

# 99 suggerimenti

per la protezione dei tuoi dati personali



Tutto il materiale contenuto nel presente documento è oggetto di diritti esclusivi da parte della società Karon srl.

Ne è vietata quindi ogni riproduzione, anche parziale, con qualsiasi mezzo, senza l'autorizzazione scritta della stessa società Karon srl.

Con il quotidiano utilizzo delle nuove tecnologie, mantenere le informazioni personali al riparo dalle minacce esterne sta diventando sempre più importante.

Per farlo è necessario adottare le metodologie più corrette, sia per quanto riguarda i comportamenti che per gli strumenti utilizzati.

In rete puoi trovare una grande quantità di informazioni per proteggere i tuoi dispositivi multimediali dalle minacce esterne e utilizzare internet in modo sicuro.

Le risorse a disposizione sono però talmente tante che è facile fare confusione, soprattutto se non si è esperti di tecnologia.

Abbiamo compilato un elenco di 99 semplici suggerimenti per aiutarti a mantenere i tuoi dati al sicuro.



# **99 SUGGERIMENTI**

**per la protezione dei tuoi dati personali**

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **1** **CRIPTA I TUOI DATI**

Utilizza programmi specifici per criptare i tuoi dati personali, rendendoli in tal modo inaccessibili a chi non conosce la password che hai impostato per proteggerli.

## **2** **EFFETTUA SEMPRE IL BACKUP DEI TUOI DATI**

Crea una copia duplicata dei tuoi dati personali, in modo che non vadano irrimediabilmente persi qualora il dispositivo nel quale sono contenuti venga rubato o compromesso.

## **3** **UTILIZZA IL “CLOUD” COME OPZIONE PREFERENZIALE PER IL BACKUP**

Il cloud rappresenta la soluzione ideale per effettuare il backup in quanto i dati, non memorizzati su un dispositivo locale, sono facilmente accessibili da remoto.

# 99 suggerimenti

per la protezione dei tuoi dati personali

4

## **DOTATI DI UNA PROTEZIONE ANTIMALWARE**

Un malware è un software progettato per infiltrarsi in un computer e danneggiarlo.

Dotati di un buon anti-malware sempre aggiornato per proteggere i maniera efficace i tuoi dispositivi.

5

## **RENDI ILLEGGIBILI I DISCHI RIGIDI DEI VECCHI DISPOSITIVI**

Rendi illeggibili i dischi rigidi prima di eliminarli.

Dopo aver eseguito il backup dei dati e trasferito i file altrove, utilizza un software specifico per eliminare definitivamente i dati dal disco.

6

## **INSTALLA GLI AGGIORNAMENTI DEL SISTEMA OPERATIVO**

Gli aggiornamenti del sistema operativo che utilizzi proteggono il tuo dispositivo dalle minacce più recenti. Imposta l'installazione automatica degli aggiornamenti in modo da essere sempre protetto.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**7**

## **AGGIORNA COSTANTEMENTE I SOFTWARE CHE UTILIZZI**

L'aggiornamento costante dei software che utilizzi ti mette al riparo dai rischi legati alle versioni obsolete. Imposta l'installazione automatica degli aggiornamenti in modo da essere sempre protetto.

**8**

## **PROTEGGI LA TUA RETE WIRELESS**

Proteggi con una password la rete wireless di casa, in modo da evitare di condividere inavvertitamente informazioni private con persone che si potrebbero collegare ad essa senza autorizzazione.

**9**

## **SPEGNI I DISPOSITIVI DOPO AVERLI UTILIZZATI**

Quando hai terminato di utilizzare un dispositivo, ricordati sempre di spegnerlo! Lasciare i dispositivi accesi e connessi alla rete mette a serio rischio la tua privacy.

