tu che ne sai?

L'intelligenza artificiale più sicura per tutti

Guida pratica per capire benefici, rischi e tutele nei servizi digitali

tu che ne sai?
L'intelligenza artificiale più sicura per tutti

Intelligenza Artificiale e cittadini

Questa guida aiuta i cittadini a usare i servizi digitali con più consapevolezza, a riconoscere i segnali di rischio e a sapere come reagire quando qualcosa non torna.

tu che ne sai?
L'intelligenza artificiale più sicura per tutti

tu che ne sai?
L'intelligenza artificiale più sicura per tutti

Indice del vademecum

1. Perché questa guida

L'Intelligenza Artificiale è già entrata nella vita quotidiana di tutti noi, anche quando non ce ne accorgiamo. La troviamo nei motori di ricerca, nei chatbot che rispondono online, nei social network, nelle piattaforme di acquisto, nei servizi bancari, nelle app, nei sistemi antifrode e in molti altri servizi digitali.

Questi strumenti possono essere utili: possono far risparmiare tempo, rendere più veloci alcune operazioni, aiutare a trovare informazioni e offrire servizi più personalizzati. Però non sono infallibili. Possono sbagliare, dare risposte incomplete o fuorvianti, prendere decisioni difficili da capire oppure usare i nostri dati in modi che non sempre risultano chiari.

Per questo è importante che ogni cittadino impari a usare i servizi digitali con maggiore consapevolezza. Non serve essere esperti di tecnologia. Basta conoscere alcune regole semplici, sapere quali segnali osservare e capire cosa fare quando qualcosa non torna.

Questa guida nasce proprio con questo obiettivo: aiutarti a riconoscere i benefici dell'Intelligenza Artificiale, a capire i rischi più comuni e a muoverti con più sicurezza nei servizi e nei contenuti digitali.

Nelle pagine che seguono troverai spiegazioni chiare, esempi pratici, consigli utili e indicazioni concrete per:

- capire quando potresti avere a che fare con un sistema di Intelligenza Artificiale;
- usare con prudenza chatbot, piattaforme e servizi automatizzati;
- proteggere meglio i tuoi dati personali;
- riconoscere possibili errori, inganni o situazioni poco trasparenti;
- sapere come reagire se subisci un problema.

Un messaggio è particolarmente importante: davanti a un servizio digitale poco chiaro o a una decisione automatizzata che ti penalizza, non devi affrontare tutto da solo. Informarsi presto, conservare le prove e chiedere aiuto può fare una grande differenza.

Questa guida non vuole creare allarmismo. L'obiettivo non è avere paura della tecnologia, ma imparare a usarla in modo più attento, informato e sicuro.

2. Intelligenza Artificiale: che cos'è, in parole semplici

Quando si parla di Intelligenza Artificiale, spesso si pensa a qualcosa di complicato, lontano o quasi "magico". In realtà, l'Intelligenza Artificiale è un insieme di tecnologie che permette ai sistemi informatici di svolgere compiti che, fino a poco tempo fa, richiedevano soprattutto capacità umane: capire un testo, riconoscere immagini, suggerire una scelta, rispondere a una domanda, fare una previsione o prendere una decisione.

Detto in modo ancora più semplice, l'IA analizza grandi quantità di dati, cerca schemi ricorrenti e produce un risultato: una risposta, un consiglio, una classificazione, un contenuto o un'azione. Può quindi aiutare a

ordinare informazioni, individuare anomalie, proporre contenuti personalizzati o rispondere in automatico agli utenti.

Questo però non significa che l'IA "capisca" il mondo come una persona. Non ha buon senso umano, esperienza di vita, coscienza o responsabilità morale. Lavora in base ai dati che riceve, alle istruzioni con cui è stata progettata e ai modelli statistici con cui è stata addestrata. Per questo può sembrare molto sicura di sé anche quando sbaglia. Una risposta plausibile non è sempre una risposta affidabile.

Un modo utile per capire la differenza è questo: un software tradizionale segue regole precise, mentre un sistema di IA spesso lavora in modo probabilistico. È stato addestrato su molti esempi e calcola quale risultato è più probabile. Proprio per questo può essere molto potente, ma anche meno trasparente e meno prevedibile di un programma tradizionale.

Non esiste poi una sola Intelligenza Artificiale. Esistono sistemi che riconoscono immagini, sistemi che aiutano a bloccare frodi o transazioni sospette, sistemi che selezionano contenuti da mostrare sui social o suggeriscono prodotti negli acquisti online. I chatbot e gli assistenti virtuali sono solo una delle forme più visibili dell'IA, ma non sono l'unica.

Negli ultimi anni si è parlato molto di IA generativa. Si tratta di sistemi capaci di creare nuovi contenuti, come testi, immagini, audio o video. Questi strumenti possono essere molto utili, ma vanno usati con prudenza, perché possono anche inventare informazioni, semplificare troppo o creare contenuti falsi ma credibili.

Per i cittadini, la cosa più importante non è conoscere i dettagli tecnici, ma ricordare tre idee di base.

- l'IA non è fantascienza: è già presente in molti servizi digitali che usiamo ogni giorno;
- l'IA può essere utile, ma non è infallibile;
- se un sistema automatico sbaglia, crea confusione o prende una decisione che ti penalizza, il problema è reale anche se la tecnologia dietro non è visibile.

Per questo non serve diventare esperti informatici. Serve piuttosto imparare a fare attenzione, a verificare le informazioni importanti e a non considerare "vero" tutto ciò che un sistema automatico dice o fa.

In breve, l'Intelligenza Artificiale è uno strumento potente. Può semplificare molti servizi, ma non sostituisce il giudizio umano, la verifica dei fatti e la tutela dei diritti. Usarla bene significa conoscerne sia le opportunità sia i limiti.

3. Dove i cittadini incontrano l'IA nei servizi digitali

Molte persone pensano di usare l'Intelligenza Artificiale solo quando aprono un chatbot o provano un'app nuova. In realtà non è così. Oggi l'IA può entrare in contatto con il cittadino in molti momenti della vita digitale: prima di un acquisto, durante l'uso di un servizio, dopo un reclamo, nella gestione di un account, nei pagamenti, nelle verifiche di sicurezza e perfino nei contenuti che vediamo ogni giorno online.

I casi che seguono sono solo alcuni esempi. L'IA può comparire in molti altri contesti, anche quando non è immediatamente visibile.

Prima dell'acquisto: offerte, risultati e contenuti personalizzati

Un primo contatto con l'IA avviene spesso ancora prima che il cittadino decida di comprare qualcosa. Può succedere quando una piattaforma mostra certi prodotti prima di altri, suggerisce offerte su misura,

propone contenuti personalizzati o modifica l'ordine dei risultati di ricerca. In pratica, quello che vedi sullo schermo non è sempre neutrale: può essere selezionato da sistemi automatici che cercano di capire cosa attira di più la tua attenzione o cosa hai più probabilità di acquistare.

