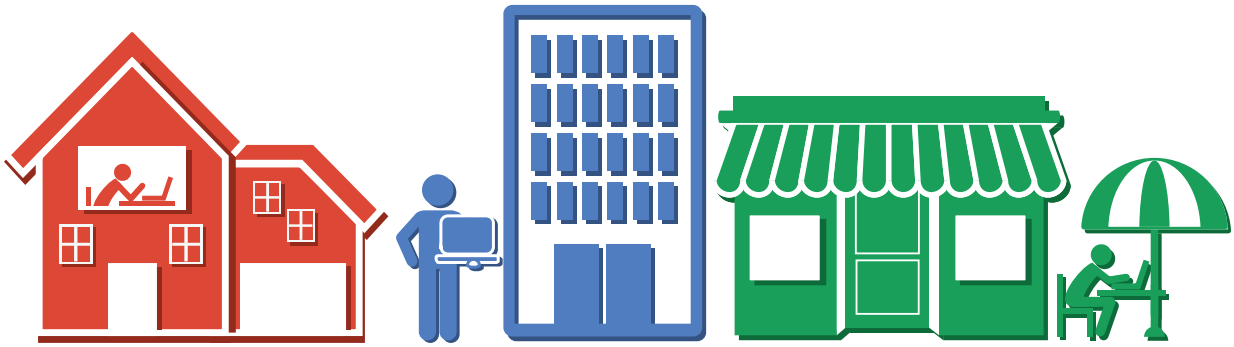
Centro per la sicurezza di Google

Una guida per la sicurezza online



Google™

Di cosa parla questo opuscolo?

Il Centro per la sicurezza di Google ha lo scopo di aiutare te, la tua famiglia e i tuoi amici a navigare in sicurezza su Internet.

Questo opuscolo è stato ideato per darti consigli e suggerimenti utili e facili da ricordare da mettere in pratica. Abbiamo incluso adesivi con alcuni consigli fondamentali che puoi attaccare sul computer o sul notebook e ti serviranno come utili promemoria.

Per informazioni dettagliate su tutti gli argomenti trattati in questo opuscolo e per avere altre informazioni, visita il sito web del Centro per la sicurezza all'indirizzo www.google.com/safetycenter.

Sommario

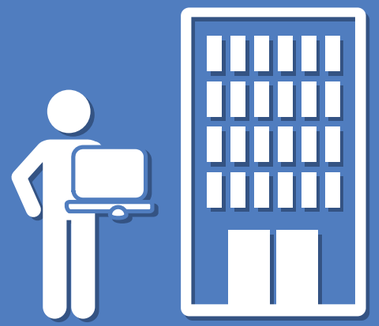
La tua sicurezza online **pag. 4**

Scegli misure di sicurezza adatte alla tua famiglia **pag. 9**

L'impegno di Google per la tua sicurezza **pag. 14**

La tua sicurezza online

Scegli la sicurezza fin da subito. Internet offre tante opportunità di esplorazione, creazione e collaborazione. Per utilizzare al meglio il Web, è importante proteggersi e preservare la propria sicurezza. Che tu sia un nuovo utente o un veterano di Internet, i consigli e i suggerimenti riportati qui possono aiutarti a esplorare il Web in totale sicurezza.



- Utilizza un insieme di lettere, numeri e simboli
- Utilizza una password diversa per ogni sito web

Proteggi le tue password

Le password sono la prima linea di difesa contro i criminali informatici. È fondamentale scegliere password sicure che siano diverse per ogni tuo account importante ed è buona prassi aggiornare regolarmente le password. Segui questi suggerimenti per creare password sicure e proteggerle.

1. Utilizza una password univoca per ogni tuo account importante, come l'account email e l'account dei servizi bancari online.
2. Utilizza una password lunga formata da numeri, lettere e simboli.
3. Molti servizi ti inviano un'email a un indirizzo email di recupero pertanto, se devi reimpostare la password, assicurati che tale indirizzo sia aggiornato e relativo a un account a cui tu possa ancora accedere.

Un'idea potrebbe essere quella di trovare una frase che conosci solo tu e che si riferisca a un determinato sito web in modo che sia più facile da ricordare. Per il tuo account email potresti provare con: "I miei amici Tom e Jasmine mi mandano un'email divertente una volta al giorno" e poi utilizzare numeri e lettere per ricrearla. "ImaT&Jmmued1vag" è una password con molte varianti. Quindi ripeti la procedura per altri siti.

