Privacy dei dati: una guida per singoli utenti e famiglie

Proteggi le tue informazioni online e salvaguarda la tua digital footprintl.

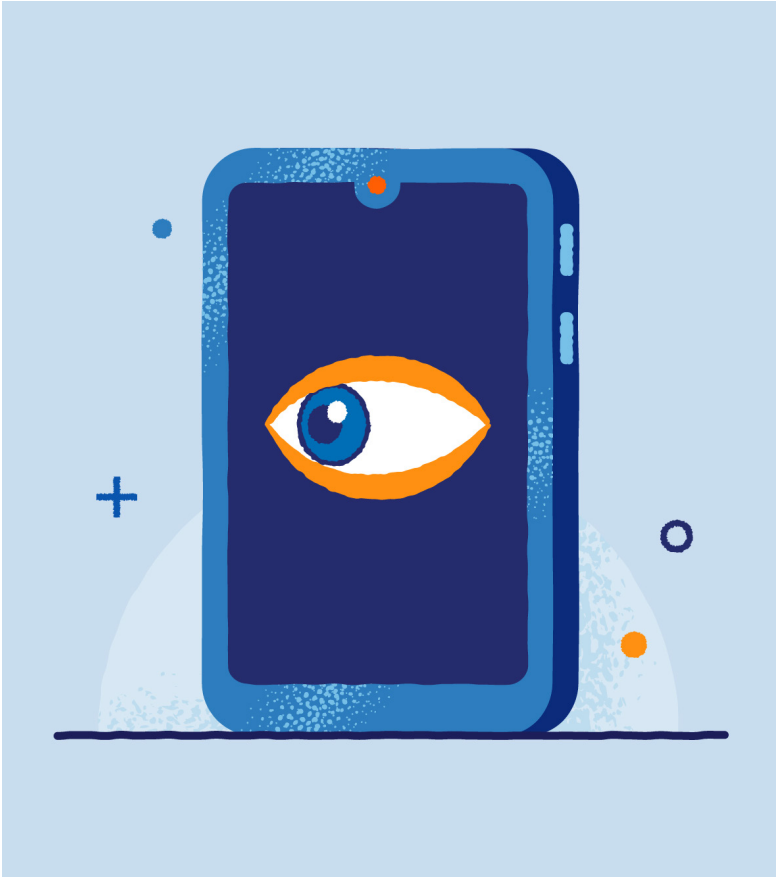
panda

Sommario

01.
Nozioni di base sulla privacy dei dati

Nell'era digitale, la privacy dei dati è diventata una protagonista poco conosciuta. È la misteriosa nozione che si nasconde dietro ogni messaggio e-mail che si invia, ogni transazione che si effettua e ogni sito che si visita. Eppure, per molti, la privacy dei dati è un concetto poco conosciuto, spesso trascurato finché non è troppo tardi.

La privacy dei dati ha come scopo garantire la protezione delle informazioni personali. Aziende, governi e criminali informatici cercano costantemente di acquisire queste informazioni per svariati motivi e, per questo motivo, di vitale importanza comprendere come mantenere i dati sicuri. Fortunatamente, questo e-book include informazioni complete sulla privacy dei dati e fornisce tutte le indicazioni necessarie per consentirti di assumere il controllo della tua digital footprint.



Che cos'è la privacy dei dati?

La privacy dei dati è il controllo che un individuo o un'organizzazione esercitano sulle proprie informazioni sensibili, sia che vengano archiviate o raccolte. È la capacità di determinare chi ha accesso a questi dati, come vengono utilizzati e le misure di salvaguardia adottate per proteggerli dall'esposizione non autorizzata.

I dati personali associati alla privacy dei dati includono informazioni sensibili come nomi, indirizzi, codici fiscali e dati finanziari, ma riguardano anche dati meno apertamente personali, come cronologia di navigazione, dati sulla posizione, indirizzi IP e acquisti online. Inoltre, possono comprendere dati biometrici, cartelle cliniche e dettagli sull'occupazione.