Anche i prezzi possono essere influenzati da sistemi automatizzati. In alcuni casi si tratta di prezzi dinamici, che cambiano in base alla domanda. In altri casi può esserci una personalizzazione più spinta, legata al profilo dell'utente, alle sue abitudini o al dispositivo usato. Per il cittadino è importante sapere che il prezzo mostrato online non sempre è uguale per tutti e che, quando la personalizzazione è poco chiara, è bene fare una verifica in più.

Durante l'acquisto o l'accesso al servizio: controlli, verifiche e blocchi automatici

L'IA entra spesso in gioco anche nel momento in cui si effettua un pagamento, si accede a un servizio o si prova a completare una procedura online. È il caso dei sistemi antifrode, dei controlli automatici sulle transazioni, delle verifiche di identità e dei meccanismi che segnalano attività considerate sospette. Questi strumenti servono a migliorare la sicurezza, ma possono anche produrre errori: per esempio bloccare una carta, sospendere un account o fermare un'operazione legittima senza una spiegazione davvero comprensibile.

In altri casi, il cittadino incontra l'IA quando un sistema decide se una richiesta può essere accettata, rallentata, limitata o respinta. Può accadere nell'accesso a servizi, nelle priorità assegnate, nelle code automatiche o nelle verifiche di idoneità. Quando la decisione arriva in modo rapido, standardizzato e poco chiaro, può esserci dietro un sistema automatizzato che valuta il caso secondo criteri non immediatamente visibili all'utente.

Dopo l'acquisto: chatbot, rimborsi e reclami

Uno dei luoghi in cui i cittadini incontrano più spesso l'IA è l'assistenza clienti. Sempre più aziende usano chatbot conversazionali, risponditori automatici e sistemi che smistano le richieste. Questo può essere comodo quando il problema è semplice, ma può diventare frustrante quando serve una risposta precisa o quando non si riesce mai a parlare con una persona.

Il problema non è solo la freddezza della risposta automatica. Un chatbot può anche dare informazioni sbagliate, incomplete o fuorvianti. Può sembrare sicuro, usare un linguaggio convincente e perfino indicare procedure o diritti che in realtà non esistono. Per questo, quando si parla di recesso, rimborso, garanzia, scadenze o penali, il cittadino dovrebbe sempre controllare anche i documenti ufficiali del servizio.

Energia, telefonia e servizi continuativi

L'IA può essere presente anche in servizi molto comuni e continuativi, come energia, gas, telefonia, connessione internet e altri servizi gestiti tramite area clienti, app o call center. Può intervenire nella proposta di offerte personalizzate, nella gestione automatica dei contatti con il cliente, nella classificazione

dei reclami, nei controlli antifrode, nella verifica di pagamenti, nella prevenzione della morosità o nella segnalazione di anomalie nei consumi.

Per il cittadino questo significa che anche in ambiti molto quotidiani possono comparire decisioni o comunicazioni standardizzate, difficili da capire o da contestare: per esempio un cambio di offerta poco chiaro, una risposta automatica a un reclamo, un blocco di una procedura, una classificazione errata del problema o una gestione molto rigida del rapporto con il cliente.

Banche, assicurazioni e valutazioni automatiche

Un altro settore importante è quello finanziario e assicurativo. Qui l'IA può essere usata per valutare richieste, controllare rischi, stimare affidabilità o attribuire punteggi automatici. In termini semplici, il cittadino può trovarsi davanti a decisioni prese o fortemente influenzate da un sistema di scoring: per esempio nella concessione di un credito, nella valutazione del rischio o nell'accesso a determinati servizi.

In questi casi il rischio per il cittadino non è solo ricevere un no, ma riceverlo senza capire bene perché. Quando una decisione è percepita come una scatola nera, il consumatore fatica a sapere quali elementi hanno pesato, se ci sono stati errori nei dati o se il caso è stato davvero rivisto da una persona.

Social network, marketplace e piattaforme online

L'IA è molto presente anche nelle piattaforme che usiamo ogni giorno: social network, marketplace, siti di video, app di contenuti e servizi digitali. Qui può decidere quali post mostrarti, quali annunci farti vedere, quali contenuti spingere di più e quali segnalare o rimuovere. Può anche contribuire alla sospensione di un account, alla limitazione di una funzione o alla riduzione della visibilità di contenuti e profili.

Per il cittadino questo significa una cosa semplice: anche quando non stai parlando con un robot, potresti comunque essere dentro un ambiente fortemente governato da sistemi automatici. Questi sistemi influenzano ciò che vedi, ciò che ti viene proposto e, in alcuni casi, ciò che ti viene impedito di fare.

Truffe, contenuti falsi e manipolazioni

C'è poi un altro ambito in cui oggi i cittadini incontrano l'IA sempre più spesso: quello dei contenuti falsi o manipolati. Audio, immagini, video e messaggi possono essere creati o modificati con strumenti di IA per sembrare credibili. Questo rende più insidiose le truffe, i falsi messaggi di assistenza, i finti premi, le richieste urgenti di pagamento e perfino i tentativi di imitare una voce o un volto conosciuto.

Per questo motivo l'IA non va cercata solo nei servizi ufficiali, ma anche nei contenuti che circolano online. Un messaggio ben scritto, una voce familiare o un video apparentemente realistico non bastano più, da soli, per garantire che ciò che stiamo vedendo sia autentico.

In sintesi

In pratica, il cittadino può incontrare l'IA in molti ambiti diversi: nelle offerte e nei contenuti che vede, nei prezzi e nelle promozioni, nei controlli di sicurezza e nei pagamenti, nell'assistenza clienti, nei servizi di

energia e telefonia, nelle decisioni che riguardano accesso, punteggi o idoneità, e anche nei contenuti che circolano online.

Sapere dove l'IA può comparire aiuta a non farsi trovare impreparati e a riconoscere più in fretta i casi in cui serve fare domande, chiedere chiarimenti o conservare prove.

4. I benefici dell'IA per i cittadini

L'Intelligenza Artificiale può offrire vantaggi concreti nella vita di tutti i giorni, soprattutto quando viene usata per semplificare attività, rendere i servizi più rapidi e aiutare le persone a trovare informazioni più facilmente.

Il primo beneficio è spesso la velocità. In molti servizi digitali, alcuni passaggi che prima richiedevano più tempo possono essere svolti in pochi secondi: cercare informazioni, ricevere una prima risposta, completare una procedura, individuare un problema tecnico o ottenere assistenza su richieste semplici. Quando questi strumenti funzionano bene, il cittadino può risparmiare tempo e fatica.

