

FEBBRAIO 2003

Le "Norme per l'utilizzo sicuro dei Servizi 3" (di seguito anche "Security Policy") sono finalizzate a facilitare la protezione di H3G S.p.A. (di seguito "3"), dei suoi Clienti, utilizzatori e della comunità Internet in generale, da utilizzi impropri o, in alcuni casi, illegali.

Fatte salve le definizioni e le modalità di utilizzo stabilite nelle applicabili Condizioni Generali di Contratto relative ai servizi di comunicazione UMTS (di seguito CGC "3") accettate dal Cliente, la Security Policy comprende una lista non esaustiva di attività vietate e di consigli per l'utilizzo corretto dei Servizi "3" (anche solo "Servizi"), che il Cliente si impegna a rispettare e far rispettare come stabilito all'art.12.4 delle applicabili CGC "3".

Ciascun Cliente "3" è responsabile del rispetto di questa Policy per il semplice fatto di accettare ed utilizzare i Servizi.

In caso di violazioni della Security Policy, "3" si riserva il diritto di interrompere la fornitura dei Servizi e/o intraprendere azioni per impedire all'offensore di violare ulteriormente le regole stabilite ed accettate, come stabilito nelle applicabili CGC "3" e nei Regolamenti di Servizio approvati.

"3" si riserva il diritto di modificare e/ o integrare la Security Policy in qualsiasi momento; la versione più aggiornata è sempre disponibile sul sito web di "3": www.tre.it.

ATTIVITÀ VIETATE

Oltre a quanto previsto nelle applicabili CGC "3", nei Regolamenti di Servizio e in conformità a leggi, regolamenti e usi vigenti in materia, "3" considera come **abusi** le attività poste in essere attraverso l'utilizzo dei Servizi "3", di seguito esemplificate.

È proibito:

1. minacciare la sicurezza e/o l'integrità della rete "3" e/o ogni altra rete o computer, attraverso - per esempio - la trasmissione di virus, worms e altri codici malevoli o l'accesso non autorizzato a sistemi o dati;
2. ottenere o tentare di ottenere un qualsiasi Servizio "3" con ogni mezzo o strumento con l'intento di evitarne il pagamento;
3. usare i Servizi per interferire con l'utilizzo dei Servizi "3" di altri clienti o utenti autorizzati;
4. falsificare informazioni del Cliente fornite a "3" o ad altri clienti/utenti che utilizzano i Servizi "3";
5. impegnarsi consapevolmente in qualsiasi attività che causi a qualsiasi cliente che utilizzi i Servizi "3" o i servizi di un altro fornitore un cosiddetto "denial-of-service", ossia l'impossibilità di utilizzare gli stessi servizi;
6. pubblicizzare, trasmettere, o in ogni modo rendere disponibile qualsiasi software, programma, prodotto, o servizio che è mirato a violare questa Policy e/o tale che possa facilitare, a titolo esemplificativo, a) invio di posta elettronica non sollecitata, anche in quantità massicce ("mail spam" e "mail-bombing"); b) attacchi mirati a rendere impossibile utilizzare i Servizi "3" ("denial of service"); c) pirateria del software;
7. utilizzare i servizi di un altro provider al fine di facilitare le suddette attività, se un tale uso dei servizi di qualsiasi altro soggetto può ragionevolmente influire in modo negativo sui Servizi "3";
8. impegnarsi in altre attività che costituiscono analogamente violazione della legge, minaccia all'integrità di qualsiasi computer, o violano standard generalmente accettati di condotta e utilizzo di Internet.
9. specificamente all'utilizzo del Servizio E-Mail 3, è strettamente proibito a) l'invio di messaggi e-mail non sollecitati, ivi compreso l'invio di cosiddetto "junk mail" (mail "spazzatura") o altro materiale pubblicitario, politico e/o di qualsiasi altra natura a soggetti che non ne hanno fatto specifica richiesta ("e-mail spam"), se tali e-mail non sollecitate possono ragionevolmente provocare reclami; b) l'invio dello stesso messaggio o di uno simile ad uno o più newsgroups, forum o altri gruppi e liste simili (cd. "excessive cross-posting" o "multiple-posting"). "3" valuta negativamente lo "spam" di qualunque tipo e si riserva pertanto di combatterlo con meccanismi che impediscano tali abusi sulla propria rete.