Il concetto di privacy dei dati affonda le sue radici negli albori dell'informatica, quando le informazioni personali venivano archiviate elettronicamente per diversi scopi. Con l'espansione dello scenario digitale, le preoccupazioni relative all'uso improprio dei dati e alla violazione della privacy sono aumentate rapidamente.

L'evoluzione dei social media ha ulteriormente aggravato tali preoccupazioni. Inoltre, con la libera condivisione da parte degli utenti delle proprie informazioni personali su piattaforme come Facebook e Twitter, la quantità di dati generati ha raggiunto livelli senza precedenti.

Perché la privacy dei dati è importante

Con il ritmo vertiginoso dello sviluppo tecnologico, la protezione dei dati e della privacy non è più un optional, ma un requisito fondamentale. La privacy dei dati dipende dalla capacità degli individui di controllare la propria digital footprint.

Ogni volta che ci colleghiamo a Internet, generiamo una grande quantità di dati. Dai semplici "Mi piace" sui social media alle nostre abitudini di acquisto, questi dati apparentemente innocui tracciano un quadro vivido di chi siamo. Quando questi dati privati finiscono nelle mani sbagliate, le ripercussioni possono includere:

Furto d'identità

I dati personali possono cadere nelle mani sbagliate, dando luogo a frodi d'identità, per cui gli individui possono essere vittime di transazioni non autorizzate o di attività criminali condotte utilizzando il loro nome.

Frode finanziaria

Ottenendo l'accesso a informazioni finanziarie sensibili, i criminali informatici possono effettuare transazioni fraudolente, con conseguenti gravi perdite monetarie per le loro vittime.

Ripercussioni legali

Nel caso in cui non vengano rispettate le leggi e le normative sulla privacy dei dati, le aziende rischiano di incorrere in pesanti sanzioni e azioni legali, con danni per la propria reputazione e le finanze aziendali.

Perdita di fiducia

Le aziende possono perdere la fiducia dei propri clienti, con effetti negativi sulla fidelizzazione e introiti commerciali.

Aumento dei crimini informatici

Con l'incremento di dati importanti facilmente accessibili, il rischio di attacchi da parte dei criminali informatici può aumentare in modo esponenziale.

Perdita della privacy

lenza la privacy dei dati, la nostra vita personale rischia di diventare un libro aperto, accessibile a chiunque.

Manipolazione e sfruttamento

I dati possono essere utilizzati per manipolare comportamenti e decisioni, spesso all'insaputa o senza il consenso dell'individuo.

Protezione dei dati, privacy dei dati e sicurezza dei dati

La protezione, la privacy e la sicurezza dei dati sono tre concetti strettamente connessi ma distinti nel mondo dei dati digitali.

In breve, la protezione, la privacy e la sicurezza dei dati operano in sintonia. Ciascuna di esse ha un ruolo distinto, ma insieme creano un ambiente digitale sicuro.

02.
Informazioni personali e informazioni personali sensibili

Nell'ampio scenario rappresentato dalla privacy dei dati, comprendere la distinzione tra informazioni personali e informazioni personali sensibili è fondamentale per la conformità legale, la gestione dei rischi e altre considerazioni etiche. Tale distinzione consente di fornire informazioni sulle pratiche di gestione dei dati, implementare le misure di sicurezza e aiutare a ridurre al minimo i potenziali danni alle persone qualora i dati venissero compromessi.

Questa sezione descrive i livelli di classificazione dei dati, con approfondimenti su come salvaguardare i dettagli più intimi della tua identità digitale.

Cosa sono le informazioni personali?

Le informazioni personali, spesso chiamate anche dati personali, sono tutte le informazioni che possono essere utilizzate per identificare un individuo specifico. Comprendono una vasta gamma di dati che possono essere collegati a una determinata persona. A seconda del contesto, possono contenere nomi, indirizzi, numeri di telefono e altro.