Un secondo beneficio è la maggiore facilità d'uso. Alcuni sistemi aiutano a orientarsi meglio tra siti, piattaforme, moduli e contenuti. Possono suggerire informazioni utili, organizzare risultati di ricerca, rendere più semplice trovare un prodotto, un servizio o una risposta. Questo può essere utile soprattutto quando le informazioni sono molte e non è facile capire da dove cominciare.

L'IA può anche contribuire a una certa personalizzazione del servizio. Per esempio può aiutare a mostrare contenuti più vicini agli interessi dell'utente, ricordare preferenze già espresse o proporre percorsi più adatti a uno specifico bisogno. Se usata bene, questa personalizzazione può rendere l'esperienza più comoda e meno dispersiva.

Un altro vantaggio importante riguarda il supporto nella comprensione delle informazioni. Alcuni strumenti possono aiutare a riassumere testi lunghi, spiegare parole difficili, riformulare un contenuto in modo più semplice o aiutare a confrontare più opzioni. Per molti cittadini questo può essere utile quando si leggono condizioni di servizio, comunicazioni tecniche, istruzioni o documenti non immediati.

L'Intelligenza Artificiale può essere utile anche sul piano dell'accessibilità. Strumenti che funzionano con testo, voce, immagini o audio possono rendere più semplice l'uso dei servizi digitali da parte di persone con esigenze diverse. In alcuni casi la tecnologia può aiutare a superare ostacoli pratici e a rendere più immediato l'accesso alle informazioni.

C'è poi un aspetto molto concreto: alcuni servizi automatizzati possono essere disponibili anche fuori dagli orari tradizionali, offrendo un primo livello di aiuto in qualsiasi momento. Questo non sostituisce il contatto umano, ma può essere utile per richieste semplici, orientamento iniziale o informazioni di base.

Detto questo, il beneficio non dipende solo dalla presenza della tecnologia. Un servizio è davvero utile quando è chiaro, corretto, facile da usare e pensato per rispondere a bisogni reali. Se invece è complicato, poco trasparente o costruito senza attenzione alle persone, anche uno strumento molto avanzato può risultare poco utile o addirittura creare problemi.

Per questo è giusto guardare all'Intelligenza Artificiale con equilibrio. Non come qualcosa da temere per forza, ma neppure come una soluzione perfetta a tutto. Può essere una risorsa preziosa quando aiuta davvero il cittadino, semplifica i passaggi, migliora l'accesso alle informazioni e rende i servizi più efficienti.

In sintesi, i benefici principali possono essere questi: più rapidità, maggiore comodità, supporto nella ricerca di informazioni, strumenti più accessibili e servizi più semplici da usare. L'importante è ricordare che la tecnologia deve restare uno strumento al servizio delle persone.

5. I rischi da conoscere

L'Intelligenza Artificiale può essere utile, ma non è perfetta. Può sbagliare, fraintendere, semplificare troppo o prendere decisioni che per il cittadino risultano poco chiare. Per questo è importante conoscerne i principali rischi, così da usare i servizi digitali con più attenzione e maggiore consapevolezza.

Risposte sbagliate, ma convincenti

Uno dei rischi più comuni è ricevere risposte errate formulate in modo molto convincente. Un chatbot o un sistema automatico può scrivere bene, usare un tono sicuro e dare l'impressione di essere affidabile, anche quando l'informazione è incompleta, imprecisa o del tutto sbagliata.

Per questo, quando si parla di rimborsi, recesso, garanzie, scadenze, contratti, pagamenti o dati personali, è sempre prudente verificare anche le informazioni ufficiali del servizio.

Decisioni automatiche difficili da capire

Un altro rischio importante riguarda le decisioni prese o influenzate da sistemi automatici. Può succedere, per esempio, con il blocco di un pagamento, la sospensione di un account, il rifiuto di una richiesta o un controllo di sicurezza che produce un risultato negativo.

Il problema non è solo l'eventuale errore. Spesso il cittadino riceve una risposta generica e non capisce bene perché quella decisione sia stata presa. Quando manca una spiegazione chiara, diventa più difficile contestare, correggere o chiedere una revisione del caso.

Uso poco trasparente dei dati personali

Molti sistemi di Intelligenza Artificiale funzionano analizzando dati: abitudini, preferenze, ricerche, cronologia, localizzazione, modalità di acquisto o altre informazioni legate all'uso dei servizi digitali.

Questo può migliorare alcuni servizi, ma può anche creare problemi se il cittadino non capisce bene quali dati vengono raccolti, per quale motivo vengono usati e per quanto tempo vengono conservati. Per questo è sempre importante fare attenzione alle informative, ai consensi richiesti e ai dati che si scelgono di condividere.

Trattamenti ingiusti o poco equi

L'uso di sistemi automatici può portare, in alcuni casi, a trattamenti diversi tra persone che si trovano in situazioni simili. Questo può riguardare il prezzo mostrato, le offerte ricevute, i controlli applicati, la priorità assegnata a una richiesta o l'accesso a un servizio.

Non ogni differenza è necessariamente scorretta, ma quando il cittadino riceve un trattamento sfavorevole senza capirne il motivo, è giusto fermarsi, fare domande e chiedere chiarimenti.

Pressioni commerciali e scelte spinte

I servizi digitali possono essere progettati per indirizzare le decisioni dell'utente. A volte questo avviene con messaggi insistenti, urgenze artificiali, percorsi poco chiari, pulsanti messi in evidenza solo in una direzione o procedure complicate per rinunciare a un acquisto, a un abbonamento o a un consenso.

Quando la tecnologia viene usata per spingere il cittadino a decidere in fretta o senza piena consapevolezza, il rischio non è solo commerciale: è anche un problema di trasparenza e di correttezza.

Truffe più credibili e contenuti falsi

L'Intelligenza Artificiale può essere usata anche per creare truffe più convincenti. Oggi esistono messaggi, email, immagini, audio e video che possono sembrare autentici anche quando non lo sono. Un volto, una voce o un testo ben fatto non bastano più, da soli, a garantire che un contenuto sia vero.

Per questo bisogna prestare ancora più attenzione a richieste urgenti di denaro, codici, password, dati bancari o conferme immediate. In caso di dubbio, è sempre meglio fermarsi e verificare attraverso canali ufficiali.

Difficoltà a parlare con una persona

Un problema molto concreto nasce quando il cittadino resta bloccato in un percorso tutto automatico: chatbot che ripetono sempre le stesse cose, risposte standard, moduli che non permettono di spiegare il caso reale, impossibilità di parlare con un operatore.