# 99 suggerimenti

per la protezione dei tuoi dati personali

10

## UTILIZZA UNA “PASSPHRASE”, NON UNA “PASSWORD”

La passphrase è una password complessa. Per comporla usa la prima lettera di ogni parola di una frase semplice da ricordare, assieme a una combinazione di numeri e caratteri speciali.

11

## PRATICA IL PRINCIPIO DEL PRIVILEGIO MINIMO (POLP)

Non accedere a un computer come amministratore (a meno che non sia necessario farlo per eseguire attività specifiche), in modo da evitare i rischi legati alla navigazione con questo tipo di accesso.

12

## UTILIZZA UN FIREWALL

I firewall bloccano programmi pericolosi, virus o spyware prima che si infiltrino nel sistema. L'utilizzo di un firewall, unito a un buon antivirus, protegge in maniera efficace i tuoi dispositivi.



# 99 suggerimenti

per la protezione dei tuoi dati personali

## **13** CRITTOGRAFA I DATI SUI TUOI DISPOSITIVI DI ARCHIVIAZIONE

La crittografia dei dati sui dispositivi di archiviazione rimovibili può rendere più complicato (anche se non impossibile) l'accesso ai tuoi dati personali in caso di smarrimento o furto del dispositivo.

## **14** PRESERVA LE CREDENZIALI CHE UTILIZZI PER ACCEDERE AI TUOI DISPOSITIVI

Proteggi le tue credenziali di accesso!  
Lasciare incollata all'esterno di un dispositivo una nota post-it contenente la password che utilizzi equivale a lasciare le chiavi inserite nel cruscotto della tua auto.

## **15** DISATTIVA LA CONDIVISIONE DEI FILE, SE NON NECESSARIA

Se non hai la necessità di condividere file e contenuti multimediali e di renderli perciò visibili su altri dispositivi, disabilita completamente le opzioni di condivisione.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**16**

## **CREA VOLUMI CRITTOGRAFATI PER PROTEGGERE I TUOI DATI**

Utilizza strumenti specifici per crittografare i volumi portatili che utilizzi per condividere le informazioni, in modo da poter trasportare in totale sicurezza i tuoi dati.

**17**

## **SOVRASCRIVI I FILE CANCELLATI PER ELIMINARLI DEFINITIVAMENTE**

Eliminare semplicemente i file presenti su un dispositivo non li rende inaccessibili. L'unico modo che hai per cancellare definitivamente i tuoi dati è quello di sovrascriverli.

**18**

## **NON DIMENTICARE DI CANCELLARE I VECCHI FILE NEI BACKUP IN CLOUD**

Se fai il backup in cloud ricorda che i vecchi dati vanno cancellati anche in quella sede, in quanto essi rimangono ancora memorizzati online nonostante siano stati eliminati dal dispositivo.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**19**

## **CONFIGURA LE IMPOSTAZIONI PRIVACY DELLE APP**

Molte app ti permettono di modificare le impostazioni privacy e di determinare di conseguenza quali informazioni vengono condivise: scegli sempre di rendere pubblica la minor quantità di dati possibile.

**20**

## **ABILITA LA LOCALIZZAZIONE REMOTA E LA PULIZIA DEL DISPOSITIVO**

Se smarrisci il tuo dispositivo o se ti viene rubato, le app di tracciamento ti possono aiutare a localizzarlo. Queste applicazioni ti permettono anche di cancellare le informazioni archiviate in remoto.

**21**

## **IMPOSTA LA PRIVACY QUANDO CONFIGURI UN NUOVO DISPOSITIVO**

Quando configuri un nuovo dispositivo determina prima di tutto le impostazioni privacy. Ciò per evitare di condividere inavvertitamente informazioni riservate durante l'utilizzo di un servizio.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**22**

## **USA APPLICAZIONI SPECIFICHE PER IMPOSTARE I PERMESSI DELLE APP**

In rete puoi trovare utili strumenti che ti permettono di controllare i permessi associati alle app e di ricevere notifiche in caso di accesso esterno alle tue informazioni personali.