Come controllare le tue informazioni personali

Per controllare in modo efficiente le tue informazioni personali, è essenziale adottare misure proattive che migliorino la tua privacy e sicurezza online. Di seguito sono elencati alcuni suggerimenti importanti da tenere a mente .

Limitare l'esposizione sui social media

Controlla e modifica le impostazioni della privacy sulle piattaforme dei social media per verificare chi può vedere i tuoi post e le tue informazioni personali.

Pubblicare contenuti in modo consapevole

Prima di condividere i tuoi dati personali online, considera le potenziali conseguenze e se è davvero necessario divulgare tali informazioni.

Esaminare le politiche sulla privacy

Prenditi il tempo necessario per leggere e comprendere le politiche sulla privacy dei siti Web e delle app che utilizzi, per verificare in che modo vengono raccolti, archiviati e condivisi i tuoi dati.

Non consentire la raccolta di dati

Quando possibile, non consentire la raccolta di dati e scegli servizi che richiedono solo le informazioni essenziali.

Cosa sono le informazioni personali sensibili?

Le informazioni personali sensibili sono una categoria di informazioni personali considerate più critiche che richiedono livelli di protezione più elevati. Includono dettagli che, se rivelati, possono avere conseguenze molto gravi come il furto di identità, il cyberstalking o la discriminazione.

Come assumere il controllo delle informazioni personali sensibili

Al giorno d'oggi, il controllo delle tue informazioni personali sensibili è più cruciale che mai. Con l'aumento delle violazioni di dati e altre minacce informatiche, è essenziale adottare misure proattive per salvaguardare questi dati preziosi.

Invio di un modulo di richiesta di accesso dell'interessato (DSAR)

- **Conosci i tuoi diritti:** ai sensi del Regolamento generale sulla protezione dei dati (GDPR), hai il diritto di chiedere a un'organizzazione se elabora o meno i tuoi dati.
- **Informazioni di accesso:** lla richiesta di accesso dell'interessato (DSAR) ti consente di accedere alle informazioni archiviate su di te per verificarne l'utilizzo.
- **Richiesta di rettifica:** richiedi la rettifica dei dati errati o la loro cancellazione; le aziende sono tenute a rispettare tale richiesta entro un mese solare per il GDPR e 45 giorni per il California Consumer Privacy Act (CCPA).