In queste situazioni il rischio è perdere tempo, non riuscire a far comprendere il problema e rinunciare a far valere i propri diritti. Quando il sistema automatico non basta, deve essere possibile chiedere un intervento umano.

Il rischio più grande: fidarsi senza verificare

Il rischio più importante, in fondo, è pensare che un sistema automatico abbia sempre ragione solo perché appare moderno, veloce o sicuro. Non è così. L'Intelligenza Artificiale può essere uno strumento utile, ma non sostituisce il controllo umano, la lettura attenta dei documenti e la verifica delle informazioni importanti.

Conoscere questi rischi non serve ad avere paura della tecnologia. Serve, al contrario, a usarla meglio. Un cittadino informato è più capace di riconoscere i segnali di allarme, evitare errori e reagire in tempo quando qualcosa non torna.

6. I segnali di attenzione: quando è bene fermarsi e verificare

Non sempre è facile capire se dietro un problema c'è un sistema automatico o di Intelligenza Artificiale. E, in molti casi, per il cittadino non è nemmeno necessario saperlo con certezza. Quello che conta davvero è riconoscere i segnali di attenzione: indizi che fanno capire che è meglio fermarsi un momento, non agire di fretta e controllare meglio la situazione.

Fermarsi e verificare non significa avere paura della tecnologia. Significa usare prudenza quando qualcosa appare poco chiaro, troppo rapido, troppo rigido o semplicemente non coerente con i fatti.

Quando la risposta è troppo generica

Se il messaggio non spiega in modo concreto che cosa è successo, perché è successo e che cosa puoi fare dopo, è giusto fermarsi e chiedere chiarimenti.

Quando tutto sembra automatico e non c'è un vero interlocutore umano

Se trovi solo chatbot, risposte preimpostate, email automatiche o percorsi che ti riportano sempre allo stesso punto, è possibile che il tuo caso venga gestito in modo troppo rigido o standardizzato. Questo conta soprattutto quando il problema riguarda soldi, contratti, blocchi, sospensioni, rimborsi, accesso a servizi o dati personali.

Quando la decisione arriva subito ed è rigida

Occorre prestare attenzione anche alle decisioni che arrivano in modo istantaneo, senza spiegazioni utili e senza tener conto della tua situazione concreta. Quando una decisione è immediata, rigida e non contestualizzata, è bene non considerarla automaticamente corretta.

Quando la risposta contraddice i documenti o quello che è già successo

Se il sistema ti dice una cosa che non coincide con il contratto, con le condizioni pubblicate sul sito, con una comunicazione ricevuta in precedenza o con il tuo storico, bisogna fermarsi.

Quando la stessa risposta si ripete sempre uguale

Se cambi domanda, spieghi meglio il problema, aggiungi informazioni utili e la risposta rimane identica, è possibile che il sistema non stia davvero valutando il caso concreto.

Quando ti viene chiesto di fare in fretta

L'urgenza artificiale è uno dei segnali più importanti da riconoscere. Se un messaggio ti spinge a decidere immediatamente, cliccare su un link, inquadrare un QR code o comunicare codici e dati bancari, è prudente rallentare e verificare.

Quando il contenuto sembra molto credibile, forse troppo

Oggi immagini, voci, video e messaggi possono sembrare autentici anche quando non lo sono. Se un contenuto sembra provenire da una banca, da un servizio clienti, da una piattaforma o perfino da una persona conosciuta, non dare per scontato che sia vero solo perché è fatto bene.

Quando non è chiaro con chi stai parlando

Se usi una chat o un assistente digitale, dovrebbe essere chiaro se stai parlando con una persona o con un sistema automatico. Se questa distinzione non è evidente, conviene fare maggiore attenzione.

Quando ti vengono chiesti troppi dati

Se per ottenere una semplice informazione o completare un passaggio ti vengono chiesti dati molto personali, documenti non necessari o informazioni sensibili, è giusto fermarsi e chiedersi se quella richiesta sia davvero proporzionata.

Quando non sai come contestare o correggere

Un servizio digitale dovrebbe permetterti di capire come segnalare un errore, come chiedere chiarimenti e come ottenere una revisione. Se tutto questo non è chiaro, oppure se non esiste un percorso reale per contestare una decisione, è bene considerarlo un segnale di attenzione.

Una regola semplice da ricordare

- risposta troppo generica;
- assenza di un contatto umano reale;
- decisione immediata e rigida;
- incoerenza con documenti, regole o comunicazioni precedenti;
- richiesta di agire in fretta;
- richiesta di dati, codici o pagamenti;
- contenuti molto realistici ma sospetti;
- mancanza di spiegazioni chiare;
- impossibilità di contestare.

Cosa fare, in pratica

1. non agire di impulso;
2. rileggi con calma il messaggio o la risposta ricevuta;
3. confronta l'informazione con il sito ufficiale, il contratto o la comunicazione originale;
4. salva screenshot, email, numeri pratica e data dell'evento;
5. evita di condividere subito dati, codici o denaro;
6. cerca un canale ufficiale e, se possibile, un contatto umano.

Riconoscere in tempo i segnali di attenzione aiuta a evitare errori, limitare i danni e muoversi con maggiore sicurezza nei servizi digitali. Non serve capire tutta la tecnologia che c'è dietro: spesso basta accorgersi che qualcosa non torna e fermarsi prima di fare il passo sbagliato.

7. Le 10 regole pratiche per usare meglio i servizi digitali

L'Intelligenza Artificiale è sempre più presente nei servizi online, nei chatbot, nelle piattaforme, negli acquisti digitali e nei contenuti che vediamo ogni giorno. Non serve essere esperti di tecnologia per difendersi e usarla bene. Spesso bastano alcune regole semplici di buon senso, applicate con attenzione.

1. Verifica prima di fidarti

Se una risposta riguarda soldi, diritti, rimborsi, contratti, scadenze, salute, pagamenti o dati personali, non fermarti alla prima risposta ricevuta. Controlla anche il sito ufficiale, il contratto, l'email originale o un'altra fonte affidabile.

2. Non condividere più dati del necessario

Quando usi un chatbot, compili un modulo o interagisci con un servizio digitale, inserisci solo i dati strettamente necessari. Evita di comunicare informazioni sensibili se non sei sicuro del motivo per cui vengono richieste e di come saranno usate.

- documenti di identità;
- dati bancari;
- codici di accesso;
- password;
- informazioni sanitarie;
- dati relativi ad altri familiari o terze persone.