- Non rispondere a messaggi sospetti fornendo informazioni personali

Previeni il furto d'identità

È bene conoscere i trucchi comuni adottati dai criminali informatici per proteggerti dalle frodi e dal furto d'identità online. Ecco alcuni semplici suggerimenti:

1. Non rispondere se trovi un'email, un messaggio immediato o una pagina web sospetti che ti chiedono informazioni personali o dati finanziari.
2. Non inserire mai la tua password se arrivi in un sito seguendo un link presente in un'email o in una chat di cui non ti fidi.
3. Non inviare la tua password tramite email e non comunicarla ad altri.

Se ricevi un messaggio da qualcuno che conosci ma che ti sembra strano, l'account della persona in questione potrebbe essere stato compromesso da un criminale informatico che sta tentando di ottenere da te denaro o informazioni. Stai attento a come rispondi o non rispondere affatto. Ecco alcune tattiche frequenti: chiederti di inviare urgentemente denaro con la scusa di essere bloccati in un altro Paese o che il cellulare è stato rubato e la persona non può essere chiamata. Nel messaggio potrebbe anche esserti chiesto di fare clic su un link per visualizzare una foto, un articolo o un video, che in realtà ti indirizza a un sito che potrebbe carpire i tuoi dati. Rifletti prima di fare clic.

- Non rispondere a email o post sospetti
- Fai ricerche su offerte online per evitare truffe
- Se sembra troppo bello per essere vero, probabilmente è così

Evita le truffe

Il Web può essere davvero straordinario, ma non tutte le persone presenti online hanno buone intenzioni. Ecco tre semplici modi per evitare i truffatori e proteggersi sul Web:

1. Diffida degli estranei che promettono regali. Se qualcuno ti dice che hai vinto qualcosa e ti chiede di compilare un modulo con le tue informazioni personali, non iniziare neanche a compilarlo. Anche se non fai clic sul pulsante "Invia", i dati che inizi a inserire nei moduli potrebbero comunque essere inviati ai truffatori.

2. Fai le tue ricerche. Quando fai acquisti online, fai ricerche sul venditore e diffida da prezzi insolitamente bassi così come diffideresti se comprassi qualcosa in un negozio locale. Esamina con attenzione le offerte online che sembrano troppo belle per essere vere. A nessuno piace essere indotto con l'inganno ad acquistare articoli contraffatti.

3. In caso di dubbi, vai sul sicuro. Hai una brutta sensazione su un annuncio o un'offerta? Fidati del tuo istinto! Fai clic su annunci o acquista prodotti soltanto di siti che sono sicuri, recensiti e ritenuti attendibili.

- Esci dall'account su computer pubblici o condivisi
- Imposta il blocco automatico su dispositivi e schermi

Blocca lo schermo o il dispositivo

Dovresti sempre bloccare lo schermo quando finisci di utilizzare il computer, il portatile o il cellulare. Questo è particolarmente importante per cellulari e tablet, che è più facile vengano smarriti e trovati da persone che non devono accedere alle tue informazioni, e i computer di casa in spazi comuni. Per maggiore sicurezza dovresti anche impostare il blocco automatico del dispositivo quando entra in modalità di sospensione.

- Proteggi il router di casa con una password WPA2

Utilizza reti sicure

È opportuno prestare molta attenzione quando accedi a Internet utilizzando una rete che non conosci o della quale non ti fidi, come una rete Wi-Fi gratuita in un bar. Il fornitore del servizio potrebbe monitorare tutto il traffico sulla sua rete, incluse le tue informazioni personali.

Quando ti connetti tramite una rete Wi-Fi pubblica, chiunque nelle vicinanze sarà in grado di monitorare le informazioni trasmesse tra il computer e l'hotspot Wi-Fi se la connessione non è crittografata. Evita di svolgere operazioni importanti come attività bancarie o acquisti tramite reti pubbliche.

Se utilizzi una rete Wi-Fi a casa, assicurati di proteggerla per evitare che altre persone la possano utilizzare. A tale scopo, imposta una password per proteggere la rete Wi-Fi che, come le altre password scelte da te, dovrebbe essere formata da una lunga sequenza univoca di numeri, lettere e simboli per evitare che possa essere intuita facilmente da altri. Per maggiore protezione, scegli l'impostazione WPA2 durante la configurazione della rete.

Infine, per maggiore sicurezza, assicurati di utilizzare una password per proteggere il router. Segui le istruzioni fornite dal tuo provider di servizi Internet o dal produttore del router per impostare una password personalizzata per il router anziché utilizzare quella predefinita, che potrebbe essere nota ai criminali informatici. Se i criminali riescono ad accedere al router, possono modificare le tue impostazioni e spiare la tua attività online.