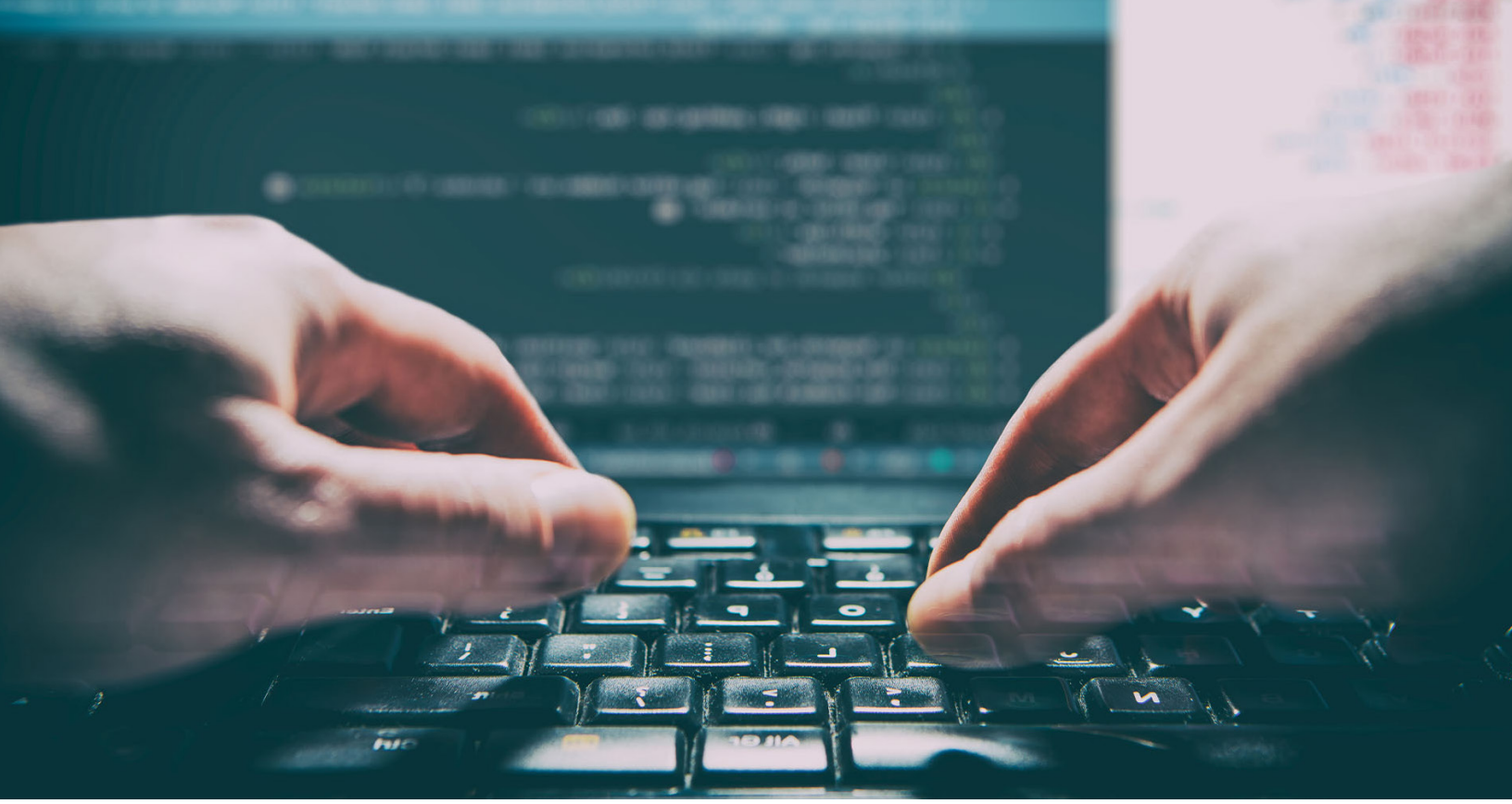
Utilizzo dei collegamenti "Non vendere o condividere le mie informazioni personali"

- **Controllo dei siti web aziendali:** cerca le opzioni complete come "Non vendere o condividere le mie informazioni", ai sensi del California Privacy Rights Act (CPRA), sulle pagine home dei siti Web aziendali e sulle pagine relative alle norme sulla privacy.
- **Non autorizzare il trattamento dei tuoi dati:** non autorizzare la vendita o la condivisione dei tuoi dati personali o sensibili con terze parti; le aziende hanno l'obbligo legale a garantire la conformità.

Non consentire la raccolta di dati su siti Web o browser

- **Ricerca online:** esegui una ricerca online con il tuo nome per scoprire se le tue informazioni sono elencate nei siti Web di broker di dati quali Radaris, Pipl, Spokeo e Whitepages.
- **Richiesta di rimozione dei dati:** visita le pagine di cancellazione delle informazioni di queste piattaforme o invia una richiesta via e-mail per ottenere la rimozione dei tuoi dati.
- **Utilizzo delle risorse:** utilizza risorse come Privacy Rights Clearinghouse per ottenere un elenco completo dei siti Web e le relative opzioni di cancellazione.
- **Verifica delle politiche sulla privacy:** verifica le politiche sulla privacy dei tuoi istituti finanziari per disattivare la condivisione dei dati con eventuali intermediari.

03.
Introduzione alle violazioni di dati



Forse hai sentito parlare degli attacchi subiti dalle aziende che hanno subito gravi violazioni di dati e hai pensato: “Com’è potuto succedere?” o ”E se fosse capitato a me?” Una violazione di dati può essere allarmante e avere conseguenze molto gravi, come la frode delle carte di pagamento o persino il furto di identità.
La sezione successiva è un approfondimento che descrive gli effetti che le violazioni dei dati possono avere, come si verificano e come è possibile prevenirle.

