a coloro che si affidano a eventuali risposte non propriamente corrette. L'eccessivo utilizzo di sistemi automatizzati potrebbe compromettere la qualità del servizio in termini di mancata fiducia dei consumatori verso aziende o istituzioni. Se un utente si trova davanti a un problema complesso e non riesce a ricevere il supporto adeguato da una chatbot potrebbe sentirsi trascurato e di conseguenza potrebbe percepire il servizio clienti poco affidabile e poco efficiente, riducendo la credibilità del fornitore.

Come riconoscere queste situazioni e come proteggersi?

1. Verificare se un servizio si affida a un algoritmo per valutare le richieste degli utenti. È possibile controllare queste informazioni nei termini di servizio e nelle policy della privacy e cercare se viene menzionato l'uso di decisioni automatizzate. In caso contrario potrebbe esserci un problema di trasparenza

2. Nell'eventualità una chatbot non riesce a dare risposte adeguate a una richiesta particolarmente complessa, controllare se esiste un'opzione per parlare con un operatore umano cercando numeri di telefono o mail ufficiali sul sito dell'azienda di riferimento

3. Quando un algoritmo prende decisioni che ci riguardano, presentate come definitive, è possibile chiedere spiegazioni in merito ai criteri utilizzati per la scelta definitiva, richiedendo possibilmente l'intervento di una revisione umana

Riferimenti normativi sull'Intelligenza artificiale

L'intelligenza artificiale è in continua evoluzione e, di conseguenza, anche le normative e le raccomandazioni per la tutela dei consumatori. Di seguito alcune fonti a cui fare riferimento:

AI Act – Regolamento Europeo sull'Intelligenza Artificiale regolamento (UE) 2024/1689

è il primo quadro giuridico globale in assoluto a livello mondiale e ha l'obiettivo di promuovere un'IA affidabile in Europa stabilendo un quadro normativo chiaro per l'uso sicuro ed etico di questo strumento. Classifica i sistemi di intelligenza artificiale in base ai livelli di rischio e impone regole stringenti per quelli ad alto impatto, come i sistemi di riconoscimento facciale o la profilazione algoritmica. Sul sito ufficiale dell'Unione Europea, è possibile consultare le versioni aggiornate del regolamento

Consulta il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio

Digital Service Act (DSA)

è la normativa dell'Unione Europea che regola le piattaforme digitali per garantire un ambiente online più sicuro e trasparente. stabilisce regole precise per social network, marketplace e motori di ricerca, con l'obiettivo di proteggere gli utenti e contrastare la diffusione di contenuti illegali

Consulta il Regolamento sui servizi digitali della Commissione Europea

GDPR – Regolamento Generale sulla Protezione dei Dati (Reg. UE 2016/679)

Il GDPR (General Data Protection Regulation) è la normativa europea che disciplina la protezione dei dati personali e il loro trattamento. Anche nell'ambito dell'intelligenza artificiale, il GDPR garantisce ai consumatori diritti fondamentali come:

- Diritto alla trasparenza e all'accesso
- Diritto alla limitazione e alla cancellazione
- Diritto di opposizione e decisioni automatizzate

Per approfondire, è possibile consultare il testo completo del GDPR sul sito dell'Unione Europea - eur-lex.europa.eu

Linee guida dell'Autorità Garante per la Protezione dei Dati Personali

La protezione dei dati personali è un tema centrale quando si parla di intelligenza artificiale. Il Garante per la Privacy italiano fornisce indicazioni pratiche su come tutelare i propri dati e su cosa fare in caso di utilizzo illecito. Il sito ufficiale del Garante offre approfondimenti su temi come il riconoscimento biometrico, il diritto alla trasparenza degli algoritmi e le modalità per esercitare il proprio diritto alla cancellazione dei dati - www.garanteprivacy.it

Dove segnalare

Se sospetti di essere vittima di una truffa basata su IA, se ritieni che i tuoi dati siano stati utilizzati in modo improprio è possibile rivolgersi a diverse autorità per segnalare il problema e ricevere supporto:

Polizia Postale - Per segnalare frodi online, deepfake fraudolenti, phishing avanzato o altre truffe digitali - www.commissariatodips.it

Consob (Commissione Nazionale per le Società e la Borsa) – L'ente che vigila sui mercati finanziari italiani, garantendo la trasparenza e la tutela degli investitori. Sito ufficiale: www.consob.it

Garante per la Protezione dei Dati Personali - Se ritieni che i tuoi dati siano stati utilizzati senza consenso o in modo illecito - www.garanteprivacy.it

Associazioni dei consumatori - Organizzazioni che tutelano i diritti dei consumatori, offrendo assistenza, informazione e supporto per segnalare abusi o pratiche scorrette.

U.Di.Con. UNIONE per la DIFESA dei CONSUMATORI Lazio

U.Di.Con. Regionale Lazio APS
Via di Santa Croce in Gerusalemme, 63 00185 Roma
Tel. 06 77250783 - 351 9076124
mail: regionelazio@udicon .org

U.Di.Con.
UNIONE per la DIFESA dei CONSUMATORI
Lazio

IA E GIOVANI CONSUMATORI
Educazione e Diritti a Portata di Click

Per essere consapevoli dei nostri diritti
e possibilità, con un click

REGIONE LAZIO
Iniziativa finanziata dal fondo Regione Lazio per i consumatori – anno 2024