- Configura la verifica in due passaggi per gli account Google
- Controlla le impostazioni prima della condivisione

Strumenti Google per la privacy e la sicurezza

Google ti mette a disposizione una gamma di strumenti che possono contribuire alla tua protezione e a tenere private e al sicuro le tue informazioni. Di seguito sono riportate informazioni su alcuni dei nostri strumenti più conosciuti che migliorano Google per te.

Verifica in due passaggi

Per proteggere ancora meglio gli account Google, offriamo ai nostri utenti la verifica in due passaggi. Questo strumento offre un ulteriore livello di sicurezza tramite la richiesta non soltanto della password ma anche di un codice di verifica per poter accedere a un account Google. La verifica in due passaggi consente a Google di accertarsi che si tratti di te chiedendoti di inserire un codice che viene inviato soltanto al tuo telefono: è molto improbabile che un malintenzionato abbia accesso sia al tuo telefono sia alla tua password.

Impostazioni dell'account Google

Nella pagina delle impostazioni del tuo account puoi esaminare le informazioni e i servizi associati al tuo account Google e modificare le tue impostazioni relative a sicurezza e privacy.

Impostazioni sulla privacy di YouTube

Potrebbe capitare che tu voglia condividere i tuoi video di YouTube soltanto con un piccolo gruppo di amici o magari tenerli solo per te. In questo caso, quando carichi un video puoi impostarlo come "non in elenco" (nascosto nei risultati di ricerca, ma visualizzabile dalle persone in possesso del link) oppure "privato" (visualizzabile soltanto da te).

Strumenti Google per la privacy e la sicurezza

Gestisci i dati memorizzati nel tuo account Google

Nella Google Dashboard vengono visualizzate le informazioni memorizzate nel tuo account Google e vengono fornite informazioni generali su alcune tue attività recenti nell'account. Da un'unica posizione centrale puoi visualizzare facilmente i tuoi dati e la tua attività, nonché accedere alle impostazioni relative a servizi come Blogger, Google Calendar, Documenti Google, Google+ e altri ancora.

Gestisci le tue preferenze relative agli annunci

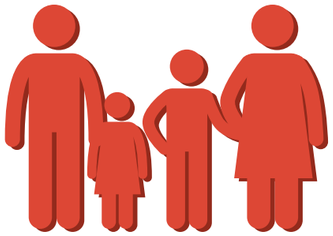
La pubblicità permette di finanziare tanti dei servizi online gratuiti che utilizzi tutti i giorni. Con Impostazioni annunci di Google puoi capire come vengono scelti gli annunci per te, controllare i tuoi dati che vengono utilizzati per la selezione degli annunci e bloccare determinati inserzionisti.

Gestisci chi può visualizzare i tuoi contenuti condivisi

Le cerchie di Google+ ti aiutano a gestire i tuoi amici e i tuoi contatti. Puoi inserire gli amici in una cerchia, la famiglia in un'altra e il capo in una cerchia tutta sua, proprio come nella vita reale. Dopodiché puoi condividere contenuti pertinenti, come post di Google+, video di YouTube o annunci di schede locali di Google, con le persone giuste in qualsiasi momento tu voglia.

Scegli misure di sicurezza adatte alla tua famiglia

Crea le basi di un comportamento online corretto. Come genitore o tutore, sai che cosa è giusto per la tua famiglia e quali sono i metodi migliori per educare i tuoi figli. Per aiutare i tuoi familiari a esplorare i nuovi servizi e gadget e le nuove tecnologie in un mondo online in costante evoluzione, qualche consiglio pratico può esserti d'aiuto. Ecco perché ci confrontiamo costantemente con genitori, educatori, community ed esperti di sicurezza in tutto il mondo: per individuare e promuovere le soluzioni più efficaci. Insieme, possiamo far crescere una community di cittadini digitali responsabili.



Regole di base per la sicurezza della famiglia

Di seguito sono riportati alcuni rapidi suggerimenti per genitori impegnati su come contribuire alla sicurezza online della famiglia.

1 Parla con la tua famiglia della sicurezza online.

Definisci in modo chiaro le regole e le aspettative della tua famiglia per quanto riguarda la tecnologia, nonché le conseguenze in caso di utilizzo inappropriato. E, cosa più importante, assicurati che i tuoi familiari si sentano abbastanza a proprio agio da chiedere consiglio quando devono prendere decisioni difficili. Questo può aiutarli a sentirsi sicuri mentre esplorano Internet in modo autonomo e a sapere di potersi rivolgere a te per qualsiasi domanda.