Che cos’è una violazione di dati?

Una violazione di dati è un incidente di sicurezza in cui informazioni private, riservate o sensibili vengono esposte o rubate da qualcuno senza autorizzazione. Le violazioni si verificano per vari motivi, dall’errore umano agli attacchi dannosi, e le conseguenze possono essere importanti. Chiunque è a rischio di subire una violazione di dati, soprattutto se dispone di account che non sono protetti.

Possibili conseguenze delle violazioni di dati:

- **Credenziali rubate**
  Esempio: dei criminali informatici potrebbero ottenere l'accesso non autorizzato a un database contenente nomi utente e password degli utenti di una piattaforma di social media, con la conseguente appropriazione generale degli account e l'utilizzo improprio delle informazioni personali.

- **Furto d'identità**
  Esempio: un criminale informatico potrebbe utilizzare informazioni personali rubate, come codici fiscali e indirizzi, per richiedere in modo fraudolento prestiti e carte di credito a nome delle vittime, causando danni finanziari e problemi relativi all'identità.

- **Risorse compromesse**
  Esempio: un malware potrebbe infettare una rete aziendale, consentendo agli aggressori di controllare sistemi critici e dati sensibili, interrompendo le operazioni e causando perdite finanziarie significative.

- **Frode delle carte di pagamento**
  Esempio: un attacco informatico potrebbe colpire il sistema di elaborazione dei pagamenti di un rivenditore online, provocando il furto dei dati delle carte di credito dei clienti, che possono quindi essere utilizzati per effettuare acquisti non autorizzati.

- **Accesso di terze parti agli account**
  Esempio: un provider di servizi cloud potrebbe subire una violazione di dati, consentendo a terzi non autorizzati di accedere a file e informazioni sensibili archiviati dei suoi clienti, con conseguente potenziale fuga di dati e violazione della privacy.

Come si verificano?

Le violazioni di dati sono un tipo di crimine informatico se eseguiti con fini dannosi, ma possono anche essere causate da un errore involontario da parte di un utente con accesso autorizzato a tali dati. Le cause delle violazioni di dati includono:

Utenti interni con fini dannosi

Persone con accesso al database che abusano intenzionalmente dei propri privilegi di accesso per rubare o divulgare informazioni sensibili.

Utenti esterni con fini dannosi

Persone esterne all'organizzazione che attaccano un database tramite phishing, malware, attacchi di vulnerabilità o attacchi Denial of Service (DoS).

Azioni fortuite di utenti interni

Persone autorizzate all'accesso che espongono in modo accidentale i dati a causa di errori o mancanza di misure di sicurezza. A livello tecnico, questo tipo di incidente viene classificato come fuga di dati, poiché si tratta di un errore interno; tuttavia, le conseguenze per le persone interessate sono le stesse, con conseguenti ripercussioni legali per le aziende.

Fasi delle violazioni di dati

Al contrario di quanto può suggerire il termine, le violazioni di dati con scopi dannosi non vengono condotte da malintenzionati vestiti di nero che si intrufolano in un edificio con una chiavetta USB, ma piuttosto da persone che, da una posizione remota, progettano come hackerare un database.

Tuttavia, non tutte le violazioni di dati sono dannose: alcune sono il risultato di un errore umano o di una negligenza, ma esamineremo questo argomento in modo più approfondito nella sezione successiva. Di seguito sono elencate le tre fasi di una violazione intenzionale dei dati.

1. Ricerca

Nella fase iniziale di una violazione di dati, gli utenti malintenzionati scelgono un obiettivo – solitamente un'azienda o un'organizzazione con accesso a dati personali – e cercano il modo di infiltrarsi nel database del loro obiettivo.