**23**

## **BLOCCA I TUOI DISPOSITIVI SMARTPHONE E TABLET**

Blocca l'accesso ai tuoi dispositivi inserendo un codice di sblocco.

In questo modo aggiungerai un ulteriore livello di protezione per i tuoi dati.

**24**

## **FAI IL BACKUP DEI DATI ANCHE DA MOBILE**

Non dimenticare di effettuare il backup dei dati anche da mobile, oltre che da PC.

In questo modo tutte le tue informazioni saranno al sicuro!

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **25** **DISABILITA IL BACKUP AUTOMATICO DEI DATI**

Per maggiore sicurezza, evita che i tuoi dati vengano caricati automaticamente in cloud disattivando le impostazioni di backup automatico sul tuo dispositivo e sulle singole app.

## **26** **DISATTIVA IL BLUETOOTH QUANDO NON LO UTILIZZI**

Ricordati di disattivare la tecnologia bluetooth del tuo dispositivo quando non ne hai bisogno.

Lasciarla accesa potrebbe consentire a chi la utilizza a sua volta di accedere ai tuoi dati.

## **27** **PROTEGGI I DISPOSITIVI MOBILI CON ANTIVIRUS O ANTIMALWARE**

Oltre al PC, dota di software antivirus o antimalware anche i dispositivi mobili che utilizzi.

Molti trascurano ancora l'importanza di questo tipo di protezione.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**28**

## **CONTROLLA LE IMPOSTAZIONI DI NOTIFICA PUSH SU MOBILE**

Le notifiche push sono quegli avvisi che spesso appaiono sulla schermata del tuo dispositivo. Se non vuoi mettere a rischio la tua privacy, scegli quali notifiche far apparire e quali no.

**29**

## **ABILITA TOUCH ID SE UTILIZZI UN DISPOSITIVO APPLE**

Se utilizzi un iPhone puoi usufruire di una misura di protezione aggiuntiva: il Touch ID. Con questa tecnologia l'autenticazione avviene grazie la lettura delle impronte digitali.

**30**

## **IMPOSTA FILTRI PER I CONTENUTI SUL WEB**

Se hai figli che utilizzano dispositivi mobili, imposta dei filtri sul dispositivo. Ti permetteranno di limitare ai ragazzi l'accesso a contenuti inappropriati.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **31** IMPOSTA IL BLOCCO AUTOMATICO DEL DISPOSITIVO

La maggior parte degli smartphone e dei tablet consente di impostare un intervallo di tempo specifico dopo il quale il dispositivo si blocca automaticamente, se inattivo, in modo da proteggere i tuoi dati.

## **32** SII CONSAPEVOLE DELLE APP CHE INSTALLI

Installa solamente app provenienti da fonti attendibili. Alcune infatti potrebbero condividere a tua insaputa informazioni personali, mettendo a rischio la tua privacy.

## **33** UTILIZZA UN SISTEMA DI ALLARME DI PROSSIMITÀ

L'utilizzo di un sistema di allarme di prossimità wireless portatile ti permette di sapere quando il tuo smartphone supera il limite di distanza impostato sul dispositivo.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **34** INSTALLA UN FIREWALL PER PROTEGGERE IL TUO DISPOSITIVO

L'utilizzo del firewall non è riservato unicamente al PC. Installa anche sul tuo dispositivo mobile un firewall per proteggerti dai rischi che puoi correre navigando in rete.

## **35** RIPRISTINA LE IMPOSTAZIONI DI FABBRICA PRIMA DI DISFARTI DI UN DISPOSITIVO

Se hai intenzione di vendere o regalare il tuo smartphone, prima di farlo ricordati di ripristinarne le impostazioni di fabbrica in modo da cancellare in maniera definitiva le tue informazioni personali.

