

SPAM: COME DIFENDERSI



Spamming o spam è l'invio, talora massiccio e ripetuto, tramite operatore o con modalità automatizzate, di **comunicazioni non richieste** (via telefono, *e-mail*, fax, sms o mms), senza che il destinatario abbia ricevuto un'**informativa** sul trattamento dei dati personali o abbia prestato il **consenso** a ricevere messaggi. Negli ultimi tempi, lo *spamming* sta interessando anche il mondo dei *social network* e quello dei sistemi di messaggistica per *smartphone* e *tablet*.

Lo **spammer** - cioè colui che invia lo *spam* - utilizza riferimenti (*e-mail*, numeri telefonici, ecc.) per l'invio di messaggi promozionali spesso raccolti in modo non lecito o in maniera automatica via Internet (su gruppi *Usenet*, *newsgroups*, *forum*, ecc.), mediante speciali programmi (*spambot*, ecc.) o, più semplicemente, facendo invii massivi a caso ad indirizzi *e-mail* basati sull'uso di nomi comuni

Scopo dello *spamming* è veicolare messaggi pubblicitari, ma tale pratica è legata anche a veri e propri tentativi di truffa, come il *phishing*. In Italia l'invio di messaggi automatizzati a fini promozionali non desiderati è soggetto a sanzioni amministrative e penali.

Come prevenire lo spam?

- **Non diffondere**, soprattutto *on-line*, il tuo indirizzo *e-mail* o il numero di telefono fisso o mobile;
- Se per ottenere un dato servizio (iscrizione a *newsletter*, acquisti *on-line*, ecc.) devi firmare un documento o iscriverti ad un sito web, **leggi sempre con attenzione le regole privacy e le condizioni d'uso del servizio**, e soprattutto verifica le modalità e le finalità del trattamento dei tuoi dati personali;
- Prendi in considerazione di **utilizzare più indirizzi *e-mail*** per le tue varie esigenze. Ad esempio, potresti crearne uno ad uso **esclusivamente** "commerciale", da impiegare per fare acquisti *on-line*, accedere a servizi su Internet, iscriverti a *newsletter*, ecc.. In questo modo, il rischio di «contagio spam» non coinvolgerebbe gli indirizzi di posta elettronica che utilizzi invece per le tue esigenze quotidiane più importanti (lavoro, amicizia, ecc.);
- Se hai un sito personale o un blog su cui vuoi pubblicare la tua *e-mail*, proteggila con accorgimenti che rendono la vita più difficile ai programmi (*i cosiddetti spider*) capaci di raccogliere in automatico gli indirizzi di posta elettronica per finalità di *spamming*;
- Se invii una *e-mail* a molti destinatari, **non rendere visibili gli indirizzi dei tuoi contatti** e usa la funzione "*destinatario in copia conoscenza nascosta (ccn)*". Stessa precauzione se frequenti dei *newsgroups*, dove possono essere attivi dei programmi *spider*;
- Prova ad usare i **filtri *anti-spam*** offerti, ad esempio, da alcuni programmi di posta elettronica, che possono aiutarti a bloccare tutti i messaggi provenienti da un particolare indirizzo. Tali funzioni possono essere disponibili anche per i *social network* e i servizi di messaggistica per *smartphone* e *tablet*;
- **Mantieni in efficienza il tuo pc**, scaricando periodicamente gli aggiornamenti (che contengono anche difese *anti-spam*) per il sistema operativo e gli applicativi più utilizzati, e installa eventualmente un programma *anti-virus* che offra anche una protezione *anti-spam*;
- **Se utilizzi i social network:**
 - 1) controlla le impostazioni privacy del tuo *account* eventualmente limitando la visibilità del tuo profilo;
 - 2) se disponibile, utilizza la funzione "*di blocco*" per i soggetti che inviano messaggi indesiderati;
 - 3) non dare l'amicizia a soggetti sconosciuti;
 - 4) evita di rendere pubblici sulla tua pagina personale il tuo indirizzo *e-mail* o il numero di cellulare.



Cosa non devi fare

- **Non rispondere allo spam**: la risposta può consentire allo *spammer* di stabilire che il tuo indirizzo *e-mail* è valido e attivo. Così può continuare a «spammarti» o rivendere il tuo indirizzo verificato a terzi. Può anche tentare di utilizzare il contatto creato per portare avanti tentativi di truffa.
- **Non cliccare su eventuali link** per la cancellazione dell'invio e tantomeno non fornire i tuoi dati personali senza aver prima fatto delle verifiche. Questi link potrebbero essere collegati a sistemi che consentono truffe telematiche e furti di identità, ma potrebbero anche aprire la strada a *software spia* o a virus informatici. Per la stessa ragione, **non devi mai cliccare su collegamenti ipertestuali** inseriti nel corpo del testo o **aprire ed eseguire eventuali allegati**, soprattutto se contengono estensioni tipo «.exe». Per la stessa ragione, se non sei sicuro del mittente, evita di scaricare le immagini eventualmente contenute nel corpo del messaggio *e-mail*.

Differenze tra spam e invii leciti

- Se il contatto *e-mail* o telefonico è stato **raccolto** con il **consenso del destinatario** o secondo le **modalità previste dalla legge** (es: nell'ambito di un contratto per la fornitura di un qualche servizio), non si può parlare di *spam*.
- In ogni caso, **se le comunicazioni pubblicitarie o altro tipo richieste** (es: invio di *newsletter*, ecc.) **risultano ad un certo punto indesiderate**, è tuo diritto opporvi al trattamento dei tuoi dati inviando una *e-mail* al mittente per chiedere la sospensione dell'invio o utilizzando, se disponibili, le procedure *on-line* per la cancellazione dei tuoi dati dal *database* di chi ti invia le comunicazioni.

Come agire contro lo spam?

Se sei una persona fisica puoi:

- presentare segnalazioni, reclami e ricorsi al Garante per la protezione dei dati personali
- rivolgerti al giudice ordinario per l'eventuale risarcimento del danno

Se sei una persona giuridica:

- puoi rivolgerti al giudice ordinario per il risarcimento del danno
- **non** puoi fare segnalazioni, reclami e ricorsi al Garante, che può però intervenire d'ufficio