Gli aggressori raccolgono dettagli quali informazioni sui dipendenti, registri finanziari e budget per la sicurezza. Inoltre, cercano vulnerabilità come password vulnerabili, software obsoleti o connessioni di rete non protette.

2. Attacco

Utilizzando ciò che hanno appreso durante la ricerca, gli aggressori ora possono attaccare il sistema di dati. Ecco alcuni modi comuni con cui possono ottenere l'accesso ai sistemi o alle reti aziendali:

- **Credenziali rubate:**
  I criminali informatici possono raccogliere nomi utente e password compromessi attraverso dark web, phishing, attacchi di forza bruta o persino furti fisici di dispositivi, per impersonare utenti legittimi e ottenere l'accesso ai sistemi.

- **E-mail di phishing**
  Gli aggressori utilizzano anche le informazioni personali acquisite durante le loro ricerche, come titoli di lavoro o nomi di colleghi, per indurre i propri obiettivi a fornire credenziali o a fare clic su un collegamento dannoso che scarica malware sul loro computer.

- **Malware**
  I criminali informatici utilizzano software dannosi per infettare segretamente e assumere il controllo dei computer o della rete della vittima per rubare dati.

- **Sfruttamento delle vulnerabilità**
  Gli aggressori sfruttano vulnerabilità come password vulnerabili, configurazioni errate o sistemi privi di patch presenti nei sistemi informatici delle aziende per ottenere l'accesso.

- **Attacchi Denial of Service (DoS)**
  Questi tipi di attacco sovraccaricano un sito Web creando un traffico falso in eccesso fino a renderlo inutilizzabile da parte degli utenti effettivi. Questo attacco funge da distrazione da altre vulnerabilità di sicurezza, in modo che gli aggressori possano effettuare le violazioni di dati.

3. Estrazione di dati

Una volta che gli aggressori hanno ottenuto l'accesso al sistema o alla rete del bersaglio, possono individuare ed estrarre dati preziosi o sensibili, comprese informazioni personali, registri finanziari o qualsiasi altro dato che è possibile vendere sul dark web.

I dati estratti vengono quindi copiati o trasferiti sui server degli aggressori, dove possono controllarli e sfruttarli. Spesso le aziende non si accorgono del furto di dati fino a quando una terza parte, come le forze dell'ordine, i fornitori di servizi o i clienti, non denunciano la violazione.

04.
Protezione di dati e informazioni personali

Sono disponibili alcuni semplici modi per garantire la sicurezza dei propri dati online. Panda Dome ha un piano di protezione per qualsiasi stile di vita, per consentirti di navigare senza preoccupazioni.

Sicurezza di rete

La sicurezza della rete prevede l'implementazione di misure per proteggere le reti utilizzate dai computer da accessi non autorizzati, attacchi informatici e violazioni dei dati. Questa include la protezione dell'infrastruttura di rete, il monitoraggio del traffico e l'implementazione di protocolli di crittografia affidabili.

Utilizzo di reti Wi-Fi pubbliche in sicurezza

Quando ti connetti a reti Wi-Fi pubbliche, adotta misure di sicurezza per impedire l'accesso non autorizzato a dati sensibili.

Utilizzo di una VPN

Migliora la privacy e la sicurezza online crittografando il traffico Internet quando accedi alle reti pubbliche.

Installazione di un firewall

Implementa una barriera contro l'accesso non autorizzato alla tua rete, aggiungendo un ulteriore livello di difesa contro le minacce informatiche.