3. Non prendere decisioni importanti basandoti solo su un chatbot

Un chatbot può essere utile per orientarti, ma non dovrebbe essere la tua unica base per una decisione importante. Se devi accettare un'offerta, rinunciare a un diritto, fare un pagamento, chiudere un contratto o contestare un addebito, è meglio controllare anche i documenti ufficiali e, se necessario, chiedere conferma attraverso un canale diretto.

4. Conserva le prove

Se qualcosa non torna, salva subito gli elementi utili: screenshot, email, chat, numeri pratica, data e ora dell'evento, nome del servizio o della piattaforma, eventuali documenti ricevuti.

5. Diffida dall'urgenza

Se un messaggio ti spinge a decidere subito, cliccare immediatamente, trasferire denaro, comunicare codici o confermare dati senza riflettere, fermati. La fretta è spesso il terreno ideale per errori, pressioni scorrette o truffe.

6. Controlla sempre il canale da cui arriva il messaggio

Email, SMS, chat, social network, telefonate e video possono oggi sembrare molto credibili anche quando non sono autentici. Prima di fidarti, verifica sempre da dove arriva la comunicazione.

- l'indirizzo email del mittente;
- il numero di telefono;
- il sito a cui porta il link;
- il nome esatto del servizio;
- eventuali errori, incongruenze o richieste insolite.

7. Chiedi spiegazioni chiare

Se una risposta è vaga o una decisione ti penalizza senza motivi comprensibili, chiedi spiegazioni concrete. Hai tutto il diritto di capire che cosa è successo, quali passaggi sono stati seguiti e che cosa puoi fare per correggere o contestare il problema.

8. Cerca, quando serve, un contatto umano

L'automazione può essere utile, ma non deve trasformarsi in un muro. Se il chatbot ripete sempre la stessa cosa, se il modulo non permette di spiegare il caso o se il sistema non dà risposte utili, prova a cercare un contatto umano: assistenza clienti, reclamo formale, PEC, email ufficiale, sportello o numero dedicato.

9. Confronta più fonti

Se ricevi una risposta da un sistema automatico, controlla se coincide con le condizioni contrattuali, il regolamento del servizio, la sezione FAQ ufficiale, una comunicazione scritta dell'azienda o altre fonti affidabili.

10. Quando qualcosa non torna, fermati

Se un servizio ti sembra poco chiaro, se una decisione appare ingiusta, se una richiesta ti sembra eccessiva o se un contenuto ti sembra sospetto, non andare avanti per inerzia.

Una regola finale da ricordare

La tecnologia può essere utile, ma non deve sostituire la prudenza. Usare bene i servizi digitali significa restare attenti, fare domande, verificare le informazioni importanti e non lasciarsi guidare solo dalla comodità o dalla fretta.

In altre parole: usa gli strumenti digitali con fiducia, ma non senza controllo.

8. Truffe e inganni potenziati dall'IA

L'Intelligenza Artificiale non viene usata solo per migliorare servizi e strumenti digitali. Può essere usata anche per ingannare, manipolare e rendere le truffe più credibili. Questo è uno dei motivi per cui oggi è importante prestare ancora più attenzione a messaggi, telefonate, immagini, video e richieste ricevute online.

In passato molte truffe si riconoscevano abbastanza facilmente: testi scritti male, immagini poco realistiche, messaggi generici o pieni di errori. Oggi non è più sempre così. Con l'aiuto dell'IA, chi vuole

truffare può creare contenuti molto più convincenti, personalizzati e difficili da distinguere da quelli autentici.

Perché le truffe sono diventate più credibili

L'IA può imitare il linguaggio umano in modo molto convincente. Può scrivere messaggi chiari, formali e ben costruiti. Può generare immagini realistiche, clonare una voce, creare video manipolati o simulare una conversazione credibile con un falso operatore.

Questo significa che un contenuto può sembrare autentico anche quando non lo è. Un messaggio ben scritto non garantisce che sia vero. Una voce familiare non garantisce che sia reale. Un video realistico non garantisce che sia affidabile.

I casi più comuni

Uno dei casi più frequenti è il falso messaggio di assistenza. Il cittadino riceve una comunicazione che sembra arrivare da una banca, da un corriere, da una piattaforma online, da un servizio clienti o da un gestore di pagamenti. Il messaggio invita a cliccare un link, aggiornare dati, confermare un'operazione o risolvere un problema urgente.

Un altro caso comune è il falso allarme di sicurezza. Per esempio:

- "Abbiamo rilevato un accesso sospetto";
- "Il tuo account sarà sospeso";
- "Il pagamento è stato bloccato";
- "Devi verificare subito la tua identità".

Questi messaggi puntano quasi sempre a ottenere qualcosa dal cittadino: password, codici, dati personali, dati bancari o un trasferimento di denaro.

C'è poi il caso dei falsi investimenti, dei falsi rimborsi e dei falsi premi. Il contenuto può sembrare professionale, ben fatto e persino personalizzato sul destinatario. Proprio questa apparente precisione può abbassare la soglia di attenzione.

Audio e video manipolati

Uno dei fenomeni più insidiosi è quello dei contenuti audio o video manipolati. Oggi esistono strumenti capaci di imitare la voce di una persona, ricrearne il volto o costruire un video apparentemente realistico.

Questo può essere usato per far credere al cittadino di stare ascoltando un familiare, un responsabile bancario, un operatore o una persona conosciuta. In altri casi può servire a dare forza a una notizia falsa, a una proposta ingannevole o a una richiesta urgente di denaro.

Per questo, anche davanti a una voce o a un volto che sembrano familiari, è sempre bene verificare con un secondo canale prima di agire.

La personalizzazione della truffa

L'IA rende molte truffe più efficaci anche perché permette di personalizzarle meglio. Un messaggio può contenere il tuo nome, fare riferimento a un acquisto recente, imitare il tono di una comunicazione ufficiale o sembrare coerente con un servizio che usi davvero.

Più il contenuto sembra vicino alla tua esperienza, più aumenta il rischio di fidarsi senza verificare. È proprio questa somiglianza con la realtà a rendere l'inganno più pericoloso.

I segnali da non ignorare

Ci sono alcuni segnali che devono far alzare subito il livello di attenzione.

- urgenza: il messaggio ti chiede di agire immediatamente;
- richiesta di dati riservati: password, codici di accesso o codici di sicurezza;
- pressione emotiva: paura, fretta, senso di colpa, minaccia di blocco o promessa di vantaggi immediati;
- difficoltà di verifica: il messaggio ti porta fuori dai canali ufficiali o ti spinge a usare solo il link ricevuto.

Cosa non fare

Quando ricevi una comunicazione sospetta, evita le reazioni istintive: non cliccare subito sul link ricevuto, non richiamare automaticamente il numero indicato nel messaggio, non inviare documenti o dati personali, non comunicare codici temporanei, non autorizzare pagamenti e non scaricare file o app senza aver verificato bene la fonte.