## **36** PROTEGGI I TUOI DATI DA OCCHI INDISCRETI

Presta attenzione all'utilizzo che fai del tuo dispositivo quando ti trovi in un luogo pubblico. Qualcuno potrebbe sbirciare le tue informazioni personali mentre le inserisci sul web o su un'app.



# 99 suggerimenti

per la protezione dei tuoi dati personali

**37**

## **DECIDI COSA DEFINIRE INFORMAZIONE D'IDENTIFICAZIONE PERSONALE (PII)**

Tra i dati che condividi, decidi quali considerare "informazioni d'identificazione personale" e valuta di conseguenza se sia opportuno pubblicarli online o meno.

**38**

## **PROTEGGI I TUOI DATI CON PASSWORD FORTI E COMPLESSE**

Per essere definita complessa, una password dovrebbe essere composta da almeno otto caratteri, contenere lettere minuscole e maiuscole e almeno un numero o un carattere speciale.

**39**

## **NON UTILIZZARE INFORMAZIONI PERSONALI PER LE PASSWORD**

Per costruire le password non utilizzare informazioni personali facilmente identificabili. Rappresenterebbero la prima scelta per eventuali malintenzionati che sanno qualcosa su di te.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**40**

## **SII CAUTO NEL CONDIVIDERE INFORMAZIONI PERSONALI**

Assicurati sempre che coloro ai quali stai fornendo informazioni siano affidabili e ricordati di non condividere mai più del necessario.

In caso di dubbio, non pubblicare mai dati sensibili.

**41**

## **FAI ATTENZIONE ALLE FALSE IDENTITÀ**

Alcune persone potrebbero cercare di ingannarti tramite email di phishing o siti web simili all'originale. Spesso si spacciano per l'azienda ufficiale e ti invitano a condividere informazioni riservate.

**42**

## **CONDIVIDI CON ATTENZIONE LE CREDENZIALI DI ACCESSO**

Valuta attentamente, caso per caso, se sia opportuno condividere le credenziali di accesso a un account con amici e colleghi di lavoro, in modo da tenere al sicuro i tuoi dati più preziosi.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **43** NON UTILIZZARE LA STESSA PASSWORD PER PIÙ DI UN ACCOUNT

Non si dovrebbe mai utilizzare la stessa password per più account.

Può essere in tal senso utile disporre di un gestore di password che automatizzi gli accessi.

## **44** STAI ATTENTO AL FURTO DI NUMERI DI IDENTIFICAZIONE IMPORTANTI

Stai attento non solo al furto del numero della carta di credito o di debito, ma anche di altri numeri di identificazione importanti quali ad esempio quelli della carta d'identità o della patente di guida.

## **45** NON APPUNTARTI LE PASSWORD DI ACCESSO AI TUOI ACCOUNT

Se appunti su carta le password di accesso ai tuoi account i tuoi dati personali saranno a rischio!

Se proprio vuoi scrivere qualcosa, annotati solo un suggerimento che ti permetta di ricordare la password.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **46** ORGANIZZA LE PASSWORD IN RAGGRUPPAMENTI LOGICI

Raggruppa le password per funzione (social, banca, lavoro) e usa un approccio diverso per la creazione delle stesse all'interno di ciascun gruppo, in modo da difenderti meglio da eventuali attacchi hacker.

## **47** NON INVIARE FAX CONTENENTI INFORMAZIONI SENSIBILI

Non inviare dati personali via fax a meno che non sia strettamente necessario.

In caso, prendi le dovute precauzioni affinché le informazioni raggiungano solo l'effettivo destinatario.

## **48** DISTRUGGI VECCHI DOCUMENTI CARTACEI CONTENENTI DATI SENSIBILI

Il "dumpster diving" (rovistare nella spazzatura per ricercare documenti contenenti informazioni private) è uno dei metodi utilizzati per appropriarsi dei dati altrui. Distruggi sempre i vecchi documenti cartacei!