2 Utilizzate insieme la tecnologia.

È un buon modo di educare alla sicurezza online e crea opportunità per affrontare gli argomenti legati alla sicurezza con la tua famiglia quando si presentano.

3 Discuti dei siti e dei servizi online.

Parla con i tuoi familiari dei tipi di siti che preferiscono visitare e di ciò che è appropriato per ciascun membro della famiglia.

4 Proteggi le password.

Aiuta la tua famiglia a capire come impostare password sicure online. Ricorda ai tuoi familiari di non divulgare le password, tranne magari a un adulto fidato, ad esempio un genitore. Assicurati che si ricordino sempre di uscire dai propri account online quando utilizzano computer pubblici a scuola, in un Internet café o in biblioteca.

5 Utilizza le impostazioni di privacy e i controlli di condivisione.

Esistono molti siti per condividere opinioni, foto, video, aggiornamenti di stato e non solo. Molti di questi servizi offrono controlli e impostazioni di privacy che ti aiutano a decidere chi può vedere i tuoi contenuti prima di pubblicarli. Parla con i tuoi familiari di ciò che è opportuno o meno condividere pubblicamente. Aiutali a rispettare la privacy degli altri non divulgando i dati personali di familiari e amici e non identificando le persone per nome nei contenuti condivisi pubblicamente.

6 Controlla i limiti di età.

Molti servizi online, tra cui Google, prevedono limiti di età che definiscono chi può usufruire dei relativi servizi. Ad esempio, devi rispettare requisiti d'età per poter avere un account Google, mentre l'utilizzo di alcuni prodotti Google è limitato agli utenti dai 18 anni in su. Controlla sempre i termini e condizioni d'uso di un sito web prima di consentire ai tuoi figli di creare un account e chiarisci con loro le eventuali regole della tua famiglia per quanto riguarda i siti e i servizi che possono utilizzare.

7 Educa la tua famiglia a comunicare in modo responsabile.

Ecco una buona regola pratica: se una cosa ti sembra inappropriata da dire di persona, non inviarla tramite SMS, email, messaggio immediato e non pubblicarla come commento nella pagina di un utente. Discuti di come ciò che dici online potrebbe fare sentire gli altri e individua linee guida per la tua famiglia su quale tipo di comunicazione è appropriato.

8 Confrontati con altri adulti ed esperti.

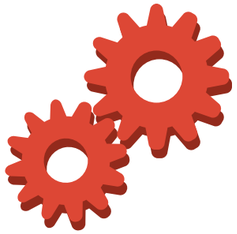
Estendi la conversazione ad amici, insegnanti, consulenti, educatori e alla tua famiglia allargata. Gli altri genitori e professionisti che lavorano a contatto con i ragazzi possono essere un'utile risorsa per aiutarti a decidere ciò che è giusto per la tua famiglia, soprattutto se hai a che fare con un'area tecnologica con cui hai poca dimestichezza.

9 Proteggi il tuo computer e la tua identità.

Utilizza software antivirus e aggiornalo regolarmente, a meno che utilizzi un Chromebook, che non ha bisogno di software antivirus. Discuti con la tua famiglia dei tipi di informazioni personali (come il codice fiscale, il numero di telefono o l'indirizzo di casa) che non è opportuno pubblicare online. Insegna ai tuoi familiari a non accettare file o aprire allegati email provenienti da sconosciuti.

10 Mantieni un dialogo costante.

La sicurezza non è un impegno occasionale: la tecnologia si evolve, così come le esigenze della tua famiglia. Assicurati di mantenere un dialogo costante. Ristabilisci le regole di base della tua famiglia, controlla i progressi di tutti e dedicate regolarmente del tempo alla discussione. I suggerimenti che seguono dei nostri partner affrontano questioni comuni che preoccupano maggiormente i genitori.



Scopri strumenti per la sicurezza facili da usare

Scopri le funzionalità di sicurezza di Google che ti aiutano a controllare i contenuti online visualizzati dalla tua famiglia.

Imposta la ricerca in modo che restituisca risultati adatti alla famiglia.

Se attivi Google SafeSearch puoi escludere la maggior parte dei contenuti per adulti che tu o la tua famiglia preferireste evitare. Se un risultato inappropriato viene comunque incluso, puoi segnalarlo a Google. Ci impegniamo costantemente per migliorare i nostri filtri dei contenuti e questo tipo di feedback ci consente di rendere SafeSearch migliore per tutti.