Cosa fare subito

La regola più utile è semplice: interrompi, verifica, poi decidi.

1. controlla il sito ufficiale entrando manualmente dal browser o dall'app ufficiale;
2. contatta il servizio usando recapiti che già conosci o che trovi sul sito ufficiale;
3. confronta il contenuto con comunicazioni autentiche ricevute in passato;
4. salva screenshot, email, numeri e orari;
5. non cancellare tutto subito, perché potrebbe servirti per ricostruire l'accaduto.

Se hai già cliccato, risposto o condiviso dati, agisci il prima possibile: cambia le password, contatta la banca o il servizio coinvolto, blocca eventuali strumenti di pagamento e segnala l'accaduto.

Una regola semplice da ricordare

Più un contenuto sembra urgente, realistico e perfettamente costruito, più vale la pena fare una verifica in più.

Oggi prudenza non significa sfiducia verso tutto. Significa sapere che la tecnologia può essere usata anche per imitare, confondere e convincere. Per questo il modo migliore di difendersi non è cercare di riconoscere ogni singolo trucco, ma abituarsi a non reagire di impulso.

In caso di dubbio, è sempre meglio perdere qualche minuto in una verifica che rischiare di perdere dati, denaro o accesso ai propri servizi digitali.

9. I tuoi diritti e le tutele principali

Quando usi un servizio digitale, non sei senza protezioni solo perché dietro c'è un sistema automatico o di Intelligenza Artificiale. Anche in questo ambito esistono regole e tutele. In pratica, il cittadino non deve conoscere il funzionamento tecnico di un algoritmo, ma può chiedere chiarezza, contestare decisioni che lo danneggiano e far valere i propri diritti.

Sapere quando stai interagendo con un sistema automatico

In diversi casi la normativa europea prevede obblighi di trasparenza quando una persona interagisce con un sistema di IA, in particolare per alcuni chatbot e per determinati contenuti generati o manipolati artificialmente. In termini semplici, il cittadino deve poter capire, quando la legge lo richiede, se sta interagendo con un sistema automatico e non dovrebbe essere indotto in errore da contenuti artificiali presentati come autentici.

Ricevere informazioni corrette e non ingannevoli

Un'impresa non può usare strumenti digitali per confondere il consumatore, omettere informazioni importanti o spingerlo a una scelta che non avrebbe fatto se fosse stato informato correttamente. Se un chatbot dà informazioni sbagliate o se una piattaforma usa modalità poco trasparenti per orientare una decisione, il problema non è solo tecnico: può diventare anche un problema di correttezza verso il consumatore.

Protezione dei dati personali

Quando un sistema di IA usa dati personali, continuano a valere le regole sulla privacy. Questo significa, in termini semplici, che il cittadino ha diritto a sapere quali dati vengono trattati, per quale motivo e con quali garanzie.

In molti casi puoi anche chiedere accesso ai tuoi dati, correggere dati inesatti e, quando ne ricorrono i presupposti, chiederne la cancellazione o opporti a determinati trattamenti. Se ritieni che i dati siano usati in modo illecito o poco trasparente, puoi presentare reclamo al Garante per la protezione dei dati personali.

Decisioni completamente automatiche

Quando una decisione si basa unicamente su un trattamento automatizzato di dati personali e produce effetti giuridici oppure incide in modo analogo significativamente sulla persona, il GDPR prevede tutele specifiche. In questi casi, a seconda della base giuridica e della situazione concreta, la persona interessata può ottenere garanzie come l'intervento umano, la possibilità di esprimere il proprio punto di vista e di contestare la decisione.

Spiegazioni comprensibili nei casi più delicati

Non in ogni situazione la legge impone lo stesso livello di spiegazione. Tuttavia, nei casi di decisioni unicamente automatizzate che rientrano nelle tutele del GDPR, la persona interessata deve ricevere informazioni significative sul trattamento e poter chiedere chiarimenti utili per comprendere e contestare l'esito.

Revisione umana reale

Quando la legge riconosce il diritto a garanzie contro una decisione unicamente automatizzata, l'intervento umano non deve essere solo formale: deve essere effettivo, cioè consentire a una persona competente di riesaminare il caso e, se necessario, correggere o superare l'esito automatico.

Divieto di pratiche particolarmente gravi

La legge europea vieta alcune pratiche considerate molto rischiose, come alcuni usi manipolativi dell'IA, lo sfruttamento illecito di vulnerabilità particolari e forme vietate di social scoring da parte di soggetti pubblici o privati.

Reclami e segnalazioni

Quando qualcosa non va, il cittadino non ha solo la possibilità di lamentarsi con l'azienda: può anche rivolgersi alle autorità competenti. In linea generale, i problemi sui dati personali possono essere portati al Garante Privacy; le pratiche commerciali scorrette, ingannevoli o aggressive possono essere segnalate all'AGCM; nei settori bancari, finanziari o assicurativi possono entrare in gioco anche autorità di settore.

Una cosa importante da ricordare

Non tutti i diritti si applicano nello stesso modo in ogni situazione. Molto dipende dal tipo di servizio, dal tipo di decisione, dai dati usati e dal settore coinvolto. Però il principio di fondo è semplice: se un sistema automatico ti riguarda, ti condiziona o ti danneggia, non sei obbligato ad accettarne passivamente il risultato. Puoi chiedere chiarimenti, contestare e domandare una verifica reale del tuo caso.

10. Cosa fare se pensi di aver subito un problema

Quando un servizio digitale ti crea un danno, ti dà una risposta poco chiara o prende una decisione che ti penalizza, la cosa più importante è non restare bloccato tra rabbia, fretta e confusione. Anche se non sai con certezza se dietro ci sia un sistema automatico o di Intelligenza Artificiale, puoi comunque fare alcune cose utili fin da subito.

L'obiettivo non è dimostrare la tecnologia, ma proteggerti, ricostruire i fatti e mettere ordine nella situazione.

1. Fermati e ricostruisci che cosa è successo

Il primo passo è semplice: fermati un momento e prova a mettere in fila gli eventi.

Chiediti:

- che cosa è successo esattamente;
- quando è successo;
- su quale sito, app o piattaforma;
- quale operazione stavi facendo;
- quale risposta hai ricevuto;
- quale danno o difficoltà ne è derivato.

2. Salva subito tutte le prove utili

Se c'è un problema, non aspettare. Molti elementi possono sparire rapidamente: una chat può chiudersi, una schermata può cambiare, un messaggio può non essere più visibile.