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **49** ELIMINA I VECCHI DATI CHE NON TI SERVONO PIÙ

Conserva solo i dati necessari per le attività correnti. Archivia o distruggi in modo definitivo i dati più vecchi, rimuovendoli da tutti i tuoi computer e dispositivi portatili.

## **50** SMALTISCI CORRETTAMENTE I DISPOSITIVI ELETTRONICI

Le apparecchiature elettroniche non più in uso conservano spesso informazioni personali riservate che possono finire in mani sbagliate. Smaltisci perciò correttamente i tuoi dispositivi.

## **51** QUANDO USI UNA CARTA DI DEBITO, FIRMA INVECE DI INSERIRE IL PIN

Quando fai acquisti, chiedi se puoi utilizzare la tua carta di debito nello stesso modo in cui usi una carta di credito, ossia se puoi firmare la ricevuta invece di inserire il PIN sul dispositivo.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**52**

## **IMPOSTA AVVISI VIA EMAIL O SMS PER LE TRANSAZIONI**

Se possibile, scegli di ricevere avvisi via email o SMS ogni qualvolta la tua carta viene utilizzata per effettuare una transazione: in tal modo avrai sotto controllo tutti i movimenti.

**53**

## **CONTROLLA REGOLARMENTE IL TUO CONTO ONLINE**

Se hai la possibilità di accedere online al tuo conto, controlla regolarmente (magari settimanalmente) la lista movimenti in modo da accertarti che non compaiano transazioni sospette.

**54**

## **TIENI SOTTO CONTROLLO ANCHE LE TRANSAZIONI DI PICCOLA ENTITA'**

Le piccole transazioni sono lo strumento più utilizzato dai truffatori per raggirare senza dare nell'occhio. Controlla regolarmente ogni transazione, comprese quelle di minore entità.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**55**

## **DIFFIDA DELLE OFFERTE DI AIUTO IN SEGUITO A VIOLAZIONE DEI DATI**

Stai attento alle email che offrono servizi di monitoraggio del credito in seguito a violazione dei dati, dal momento che molte di esse sono spesso fraudolente: se necessario, rivolgiti a servizi affidabili.

**56**

## **ACQUISTA SOLO DA SITI WEB AFFIDABILI**

Effettua i tuoi acquisti online solo presso rivenditori di cui riconosci affidabilità e serietà. In questo modo andrai sul sicuro e scongiurerai quasi certamente il rischio di frode.

**57**

## **IN FASE D'ACQUISTO ONLINE, NON FORNIRE INFORMAZIONI SUPERFLUE**

Quando fai un acquisto online non fornire più dati di quanto non sia strettamente necessario. Evita inoltre di lasciare memorizzate informazioni sul tuo conto corrente e sulle tue carte di credito/debito.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## 58 USA UNA CARTA A PLAFOND RIDOTTO PER GLI ACQUISTI ONLINE

Per minimizzare i rischi legati agli acquisti online, dotati di una carta di credito appositamente dedicata allo scopo, dotata di un plafond (tetto massimo di spesa mensile raggiungibile) ridotto.

## 59 NON CONDIVIDERE TROPPE INFORMAZIONI SUI SOCIAL NETWORK

Condividere troppe informazioni personali sul profilo social potrebbe risultare pericoloso.

La password che protegge l'account potrebbe essere identificata partendo dai dati che pubblichi.

## 60 PERSONALIZZA LE IMPOSTAZIONI PRIVACY DEI SOCIAL NETWORK

Molto spesso i social network consentono agli utenti di personalizzare le impostazioni sulla privacy.

Scegli sempre il massimo livello di riservatezza per evitare che i tuoi dati finiscano in cattive mani.



# 99 suggerimenti

per la protezione dei tuoi dati personali

## **61** STAI ATTENTO ALLE RICHIESTE CHE TI VENGONO FATTE SU FACEBOOK

Può capitare che su Facebook tu conceda l'amicizia a persone che non conosci.