Autenticazione e controllo degli accessi

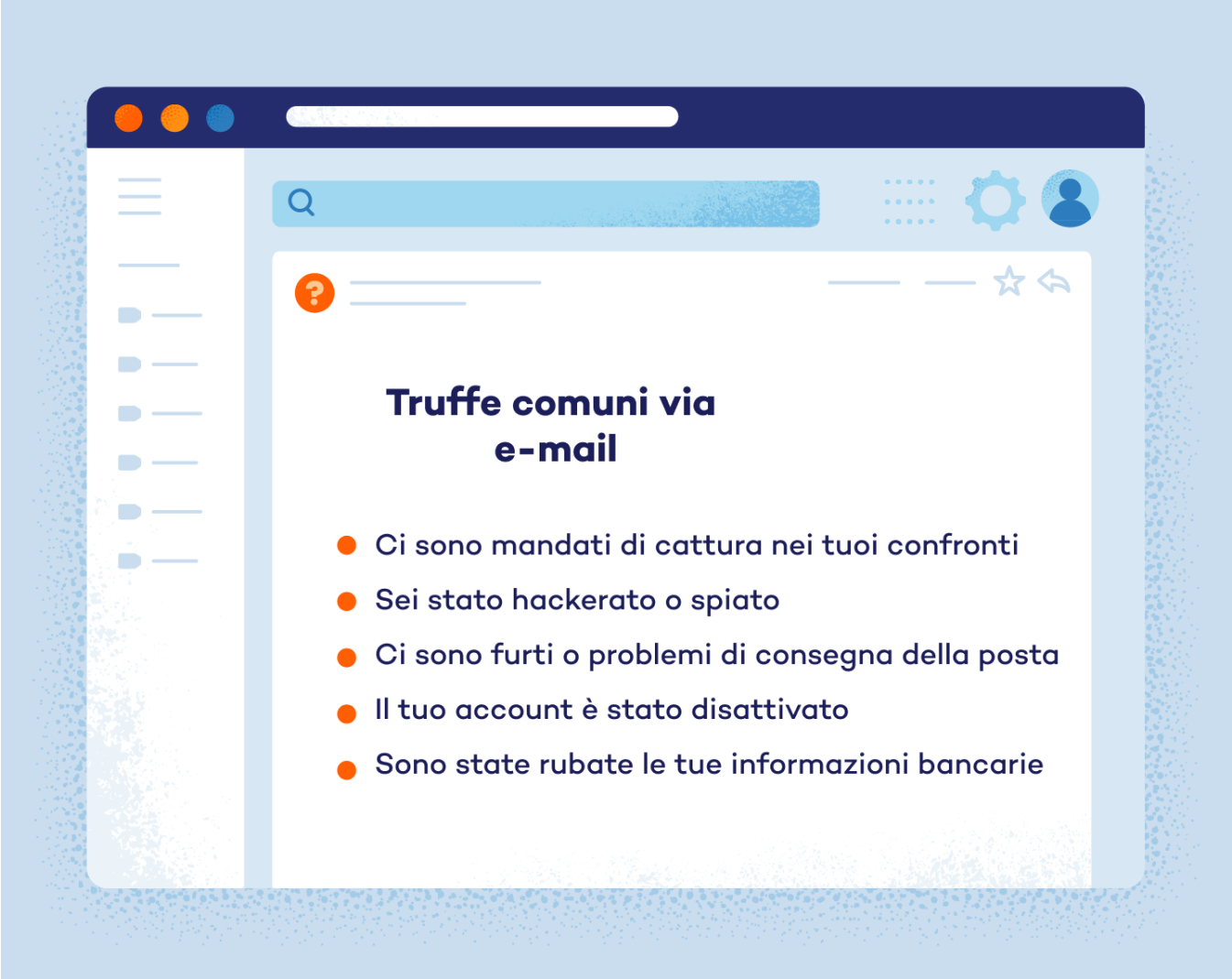
L'autenticazione e il controllo degli accessi sono componenti essenziali per la privacy dei dati, poiché garantiscono che unicamente le persone o i sistemi autorizzati possano accedere a dati o risorse sensibili. Queste misure consentono di verificare l'identità degli utenti e di imporre restrizioni alle loro azioni all'interno di una rete o di un sistema.

- **Selezione di password sicure e univoche**
  Rafforza la sicurezza dei tuoi account creando password complesse univoche per ciascun account, per mitigare il rischio di accessi non autorizzati.