Per questo conviene salvare subito:

- screenshot delle schermate;
- email ricevute;
- messaggi in chat;
- numeri pratica;
- data e ora dell'evento;
- eventuali documenti scaricati;
- nome del servizio o della piattaforma;
- eventuali importi coinvolti.

3. Non cancellare tutto per impulso

Quando si è irritati o preoccupati viene spontaneo cancellare messaggi, chiudere finestre o uscire subito dal servizio. È comprensibile, ma non sempre è la scelta migliore.

Prima di eliminare o chiudere tutto, prova a salvare almeno gli elementi essenziali. In molti casi, una semplice schermata può fare la differenza tra un problema difficile da ricostruire e un reclamo chiaro e fondato.

4. Verifica se il problema è reale, ripetuto o solo apparente

A volte un errore può dipendere da un problema temporaneo, da una connessione instabile o da un passaggio tecnico non andato a buon fine. Altre volte, invece, il problema è reale e si ripete.

Per capirlo, può essere utile controllare:

- se il messaggio compare ancora;
- se il problema si ripresenta;
- se esistono comunicazioni ufficiali sul disservizio;
- se il contratto o il regolamento dicono qualcosa di diverso;

- se altri canali ufficiali riportano le stesse informazioni.

5. Chiedi spiegazioni chiare

Se una decisione ti penalizza o una risposta è troppo generica, non fermarti alla prima formula standard. Chiedi spiegazioni concrete.

Per esempio, puoi chiedere:

- perché l'operazione è stata bloccata;
- quale regola è stata applicata;
- se il caso è stato esaminato da una persona;
- come puoi correggere eventuali errori;
- come puoi contestare la decisione;
- entro quali tempi riceverai una risposta.

6. Cerca un canale ufficiale e tracciabile

Quando devi contestare un problema o chiedere chiarimenti, è meglio usare canali ufficiali e il più possibile tracciabili. Per esempio:

- area assistenza del servizio;
- email ufficiale;
- modulo reclami;
- PEC, se disponibile;
- numero clienti indicato sul sito ufficiale;
- area personale dell'account.

7. Chiedi una revisione del caso

Se il problema deriva da un blocco, un rifiuto, una sospensione o un'altra decisione sfavorevole, chiedi che il caso venga riesaminato.

In pratica, puoi domandare:

- una verifica più approfondita;
- una revisione della decisione;
- un controllo umano del caso;
- la correzione di eventuali dati errati;
- una risposta scritta più dettagliata.

8. Proteggi subito i tuoi dati e i tuoi account, se necessario

Se pensi di aver cliccato su un link sospetto, comunicato dati sensibili o autorizzato qualcosa per errore, non aspettare.

Agisci subito per:

- cambiare la password;
- attivare o rafforzare i sistemi di sicurezza disponibili;
- controllare movimenti, accessi e notifiche;
- contattare la banca o il servizio coinvolto;
- bloccare carte o strumenti di pagamento, se serve.

9. Metti per iscritto il problema

Anche se all'inizio hai parlato con un chatbot o al telefono, a un certo punto conviene scrivere il problema in modo ordinato.

Una buona segnalazione dovrebbe contenere:

- chi sei;
- quale servizio è coinvolto;
- che cosa è successo;
- quando è successo;
- quale danno o difficoltà hai subito;
- quali prove hai conservato;
- che cosa stai chiedendo.

10. Non aspettare troppo se il danno è concreto

Se il problema riguarda denaro, accesso a un account, uso improprio dei dati, impossibilità di utilizzare un servizio importante o rischio di ulteriore danno, è bene non aspettare troppo.

11. Distingui tra disagio, danno e urgenza

Per orientarti meglio, può essere utile farti tre domande:

- si tratta solo di un fastidio o c'è un danno concreto?
- il danno è economico, pratico, reputazionale o legato ai dati personali?
- c'è urgenza, cioè il problema può peggiorare in poco tempo?

12. Una regola pratica: prima documenta, poi contesta

Quando succede qualcosa di poco chiaro, molte persone fanno il contrario: prima discutono, poi cercano le prove. Di solito è meglio procedere così:

- documenta;
- verifica;
- proteggi dati e accessi, se serve;

- contesta in modo chiaro;
- chiedi revisione e risposta tracciabile.

In sintesi

- ricostruisci i fatti;
- salva subito le prove;
- verifica con calma;
- usa canali ufficiali;
- chiedi spiegazioni chiare;
- domanda una revisione del caso;
- proteggi dati, account e strumenti di pagamento, se necessario;
- metti tutto per iscritto.

Non serve sapere con precisione quale tecnologia c'è dietro. Quello che conta è non restare passivi davanti a un problema poco chiaro o a una decisione che ti penalizza. Muoversi con ordine e tempestività è spesso il modo migliore per limitare il danno e far valere le proprie ragioni.

11. Le associazioni dei consumatori: un aiuto concreto

Quando un servizio digitale è poco chiaro, quando un chatbot non risponde davvero al problema, quando un acquisto online si complica o quando una decisione automatizzata sembra ingiusta, il cittadino può sentirsi solo e disorientato.

È proprio in questi casi che il supporto di un'associazione dei consumatori può fare la differenza.

Perché rivolgersi a un'associazione dei consumatori

Oggi molti problemi nascono in ambienti digitali: piattaforme online, e-commerce, servizi automatizzati, app, sistemi di pagamento, chatbot, account sospesi, rimborsi bloccati, offerte poco trasparenti, difficoltà a parlare con un operatore umano.

In queste situazioni non è sempre facile capire:

- se il comportamento del servizio è corretto;
- quali diritti si possono far valere;
- quali documenti conviene conservare;
- come scrivere una contestazione efficace;
- a chi rivolgersi e con quali tempi.

Un'associazione dei consumatori aiuta proprio a fare ordine.

Un supporto pratico, non solo informativo

Rivolgersi alle Associazioni dei Consumatori non significa solo chiedere un'opinione. Significa poter contare su un punto di riferimento che può aiutarti a leggere meglio il problema e a scegliere il passo successivo più adatto.

A seconda del caso, il supporto può riguardare:

- orientamento sui tuoi diritti;
- aiuto nel ricostruire i fatti;
- indicazioni su quali prove conservare;
- supporto nella scrittura di richieste, reclami o diffide;
- aiuto nel contatto con aziende, gestori o piattaforme;
- indicazioni sui canali più adatti da utilizzare;
- supporto nelle procedure di tutela e composizione delle controversie.

Quando è utile contattare l'associazione

Può essere utile rivolgersi all'associazione quando:

- ricevi risposte automatiche poco chiare o contraddittorie;
- non riesci a parlare con una persona;
- un rimborso, un recesso o una contestazione vengono respinti senza spiegazioni adeguate;
- un pagamento o un account vengono bloccati;
- sospetti un uso scorretto dei tuoi dati;
- ritieni di aver subito una pratica poco trasparente o ingannevole;
- hai dubbi su offerte, contratti, consensi o richieste digitali;
- pensi di essere stato vittima di una truffa o di un contenuto falso.

