

SPAMMING

Lo **spamming** è una tecnica illecita di invio di messaggi indesiderati attraverso un qualunque mezzo di comunicazione.

Origine

Il termine "**spamming**" deriva da "**SPAM**", che è il nome di una carne in scatola spalmabile prodotta dalla Hormel Foods Corporation a partire dal 1937 e particolarmente nota in Gran Bretagna e negli USA per la martellante pubblicità.

A causa di questa pubblicità essa è stata presa di mira da un gruppo di comici, i Monty Python, in uno sketch, intitolato proprio "**SPAM**", del Monty Python's Flying Circus, una serie televisiva di successo della BBC, trasmessa dal 1969 al 1974.

Questa serie, concepita, scritta ed interpretata dai Monty Python, tentava di stimolare la coscienza degli Inglesi prendendo in giro, in modo spesso irriverente, le loro abitudini ed ipocrisie.

Lo sketch è ambientato in un locale nel quale la cameriera propone ad una coppia, marito e moglie, esclusivamente pietanze a base di SPAM, che, come dice la pubblicità, si può usare in ogni piatto.

Nonostante ciò sia ben accetto dal marito ed osannato dagli altri avventori, la moglie si oppone fermamente, con scarsi risultati. La "gag" sottolinea gli effetti dirompenti della pubblicità con una notevole "vis comica", anche grazie alla presenza di altri personaggi.

Se desiderate vederlo ed ascoltarlo nella versione originale in lingua inglese, premete [QUI](#).

L'uso informatico di *spamming* pare che sia nato da una email pubblicitaria del primo maggio 1978, inviata dalla Digital Equipment Corporation a tutti gli utenti di ARPANET, il padre di Internet, alla quale parecchi hanno risposto infastiditi chiedendo se si trattava di "**SPAM**". Per quella prima volta tutto si è concluso con le scuse della DEC, ma il termine è rimasto, e purtroppo anche la tecnica.

Definizione

Secondo la legislazione europea l'invio ad ogni destinatario del primo messaggio deve essere preceduto dal consenso esplicito dell'interessato (**opt-in**), mentre per quella americana il consenso è implicito e l'interessato può successivamente negare il consenso ad ulteriori invii (**opt-out**).

Questi sono i concetti generali, ma vediamo l'applicazione pratica nella legislazione italiana.

L'invio di messaggi da parte di uno sconosciuto è un fatto lecito in fase di primo contatto, sia commerciale che sociale, purché il mittente sia individuabile, l'indirizzo del destinatario sia conoscibile, il contenuto sia lecito, il destinatario sia informato sui diritti previsti dal Codice Privacy ed non abbia precedentemente negato il consenso all'invio di messaggi pubblicitari.

Quindi è **spam** il messaggio che:

- proviene da siti che rimandano ad altri siti, rendendo a volte molto difficile la sua individuazione ed un'eventuale risposta, od usa degli artifici tecnici per nascondere l'identità del mittente **(1)**;
- è indirizzato ad un destinatario "non conoscibile", cioè reperito con modalità illegittime **(2)**;
- contiene argomenti non graditi al destinatario, ad esempio pornografici, od illegali, ad esempio link a software pirata, fino a tentativi di truffa diretti od indiretti, come attacchi al vostro conto corrente bancario o proposte illusorie di lavoro;
- non indica chiaramente le azioni che il destinatario deve compiere per impedire l'invio di nuovi messaggi dallo stesso soggetto **(3)**;
- viene inviato ad un soggetto che ha, in precedenza, negato il consenso all'invio di messaggi commerciali.

Tuttavia, la maggiore utilizzazione dello *spamming* avviene solitamente con l'invio dello stesso messaggio, in "fotocopia", ad una lista di destinatari colpevoli solo di essere inclusi in un database, di provenienza spesso legale. Ciò crea problemi, oltre che ai destinatari, all'Internet Service Provider (ISP) che gestisce gli accessi al web, all'operatore di telefonia mobile che deve inviare ai cellulari gli SMS e gli MMS, alle Poste che devono consegnare la pubblicità ai vostri domicili, ecc., poiché lo *spam* può rallentare il traffico fino a bloccarlo, con notevoli costi per il sistema di comunicazione che, in ultima analisi, pagate voi.

Mezzi di contrasto

Tutti i mezzi di comunicazione possono essere veicoli di messaggi indesiderati (4).

Nell'era di Internet le email, le famose *unsolicited commercial email* o *UCE*, i messaggi commerciali non richiesti, e le voluminose *unsolicited bulk email* o *UBE*, le grosse liste di distribuzione di messaggi pubblicitari, rappresentano ampiamente la maggioranza dello *spamming*. Ciò ha portato ad una notevole diminuzione della pubblicità nella vostra cassetta postale, ma anche ad un aumento di quella tramite telefono, fisso e mobile, sia senza che con la presenza di operatori.

Vi rimandiamo a testi più corposi per conoscere nei dettagli le varie tecniche di *spamming* fin qui note, ricordandovi che, mentre state leggendo, gli *spammer*, i mittenti dello *spam*, hanno trovato un nuovo modo per colpirvi.

