



## **Lista di controllo: «Proteggere i propri dati e la propria reputazione in rete»**

**Come proteggere i propri dati e la propria reputazione in rete? Specialista della reputazione online e della protezione dei dati, Stéphane Koch\* ci dà qualche semplice consiglio.**

### **✓ Contenuti in rete associati al proprio nome**

Per proteggere efficacemente la propria reputazione in rete, è essenziale conoscere i contenuti che vi si trovano in associazione al proprio nome digitandolo regolarmente in un motore di ricerca. In alcuni casi si può inoltrare una richiesta per il ritiro del contenuto al webmaster del sito o del motore di ricerca su cui il sito figura.

### **✓ Facebook e reti sociali**

Evitate di pubblicare contenuti sensibili e prendete le stesse precauzioni che adottate nella vita reale. Imparate come [disattivare ed eliminare il vostro account](#). Attivate [l'autenticazione a due fattori](#). Non condividete [pubblicamente la vostra lista di amici](#) né [i vostri interessi \(«Mi piace»\)](#). Accettate come amici solo persone che conoscete davvero.

### **✓ Comportamenti strani degli amici**

I truffatori possono piratare gli account dei vostri amici e inviare link dai loro conti. Se un contenuto è diverso da quello che un vostro amico pubblica o invia solitamente, non cliccatelo e avvertite il vostro amico chiamandolo sul suo numero fisso o di cellulare.

### **✓ Copie di sicurezza**

Effettuate regolarmente copie di sicurezza dei vostri dati importanti. Provvedete a proteggere i vostri supporti di sicurezza con una [password sicura](#) e a conservarli in un luogo diverso dall'originale.

✓ **Cancellazione dei dati**

Quando buttate, fate riparare o rivendete un dispositivo (smartphone, tablet, computer, chiave USB, carta SD), pensate a cancellare tutti i dati che vi sono registrati. Sappiate comunque che alcuni possono rimanere anche dopo la cancellazione.

✓ **Password**

Rendete sicuri i vostri dispositivi e conti online con [password sicure](#). Per aumentare la sicurezza, si può ricorrere a un [gestore di password](#) che occorre abbinare a un secondo fattore di autenticazione (p. es. utilizzando [Google Authenticator](#) o una chiave Yubikey).

✓ **Connessione da un dispositivo pubblico o di terzi**

Accedete utilizzando un [codice monouso](#). Una volta terminate le vostre attività, sconnettetevi manualmente da tutti i conti online.

✓ **Gestione a distanza in caso di furto di un dispositivo**

In caso di perdita o furto di un dispositivo, Android Device Manager e iCloud vi permettono di localizzarlo, bloccarlo e cancellarne il contenuto a distanza.

✓ **Antivirus e firewall**

Installate un antivirus su tutti i vostri dispositivi (smartphone, tablet e computer). Molte versioni gratuite offrono una protezione soddisfacente. Se navigate su reti Wi-Fi pubbliche, prevedete anche un firewall e pensate a rendere sicura la ricezione delle vostre e-mail.

✓ **Applicazioni**

Scaricate programmi e applicazioni solo da siti che ritenete affidabili; in caso di dubbi, non lo fate. Inoltre, pensate a mantenere sempre aggiornati il vostro browser e le altre applicazioni.

✓ **Componenti aggiuntivi per rendere sicura la navigazione**

Grazie a componenti aggiuntivi per il vostro browser, potete [attivare la navigazione sicura](#) (sito disponibile solo in inglese) non appena possibile, [evitare che le imprese possano raccogliere informazioni sui vostri comportamenti in rete](#) (sito disponibile solo in inglese), [verificare l'affidabilità dei siti che consultate](#) o [bloccare le pubblicità in rete](#).

✓ **Gratuità e pubblicità**

Oggi su Internet niente è gratis: le imprese sono commerciali. Riducete al minimo indispensabile le vostre tracce in materia pubblicitaria fornendo solamente le [informazioni strettamente necessarie](#).

✓ **Geolocalizzazione e pubblicità**

Pensate a [disattivare le funzioni di geolocalizzazione](#) e di tracciamento pubblicitario sui vostri dispositivi quando non vi servono.

✓ **Porre le domande giuste per ottenere le risposte giuste**

Non bisogna essere un esperto per proteggere la propria vita privata in rete. Utilizzate i motori di ricerca per imparare, ad esempio, a [modificare le impostazioni sulla privacy](#) delle principali reti sociali, [cancellare i dati di navigazione](#) su Internet o disattivare la funzione di geolocalizzazione del vostro [smartphone](#).

Consultate inoltre la nostra [rubrica dedicata alla protezione dei dati](#), che vi propone una panoramica dei [maggiori rischi recenti in materia di protezione dei dati](#), consigli su come proteggersi e rimanere nella legalità nonché documenti e [informazioni utili per i bambini e i giovani](#), [per i genitori](#) e [per gli insegnanti](#).

\* Titolare di un Master of Advanced Studies in lotta contro la criminalità economica e di un titolo quale specialista in relazioni pubbliche, **Stéphane Koch** è formatore, consulente e incaricato di corsi nell'ambito delle tecnologie dell'informazione e della comunicazione.

**Giovani e media** è il programma nazionale di promozione delle competenze medialì. Il suo scopo è insegnare ai bambini e ai giovani a utilizzare i media digitali in modo sicuro e responsabile, offrendo a genitori, insegnanti e specialisti informazioni, sostegno e consigli su come seguirli. Ulteriori informazioni sono disponibili sul sito [www.giovanimedia.ch](http://www.giovanimedia.ch).