In tutti questi casi, il problema non va affrontato solo a intuito. Un confronto tempestivo può aiutare a evitare errori, perdite di tempo e ulteriori danni.

Perché è utile muoversi presto

Molti cittadini chiedono aiuto solo dopo aver perso tempo tra chatbot, messaggi automatici, email senza risposta e passaggi poco chiari. Ma spesso intervenire prima è meglio.

Muoversi presto può servire a:

- conservare correttamente le prove;
- evitare che il problema peggiori;
- contestare in tempi utili;

- scegliere subito il canale più efficace;
- impostare meglio la richiesta fin dall'inizio.

Anche quando il danno sembra piccolo, una valutazione tempestiva può essere utile per capire se si tratta solo di un disservizio o di qualcosa di più serio.

Un aiuto anche per orientarsi nella complessità digitale

Oggi molti servizi digitali usano linguaggi tecnici, condizioni lunghe, procedure automatizzate e comunicazioni standard. Questo rende difficile per il cittadino capire che cosa stia realmente accadendo.

L'associazione può aiutare anche in questo: tradurre la complessità in indicazioni pratiche, spiegare con parole semplici quali sono i punti importanti e aiutarti a capire quali passi conviene fare davvero.

Non solo tutela individuale

C'è anche un altro aspetto importante. Quando più cittadini segnalano problemi simili, le associazioni dei consumatori possono individuare criticità ricorrenti, pratiche scorrette diffuse o difficoltà che meritano attenzione.

Questo significa che chiedere aiuto non serve solo a gestire il singolo caso, ma può contribuire anche a rafforzare la tutela dei consumatori in modo più generale.

Un punto di riferimento vicino al cittadino

L'Associazione dei Consumatori può rappresentare un supporto concreto per chi vuole affrontare con maggiore sicurezza i problemi legati ai servizi digitali, all'uso dei dati, ai contenuti online, agli acquisti su piattaforma e alle decisioni automatizzate.

Per questo, in caso di dubbio, è utile non aspettare troppo e chiedere un primo orientamento.

12. Scheda pratica finale

Questa scheda riassume i comportamenti più utili da tenere quando usi servizi digitali, chatbot, piattaforme online o contenuti che potrebbero essere generati o influenzati dall'Intelligenza Artificiale.

La regola di fondo è semplice: fermarsi, verificare, documentare e poi agire.

Le 5 cose da ricordare sempre

1. **Non fidarti in automatico della prima risposta.** Se una risposta riguarda soldi, diritti, contratti, rimborsi, pagamenti, dati personali o accesso a un servizio, verifica sempre anche da una fonte ufficiale.
2. **Non agire di fretta.** Se un messaggio ti mette pressione, ti chiede di decidere subito o di condividere dati, fermati.
3. **Salva tutto ciò che può essere utile.** Screenshot, email, chat, numeri pratica, date, orari e documenti possono diventare importanti se nasce un problema.

4. **Proteggi i tuoi dati.** Non comunicare con leggerezza password, codici temporanei, documenti, dati bancari o altre informazioni sensibili.
5. **Chiedi spiegazioni chiare.** Se una decisione ti penalizza o una risposta è vaga, chiedi una spiegazione comprensibile e, se serve, una revisione del caso.

Se succede questo, fai questo

Situazione	Cosa fare
Se un chatbot ti dà una risposta importante	• non fermarti alla sola chat; • controlla il sito ufficiale, il contratto o la comunicazione scritta; • fai uno screenshot della risposta ricevuta; • verifica se esiste un contatto umano.
Se un pagamento viene bloccato	• non ripetere subito la stessa operazione più volte; • controlla se hai ricevuto una comunicazione ufficiale; • contatta la banca o il servizio dai canali ufficiali; • conserva data, ora, importo e messaggio di errore.
Se un account viene sospeso o limitato	• salva subito la schermata; • verifica se è indicata una motivazione; • controlla email e notifiche ufficiali; • chiedi una revisione del caso e una spiegazione più chiara.
Se ricevi un messaggio urgente che chiede dati o denaro	• non cliccare subito; • non condividere codici, password o documenti; • controlla il mittente; • entra dal sito o dall'app ufficiale, senza usare il link ricevuto; • se hai dubbi, interrompi e verifica.
Se un'offerta o un contratto non ti sono chiari	• non accettare subito; • rileggi con calma condizioni, costi e durata; • verifica se ci sono rinnovi automatici, limiti o penali; • conserva una copia del testo che hai letto prima di confermare.
Se pensi di aver subito una truffa	• blocca subito ciò che puoi bloccare; • cambia le password coinvolte; • contatta la banca o il servizio interessato; • salva tutte le prove; • ricostruisci i passaggi fatti.
Se sospetti un uso scorretto dei tuoi dati	• controlla quali dati hai comunicato; • rileggi informativa e impostazioni privacy;

	• conserva le schermate utili; • chiedi chiarimenti sul trattamento dei dati e sulle possibilità di rettifica, opposizione o cancellazione, quando applicabili.

Documenti e prove da conservare

- screenshot delle schermate;
- email e messaggi ricevuti;
- conversazioni in chat;
- numeri pratica o codici identificativi;
- data e ora degli eventi;
- link, indirizzi web e nome del servizio;
- contratto, condizioni o regolamento consultato;
- eventuali ricevute, importi o movimenti di pagamento.

Domande utili da farti subito

- Che cosa è successo esattamente?
- Quale danno o difficoltà mi sta creando?
- Ho salvato le prove principali?
- La risposta ricevuta è davvero chiara?
- Sto usando un canale ufficiale?
- Mi stanno mettendo fretta?
- Mi stanno chiedendo dati o soldi in modo insolito?
- Posso chiedere una verifica o una revisione del caso?

La regola finale

Davanti a un servizio digitale poco chiaro, a una decisione automatica che ti penalizza o a un contenuto sospetto, non devi scegliere tra fidarti ciecamente e diffidare di tutto. La scelta migliore è un'altra: usare la tecnologia con attenzione, fare verifiche semplici e agire con metodo.

Per ulteriori informazioni e orientamento

Inserire i riferimenti delle AACC

tu che ne sai?

L'intelligenza artificiale più sicura per tutti

Promosso da

UNC CONSUMATORI.IT

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

CITTADINANZATTIVA

ADOC Associazione Difesa Orientamento Consumatori APS

Federconsumatori

Finanziato dal MIMIT - D.D. 12 maggio 2025