Le difese da adottare, anche se non garantiscono l'eliminazione del fenomeno, sono principalmente le seguenti:

- **Usare indirizzi non facilmente riconoscibili**

Uno dei metodi più utilizzati dagli *spammer* è la ricerca automatica in Internet di indirizzi di posta elettronica. Se non li avete mai comunicati via Internet, potete stare abbastanza tranquilli, altrimenti, se ad esempio siete iscritti ad un blog, utilizzate per la vostra casella di posta elettronica nomi non presenti nel dizionario o alterateli in modo che non siano riconoscibili automaticamente.

Esiste una tecnica nota come *adress munging*, con la quale, ad esempio il vostro indirizzo mario@sito.com, può diventare marioLASCIASTEMI@INPACE.sito.com, rendendovi irricognoscibile ai sistemi di ricerca automatica. Tuttavia queste tecniche non sfuggono ad uno *spammer* esperto.

- **Non utilizzare HTML o immagini**

Nei programmi di posta elettronica sono spesso incorporate le funzionalità di visualizzazione di codice HTML e immagini. L'utilizzo della prima funzionalità vi espone all'inserimento di codici di reindirizzamento ad altri siti od all'installazione di *spyware*, programmi che monitorano la vostra navigazione Internet, e dei micidiali *virus* informatici. Invece, con l'utilizzo della seconda, vi potrà essere offerta la visione di immagini offensive o pornografiche.

Per difendervi non impostate queste funzionalità come default, ma utilizzatele solo se necessario.

- **Installare antispam**

Questo software, installato sul computer o presso il *provider*, il fornitore dell'accesso a Internet, confronta l'indirizzo del mittente con elenchi di noti *spammer* e di siti "tolleranti" nei loro confronti e/o analizza il contenuto del messaggio, spostando in un'apposita cartella quelli che assomigliano a *spam*. In quest'ultimo caso, anche se ciò avviene in modo automatico, si possono presentare casi di violazione del Codice Privacy da parte dei *provider*.

- **Evitare di rispondere**

La risposta ai messaggi di *spam* è la conferma che il vostro indirizzo è valido ed attivo. Inoltre il link per la richiesta di rimozione è spesso un invito all'invio di nuovi e più frequenti messaggi.

Quindi, specialmente se il messaggio proviene da generici od anonimi siti commerciali, non rispondete.

- **Denunciare lo spam al provider**

Quando il sito dello *spammer* non è facilmente individuabile e non siete degli esperti di posta elettronica, denunciarlo al vostro *Internet Service Provider (ISP)* può rivelarsi il miglior tentativo per ridurre lo *spamming*. Infatti, conviene economicamente anche al vostro *ISP* conoscere le fonti dei messaggi di *spam* perché può ridurre i tempi di risposta del sito e liberare spazio per gestire nuovi clienti.

Molti *ISP* hanno installato complessi software *antispam*, che aumentano effettivamente il livello di servizio del sito.

Anche quando lo *spammer* è facilmente individuabile, la denuncia può portare ottimi risultati: molti *provider* chiudono immediatamente l'abbonamento e lo inseriscono nelle "*black list*", una lista di proscrizione disponibile a tutti gli *ISP*. Lo *spammer*, tuttavia, può ritornare a fare *spamming* con un nuovo indirizzo.

- **Denunciare lo spam al Garante**

Tutte le denunce al Garante per la protezione dei dati personali, se sufficientemente documentate, portano a pesanti sanzioni amministrative per lo *spammer*. Per rendervene conto andate alla sezione **Provvedimenti sanzionatori** alla pagina del **GARANTE**. Tuttavia, fondamentale per il buon fine della denuncia è la conoscenza dei dati identificativi del mittente.

Se la violazione è stata commessa da un soggetto con una stabile struttura nel territorio italiano, segnalatela con le modalità indicate nella sezione **Accesso al Garante**, altrimenti occorrerà rivolgersi al Garante per la protezione dei dati personali dello Stato in cui questa struttura è residente. Ciò è relativamente facile per i paesi dell'Unione Europea, ma può essere estremamente difficoltoso negli altri casi.

Vi ricordiamo che, per tutti i nostri Clienti, l'assistenza tecnico-legale per eventuali segnalazioni, reclami e ricorsi presso il Garante italiano per la protezione dei dati è compresa nel **SERVIZIO PRIVACY**

-
- (1) L'indirizzo email del mittente deve rendere sempre possibile una risposta da parte del destinatario od il messaggio deve chiaramente indicare l'indirizzo a cui rivolgersi per negare il consenso ad ulteriori invii. Il numero telefonico non può essere nascosto nei messaggi di comunicazione commerciale. La corrispondenza postale deve sempre indicare il mittente, sulla busta od all'interno della stessa.
 - (2) L'indirizzo email non presente sul Web è riservato. Per utilizzarlo occorre che il proprietario lo abbia reso pubblico in elenchi a cui avete accesso in modo legale. Il numero telefonico, presente in archivi costituiti prima del primo agosto 2005, è liberamente utilizzabile per fini commerciali fino al 31 dicembre 2009. Dopo tale data sono utilizzabili solo i numeri telefonici di coloro che hanno espresso il loro esplicito consenso.
 - (3) Nel messaggio deve essere inclusa, come minimo, l'avvertenza: "*Se non desidera ricevere ulteriori comunicazioni in merito da parte nostra, La preghiamo di avvisarci immediatamente*".
 - (4) Il Garante attualmente ha evidenziato i seguenti mezzi di comunicazione come possibili veicoli di *spam*: email, telefono fisso e mobile, fax, SMS ed MMS.