In caso ti chiedessero denaro dicendo che sono in difficoltà, stai attento: potrebbe essere una truffa.

## **62** BLOCCA GLI UTENTI SOSPETTI SU FACEBOOK

Se alcuni utenti che non conosci ti mettono a disagio inviandoti messaggi su Facebook contenenti richieste di incontro, puoi bloccarli agendo sulle impostazioni della privacy.

## **63** PROTEGGI I TUOI TWEET

Se utilizzi Twitter per le comunicazioni personali hai la possibilità di impostare i tuoi tweet su "privato": in questo modo solo i tuoi follower potranno visualizzare i contenuti da te pubblicati.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **64** CONTROLLA REGOLARMENTE LE IMPOSTAZIONI PRIVACY DEI SOCIAL

Sulle piattaforme social le opzioni di gestione della privacy cambiano continuamente. Assicurati di controllare regolarmente le impostazioni e di apportare le modifiche che ritieni più opportune.

## **65** FAI ATTENZIONE ALLE RICHIESTE DI AMICIZIA

Il consiglio è quello di non accettare le richieste di amicizia da parte di sconosciuti. Usa il tuo profilo personale solamente per mantenere i contatti con chi conosci veramente.

## **66** SE PUOI, UTILIZZA L'AUTENTICAZIONE IN DUE FASI

L'autenticazione in due fasi richiede una seconda fase di verifica, quale ad esempio la risposta a una domanda segreta o l'inserimento di un PIN. Se è possibile, sfrutta questa opportunità!

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **67** COMUNICA UN'EVENTUALE VIOLAZIONE DEL TUO ACCOUNT

Se il tuo account è stato violato, fallo sapere ai tuoi amici (in modo che facciano attenzione a eventuali richieste che provengono dal tuo profilo) e segnala immediatamente il problema alla piattaforma.

## **68** EVITA DI EFFETTUARE OPERAZIONI SU DATI SENSIBILI SU WI-FI PUBBLICO

Se usi una connessione Wi-Fi pubblica, evita di compiere operazioni sui tuoi dati sensibili. Le informazioni che viaggiano su un canale pubblico potrebbero essere intercettate da estranei.

## **69** SETTA LE IMPOSTAZIONI SULLA PRIVACY NEI SITI WEB CHE LO PERMETTONO

Alcuni siti web (ad esempio Youtube) consentono agli utenti di determinare diversi livelli di privacy. Quando puoi, approfitta di questa opportunità e imposta il livello di privacy più elevato possibile.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**70**

## **NON DIMENTICARE DI EFFETTUARE IL LOGOUT**

Quando accedi a un tuo account personale da un computer pubblico ricordati di effettuare il logout a fine sessione, in modo che nessuno possa avere accesso al tuo profilo.

**71**

## **NON APRIRE EMAIL PROVENIENTI DA MITTENTI SCONOSCIUTI**

Se ricevi un'email proveniente da un indirizzo sconosciuto, non aprirla.

Se ti capita accidentalmente di farlo, evita di cliccare su eventuali collegamenti o di scaricare allegati.

**72**

## **CONFIGURA L'APERTURA DELLE EMAIL IN MODALITA' "SOLO TESTO"**

Imposta sempre il client di posta elettronica con visualizzazione "solo testo" o comunque scegli di non far caricare i contenuti remoti in modo da evitare il tracciamento delle email.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **73** NON CREDERE A TUTTO CIÒ CHE LEGGI ONLINE

Non credere alle false promesse sul web, quali ad esempio quelle di facili guadagni. Potresti rimetterci del denaro o perdere i tuoi dati personali.

## **74** UTILIZZA SITI WEB SICURI PER LE TRANSAZIONI SENSIBILI

Se devi effettuare una transazione bancaria o condividere informazioni sensibili, accertati che il sito web che stai utilizzando sia sicuro (lo puoi considerare tale se prima dell'indirizzo trovi la sigla: <https://>).

