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 gestione della reputazione online e della protezione dei dati, Stéphane Koch* ci dà qualche semplice consiglio.

✓ **Ricerca regolare del proprio nome in Internet**

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 indesiderato al webmaster del sito o del motore di ricerca su cui il sito figura o chiedere la deindicizzazione del contenuto dai principali motori di ricerca.

✓ **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'autentificazione a due fattori. Non condividete pubblicamente la vostra lista di amici né i vostri interessi («Mi piace»). Verificate le pubblicazioni in cui siete identificati. Accettate come amici solo persone che conoscete davvero. Il numero di «amici in comune» non è un criterio affidabile.

✓ **Comportamenti strani degli amici**

I truffatori possono piratare gli account dei vostri amici e inviare link dai loro profili. Se un contenuto è diverso da quello che un vostro amico pubblica o invia solitamente, non cliccatelo e telefonate al vostro amico per avvertirlo. Procedete allo stesso modo per i messaggi privati, compresi quelli ricevuti su WhatsApp. In generale, prestate attenzione a non cliccare direttamente sui link ricevuti per messaggio e che vi rindirizzano su un contenuto o una piattaforma (o altre azioni che vi domandano di identificarvi su uno dei vostri profili, per esempio "Connettetevi a Facebook per vedere questo video").

✓ **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), assicuratevi di cancellare tutti i dati che vi sono registrati. Sappiate comunque che alcuni possono rimanere anche dopo la cancellazione. Cancellarli o spostarli nel cestino non basta: bisogna procedere a una cancellazione sicura dei dati.

✓ **Password**

Rendete sicuri i vostri dispositivi e conti online con password sicure. Ogni conto deve disporre di una password specifica e unica. È utile ricorrere a un gestore di password (ma solo se è attivata l'autenticazione a due fattori). Strumenti quali Keepass, Dashlane, LastPass e 1Password funzionano anche con gli smartphone Android o Apple.

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

Accedete utilizzando un codice monouso. Una volta terminate le vostre attività, sconnettetevi manualmente da tutti i vostri 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. È importante conservare il codice IMEI del dispositivo per comunicarlo al vostro servizio di telecomunicazione e alla vostra assicurazione in caso di furto. Questo codice si trova di solito sulla fattura, sulla scatola del dispositivo oppure nelle sue impostazioni.

✓ **Antivirus e firewall**

Installate un antivirus su tutti i vostri dispositivi (smartphone, tablet e computer). Le versioni gratuite di Sophos o Avast, ad esempio, offrono una protezione di base. Ciononostante, le versioni a pagamento di G Data, Kaspersky o Bit Defender hanno generalmente un tasso di individuazione di virus più elevato e includono un set completo di strumenti di sicurezza (firewall e protezione contro i ransomware, l'accesso alla webcam o le intrusioni). Se navigate su reti Wi-Fi pubbliche, prevedete anche un VPN 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**

Nelle impostazioni del vostro browser, potete attivare la navigazione sicura (sito disponibile solo in inglese) per evitare che le imprese possano raccogliere informazioni sui vostri comportamenti in rete e generare prezzi in modo dinamico durante i vostri acquisti, in funzione del livello di reddito percepito tramite i dati comunicati dal vostro computer. Attivate la funzione "Do not track" nelle impostazioni del vostro browser. Rimane essenziale anche verificare l'affidabilità dei siti che consultate o bloccare le pubblicità in rete. I link preceduti dalla sigla "HTTPS" sono considerati generalemente come più sicuri.

✓ **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. Pensate a consultare due fonti d'informazione differenti e verificate che i contenuti siano simili.

✓ **Consultate la nostra rubrica dedicata alla protezione dei dati**

La nostra rubrica "Sicurezza & protezione dei dati" fornisce delle informazioni complementari e illustra i possibili rischi. La rubrica contiene anche consigli per la vita quotidiana con i media, per rimanere nella legalità e propone risorse utili per bambini, giovani, genitori e insegnanti.

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