Imposta un filtro per escludere i contenuti inappropriati.

Se preferisci non visualizzare contenuti per adulti o soggetti a limiti di età mentre esplori YouTube, scorri fino in fondo una pagina qualsiasi di YouTube e attiva la Modalità di protezione. La Modalità di protezione ti consente di escludere i contenuti potenzialmente discutibili dalla ricerca, dalle playlist, dai programmi, dai film e dai video correlati.

Supervisiona gli utenti che utilizzano Chromebook condivisi.

Non puoi essere sempre presente per supervisionare l'attività web della tua famiglia. Per le volte in cui non sei nella stessa stanza con loro, c'è la funzione Utente supervisionato per Google Chrome. Quando questa funzione è attiva, puoi esaminare la cronologia delle pagine visitate dall'utente, consentire o bloccare determinati siti e gestire i siti web che un membro della tua famiglia può vedere.

Consenti l'accesso solo ad app e giochi approvati.

Vuoi condividere il tuo tablet senza condividere tutti i tuoi contenuti? Sui tablet con sistema operativo Android 4.3 e versioni successive, puoi creare profili con limitazioni che consentono di limitare l'accesso di altri utenti alle funzioni e ai contenuti del tuo tablet.

Utilizza le classificazioni per scegliere app appropriate in base all'età.

Proprio come al cinema, puoi decidere quali app di Google Play sono appropriate per la tua famiglia consultando le classificazioni: Per tutti, Maturità bassa, Maturità media o Maturità alta. Puoi filtrare le app per livello, nonché bloccare il livello di filtro con un semplice codice PIN (impedendo ad altri utenti di disattivare involontariamente il filtro).

Scopri gli strumenti per la sicurezza di Google ideati per aiutare la tua famiglia a monitorare la reputazione online.

Blocca tag o commenti indesiderati.

Se preferisci non visualizzare i post di un utente su Google+, puoi bloccarli accedendo al suo profilo e selezionando Segnala/blocca [nome della persona]. Puoi anche disattivare post specifici per non visualizzarli più nel tuo stream.

Modera i commenti ai tuoi video.

Moderare i commenti sul tuo canale di YouTube è facile. Puoi scegliere di eliminarli o di non pubblicare i commenti di determinati utenti o con determinate parole chiave prima di averli esaminati.

Blocca gli utenti offensivi di YouTube.

Se un utente fa commenti che non gradisci sui tuoi video o sul tuo canale, puoi bloccarlo su YouTube. L'utente non potrà più commentare i tuoi contenuti o inviarti messaggi privati.

Proteggi il tuo dispositivo da sguardi indiscreti.

Il blocco dello schermo non è importante soltanto per proteggere il tuo account, ma anche per assicurarti che altre persone non rovistino sul tuo telefono se lo lasci incustodito. Puoi scegliere un PIN, una password o una sequenza per impostare un blocco dello schermo sul telefono o sul tablet.

Segnala contenuti offensivi.

Se un utente pubblica un commento o un post inappropriato su Google+, YouTube o Blogger puoi segnalarlo. Le norme relative ai contenuti di Google spiegano chiaramente le azioni considerate appropriate e non appropriate su questi siti. Pertanto, se riscontri contenuti o comportamenti che violano le nostre norme, puoi segnalarli perché vengano esaminati. Esaminiamo i contenuti segnalati in modo continuo e potremmo rimuovere contenuti e chiudere o applicare limiti agli account degli utenti che violano le nostre norme.

L'impegno di Google per la tua sicurezza

Internet è una cosa fantastica. Ma così come nella realtà, non tutte le persone online hanno buone intenzioni. Per Google la tua privacy e la tua sicurezza sono molto importanti. Investiamo milioni di dollari ogni anno e ci rivolgiamo a esperti in sicurezza dei dati di fama internazionale per tenere al sicuro i tuoi dati. Lo scopo di questi esperti è tenere te e i tuoi dati al sicuro ed essere sempre un passo più avanti dei criminali informatici.

Google si adopera per proteggerti da furti d'identità, frode personale e truffe online, per proteggere il tuo computer e per rendere Internet un luogo più sicuro. Ti diamo le conoscenze e gli strumenti necessari per tenere al sicuro te stesso e la tua famiglia online. Inoltre facciamo costanti investimenti e miglioramenti per contrastare tutto questo per tuo conto.