## **75** NON CLICCARE SUI COLLEGAMENTI DELLE EMAIL SOSPETTE

Stai attento alle email di phishing! I link in esse contenuti ti potrebbero reindirizzare a pagine richiedenti l'inserimento dei dati personali. Accertati sempre dell'attendibilità del mittente!

## 99 suggerimenti

per la protezione dei tuoi dati personali

**76**

### **STAI ATTENTO ALLA TUA REPUTAZIONE SUL WEB**

Se non stai attento ai contenuti che pubblichi online potresti andare incontro a problemi. Qualsiasi informazione inserita sul web potrebbe raggiungere chiunque, precludendoti delle possibilità.

**77**

### **NON SCARICARE FILE DA SITI INTERNET POCO AFFIDABILI**

In rete il rischio di scaricare malware o programmi indesiderati è piuttosto elevato. Evita perciò il download di file da siti web di cui non ti fidi completamente.

**78**

### **VALUTA SE UTILIZZARE UN INDIRIZZO EMAIL USA E GETTA**

Vuoi testare un programma ma non intendi fornire il tuo indirizzo email in fase di registrazione? Puoi creare online un indirizzo usa e getta e utilizzarlo una sola volta per tale scopo.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**79**

## **APPROFITTA DELLE OPZIONI DI ACCESSO MOBILE SICURO**

Alcuni servizi online ti offrono opzioni di accesso mobile sicuro, consentendoti di accedere ai servizi senza la necessità di esporre le tue credenziali di accesso.

**80**

## **DISATTIVA IL MONITORAGGIO DEGLI ANNUNCI PUBBLICITARI**

Per ridurre il tracciamento dei dati, attiva sullo smartphone l'opzione che impedisce alle applicazioni di utilizzare il tuo ID per mostrarti annunci pubblicitari basati sui tuoi interessi.

**81**

## **NON SALVARE LE PASSWORD NEL BROWSER**

La pratica comune di memorizzare le password nel browser potrebbe mettere a rischio la sicurezza dei tuoi dati in caso qualcuno riuscisse ad accedere al dispositivo che stai utilizzando.

# 99 suggerimenti

per la protezione dei tuoi dati personali

## **82** UTILIZZA EMAIL DIVERSE PER CONTESTI DIVERSI

Per proteggere al meglio le tue informazioni personali dovresti utilizzare email diverse per contesti diversi: ad esempio un indirizzo per gli account privati e un indirizzo diverso per quelli aziendali.

## **83** CREA UN INDIRIZZO EMAIL SPECIFICO PER I PROGETTI A LUNGO TERMINE

Se sei impegnato in un progetto a lungo termine, crea un indirizzo email specifico per tale progetto in modo che tutti coloro i quali sono coinvolti in esso possano accedervi utilizzando credenziali comuni.

## **84** CONSIDERA LE TRACCE CHE HAI LASCIATO NEL TEMPO SUL WEB

Nel corso del tempo potresti avere immesso i tuoi dati nei form di molti siti web.

Elimina gli account che non utilizzi più per cercare di ridurre la dispersione delle tue informazioni personali.



# 99 suggerimenti

per la protezione dei tuoi dati personali

## **85** VALUTA SE UTILIZZARE UNA SANDBOX

Se tratti dati sensibili, per affrontare le minacce malware presenti sul web prendi in considerazione l'utilizzo di soluzioni di ultima generazione, quali ad esempio una sandbox.

## **86** FAI ATTENZIONE AI MALWARE QUANDO RICERCHI CONTENUTI POPOLARI

Se effettui una ricerca su argomenti molto popolari sul web, potresti imbatterti in malware o in siti che, attraverso un semplice clic su un link, eseguono sul tuo dispositivo file dannosi.