- **Impostazione dell'autenticazione in due passaggi**
  Aggiungi un ulteriore livello di sicurezza richiedendo un metodo secondario di verifica, come un codice inviato a un dispositivo attendibile, oltre a una password.

- **Monitoraggio delle informazioni degli account**
  Controlla regolarmente l'attività dei tuoi account per rilevare comportamenti sospetti o tentativi di accesso non autorizzati. Segnala tempestivamente qualsiasi attività sospetta o tentativo di accesso non autorizzato alle autorità competenti o ai fornitori di servizi.

- **Evitare la condivisione dei codici ricevuti tramite SMS o e-mail**
  Evita di condividere i codici di verifica ricevuti tramite SMS o e-mail, poiché potrebbero essere intercettati da aggressori che tentano di accedere ai tuoi account senza autorizzazione.



Protezione e recupero dei dati

La protezione e il recupero dei dati si riferiscono alle strategie e alle tecnologie utilizzate per salvaguardare e ripristinare i dati in caso di cancellazione accidentale, danneggiamento o attacco informatico. Prevede l'implementazione di soluzioni di backup, crittografia e piani di ripristino di emergenza per garantire l'integrità e la disponibilità dei dati.

Backup dei dati

proteggiti dalla perdita di dati dovuta ad attacchi informatici o a problemi hardware eseguendo regolarmente il backup di file e documenti importanti.

Installazione di software antivirus

proteggiti da malware e altre minacce informatiche installando un software antivirus affidabile per rilevare e rimuovere eventuali software dannosi dai tuoi dispositivi.

Nozioni generali in materia di sicurezza informatica

È importante riconoscere i segnali più comuni di pirateria informatica in modo da poter agire il prima possibile e recuperare i tuoi account.

Ecco alcuni segnali di avvertimento che possono indicare un attacco informatico:

- Aumento notevole dell'utilizzo di Internet da parte dei tuoi dispositivi
- Rallentamento della velocità operativa dei dispositivi
- La batteria si scarica rapidamente senza spiegazioni
- Ricezione di richieste non autorizzate di modificare le password
- Download automatico di nuovi software o applicazioni

05.
FAQ sulla privacy dei dati

In questa sezione troverai le risposte ad alcune delle domande più comuni sulla privacy dei dati

Qual è lo scopo del Data Privacy Act?

Lo scopo del Data Privacy Act, ossia della legge sulla privacy dei dati, è quello di salvaguardare le informazioni personali degli individui regolandone la raccolta, il trattamento e l'archiviazione, promuovendo così la trasparenza e la sicurezza dei dati.

Quali sono le 4 categorie della privacy dei dati?

Le quattro categorie della privacy dei dati corrispondono a diversi livelli di accesso e sensibilità:

Privacy dei dati pubblici

Si riferisce alle informazioni destinate al consumo pubblico, come le informazioni di contatto generali dell'azienda, e in genere non richiede una rigorosa tutela della privacy.

Privacy esclusiva dei dati interni

Si riferisce ai dati accessibili solo all'interno dell'organizzazione e in genere richiede misure di salvaguardia per impedire l'accesso non autorizzato da parte di soggetti esterni.

Privacy dei dati riservati

Si riferisce alle informazioni sensibili che richiedono misure di privacy rafforzate per limitare l'accesso alle persone autorizzate all'interno dell'organizzazione.

Privacy dei dati riservati

Si riferisce a dati altamente sensibili soggetti a rigorosi controlli della privacy, che spesso richiedono autorizzazioni speciali per l'accesso e la gestione, allo scopo di ridurre al minimo il rischio di esposizione non autorizzata o uso improprio.

Che cosa si intende per dati sulla privacy?

I dati sulla privacy, noti anche come informazioni di identificazione personale (PII), comprendono qualsiasi informazione che possa identificare direttamente o indirettamente un individuo. Questi includono dettagli identificativi di base come nome e data di nascita, informazioni di contatto come indirizzi e-mail e numeri di telefono, dati finanziari come numeri di carta di credito e informazioni sensibili come i dati sanitari.