Contro il furto d'identità

Google utilizza una serie di tecnologie per proteggerti meglio dal furto d'identità online e assicurarsi che il tuo account Google sia sempre protetto.

Verifica in due passaggi

Per proteggere ancora meglio gli account Google, offriamo ai nostri utenti la verifica in due passaggi. Questo strumento offre un ulteriore livello di sicurezza tramite la richiesta non soltanto della password ma anche di un codice di verifica per poter accedere a un account Google. La verifica in due passaggi consente a Google di accertarsi che si tratti di te chiedendoti di inserire un codice che viene inviato soltanto al tuo telefono: è molto improbabile che un malintenzionato abbia accesso sia al tuo telefono sia alla tua password.

Crittografia

Google adotta molte misure per proteggere le tue informazioni personali da malintenzionati e curiosi. Per impostazione predefinita, crittografiamo la connessione Gmail tra il tuo computer e Google per cercare di proteggere la tua attività su Google da occhi indiscreti. Utilizziamo sempre questa protezione, chiamata crittografia SSL a livello di sessione, anche quando accedi a Google Drive e a tanti altri servizi.

Misure per mantenere protetti il tuo computer e il tuo dispositivo

Tu stesso puoi contribuire a proteggere il tuo computer dal malware, ma anche Google si adopera per proteggerti, con centinaia di esperti di sicurezza che lavorano incessantemente per garantire la protezione dei tuoi dati e dispositivi.

Il nostro aiuto per evitare il malware

Google, oltre a cercare sul Web i siti con le risposte migliori alle tue domande, cerca anche i siti che sembrano essere dannosi per gli utenti o che contengono malware. Ogni giorno identifichiamo e contrassegniamo oltre 10.000 siti non sicuri e visualizziamo avvisi per 14 milioni di risultati di ricerca di Google e 300.000 download per comunicare ai nostri utenti che potrebbe esserci qualcosa di sospetto dietro un determinato sito web o link.

Il nostro contributo alla sicurezza del tuo dispositivo mobile

Gli smartphone con software Android di Google hanno protezioni simili per ridurre il rischio di danni. Android richiede inoltre che per ogni app del Google Play Store siano indicate le informazioni che l'app deve raccogliere o a cui deve accedere dal dispositivo, quindi puoi decidere se ritenere attendibile o meno l'app. Eseguiamo anche la scansione automatica di Google Play per bloccare e rimuovere app dannose. Per alcuni cellulari Android, il nostro servizio di verifica delle applicazioni Google cerca applicazioni potenzialmente dannose a prescindere dalla fonte di installazione.

Internet più sicuro per tutti

La protezione degli utenti è responsabilità di tutti. Stiamo tutti meglio se ognuno di noi utilizza le migliori tecnologie e tecniche di sicurezza.

Condivisione di strumenti ed esperienza

La tua sicurezza è importante per noi, a prescindere dai servizi e prodotti che utilizzi, pertanto comunichiamo le informazioni relative ai siti e ai link non sicuri che troviamo ad altre società per consentire loro di proteggere anche i loro utenti. Tramite la collaborazione e l'aiuto reciproco, l'intero Web è molto più sicuro.

Comunicazione con utenti e proprietari di siti web

Mentre ci adoperiamo per proteggere i nostri utenti e le relative informazioni, a volte rileviamo ed effettuiamo accertamenti in merito ad andamenti insoliti dell'attività. Ogni giorno identifichiamo e contrassegniamo oltre 10.000 siti non sicuri. Ogni giorno inviamo anche messaggi a migliaia di proprietari di siti web, se riteniamo che i loro siti potrebbero essere stati oggetto di attacco, per consentire loro di ripulire i siti.

Collaborazione con organizzazioni che si occupano di sicurezza

Google fa parte di una serie di organizzazioni che si adoperano per aiutare le società a migliorare la sicurezza per i loro utenti. Ad esempio, abbiamo contribuito a fondare StopBadware.org e collaboriamo con questa organizzazione per rendere più sicuro il Web tramite l'interruzione, la riduzione e la pulizia di siti web contenenti malware o altro software dannoso.

ADESIVI

15 suggerimenti da portare con te per la tua sicurezza online. Per ulteriori suggerimenti per la sicurezza, visita il sito www.google.com/safetycenter.

Per conoscere i partner e trovare altre risorse, visita il sito www.google.com/safetycenter.

Google™

Per ulteriori informazioni sulla sicurezza online, visita il sito **www.google.com/safetycenter.**