## **87** NON INVIARE CREDENZIALI DI ACCESSO SU RETI WI-FI PUBBLICHE

Le reti Wi-Fi pubbliche non vanno assolutamente utilizzate per inviare credenziali di accesso o password: correresti il rischio di trasmetterle a tutti coloro i quali dispongono della connessione.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**88**

## **MEMORIZZA LOCALMENTE I TUOI DATI PIÙ SENSIBILI**

Se non ti senti sicuro di conservare in cloud i dati che ritieni più importanti, esegui un backup degli stessi su un dispositivo di archiviazione removibile da custodire con cura.

**89**

## **NON CAMBIARE TROPPO SPESSO LA PASSWORD**

Dopo che ha violato un account, un hacker agisce con rapidità, senza attendere troppo. Cambiare spesso password, perciò, potrebbe rivelarsi un'operazione inutile.

**90**

## **UTILIZZA UN SERVIZIO CLOUD CRITTOGRAFATO**

Crittografa i dati archiviati in cloud o utilizza un servizio di cloud storage che li crittografi automaticamente, in modo da poterli conservare online in tutta sicurezza.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**91**

## **SCEGLI UN PROVIDER DI POSTA ELETTRONICA SICURO E AFFIDABILE**

Non tutti i provider di posta elettronica sono uguali. Assicurati che quello che utilizzi sia dotato di una tecnologia appositamente realizzata per bloccare le email di phishing.

**92**

## **MODIFICA LA PASSWORD DOPO UNA VIOLAZIONE DI DATI**

Se hai un account presso una società che ha subito una violazione di dati, modifica la tua password appena puoi per tentare di proteggere le tue informazioni personali.

**93**

## **VERIFICA CHE UNA VIOLAZIONE SIA REALMENTE AVVENUTA**

Se ricevi via email una notifica di violazione che richiede un aggiornamento dei tuoi dati, accertati che tale violazione sia veramente avvenuta contattando direttamente l'azienda.

# 99 suggerimenti

per la protezione dei tuoi dati personali

**94**

## **BLOCCA LA CARTA IN CASO DI VIOLAZIONE DEI DATI**

Se una violazione di dati ha colpito una società che ti ha rilasciato un qualsiasi tipo di carta, bloccala e richiedine immediatamente una nuova in sostituzione della precedente.

**95**

## **APPROFITTA DEL MONITORAGGIO GRATUITO DEL CREDITO**

Se un'importante società subisce una violazione di dati e le informazioni del tuo account sono state compromesse, approfitta, se possibile, dei servizi gratuiti di monitoraggio del credito.

**96**

## **CONSIDERA LE SEGNALAZIONI DI STRANE EMAIL PROVENIENTI DAI TUOI ACCOUNT**

Se il tuo account è stato hackerato, è possibile che i tuoi contatti ricevano delle email che contengono virus o malware inviate a tuo nome.

Stai attento a ogni segnalazione!

# 99 suggerimenti

per la protezione dei tuoi dati personali

**97**

## **IMPARA A RICONOSCERE I SEGNALI DI UNA VIOLAZIONE**

Informati sui segnali di allarme di una violazione e crea abitudini positive per monitorare la sicurezza dei tuoi dati personali in modo da identificare i potenziali attacchi ai tuoi account.

**98**

## **RIOTTIENI IL CONTROLLO DI UN ACCOUNT COMPROMESSO**

Riottenere il controllo di un account compromesso può risultare complicato.

Devi contattare il fornitore del servizio e dimostrare di essere il vero titolare dell'account.

**99**

## **SCOPRI LE RAGIONI CHE HANNO PORTATO ALLA VIOLAZIONE**

Guarda il bicchiere mezzo pieno: prova a considerare una violazione come un'opportunità.

Scopri cos'è andato storto e come potresti proteggere meglio i tuoi dati in futuro.



*Vuoi gestire l'infrastruttura IT  
del tuo istituto in sicurezza?*

Scopri il nostro nuovo servizio!

## **Amministratore di sistema**



<https://gdprscuola.it/amministratoredisistema>