UTILIZZO SICURO DEI SERVIZI "3"

Di seguito, "3" suggerisce alcuni comportamenti che - in aggiunta a quelli indicati nelle applicabili CGC e nei regolamenti di servizio "3", obbligatorie per i Clienti e/o i legittimi utilizzatori - possono essere utili al fine di elevare il livello di sicurezza nell'utilizzo dei Servizi "3".

- a) Non disattivare il codice PIN per l'accesso ai Servizi "3".
- b) Se presente, la password di accesso ai Servizi "3" non deve essere composta da una stringa di caratteri facilmente individuabili; non deve essere comunicata ad altri soggetti per nessun motivo; non deve essere trascritta o annotata in maniera evidente o visibile da altri. Username e Password non devono essere costituiti da una stringa di caratteri uguali. In caso sia stata conosciuta da terzi o abbia comunque perso di sicurezza, la password deve essere modificata al più presto.
- c) Internet non è un ambiente che, per la sua configurazione, consente la confidenzialità dei dati o delle comunicazioni. Occorre quindi accedervi considerando la sua natura di Rete pubblica.

NETIQUETTE

Tra gli altri principi per l'utilizzo sicuro dei servizi, 3 ti suggerisce di prendere visione delle norme ufficiali di cosiddetta "Netiquette", accettate e divulgate dalla Naming Authority Italiana, l'organismo che detta le procedure in base alle quali sono assegnati i nomi di dominio terminanti con il suffisso ".it". Tale insieme di principi di buon comportamento aiuta ogni utente di Internet a rispettare il "galateo" di Internet nel comunicare con altri, o nello svolgimento di varie attività on line.

Etica e norme di buon uso dei servizi di rete.

Fra gli utenti dei servizi telematici di rete, prima fra tutta la rete Internet, ed in particolare fra i lettori dei servizi di "news" Usenet, si sono sviluppati nel corso del tempo una serie di "tradizioni" e di "principi di buon comportamento" (galateo) che vanno collettivamente sotto il nome di "netiquette". Tenendo ben a mente che l'entità che fornisce l'accesso ai servizi di rete (provider, istituzione pubblica, datore di lavoro, etc.) può regolamentare in modo ancora più preciso i doveri dei propri utenti, riportiamo in questo documento un breve sunto dei principi fondamentali della "netiquette", cui tutti sono tenuti ad adeguarsi.

- 1 - Quando si arriva in un nuovo newsgroup o in una nuova lista di distribuzione via posta elettronica, e' bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi sulla Rete: in tale modo ci si rende conto dell'argomento e del modo nel quale viene trattato in tale comunità.
- 2 - Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema. Specificare sempre, in modo breve e significativo, l'oggetto (campo "Subject") del testo incluso nella mail. Se si utilizza un "signature file", mantenerlo breve e significativo.
- 3 - Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione via posta elettronica.
- 4 - Evitare, quanto più possibile, broadcast del proprio messaggio verso molte mailing list (o newsgroups). Nella maggioranza dei casi esiste una sola mailing list significativa, che costituisce il destinatario corretto e include gli utenti effettivamente interessati.
- 5 - Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale, se non quando sia necessario.
- 6 - Non condurre "guerre di opinione" sulla rete: se ci sono diatribe personali, è meglio risolverle via posta elettronica in corrispondenza privata tra gli interessati.
- 7 - Non pubblicare mai, senza l'esplicito permesso dell'autore (o degli autori), il contenuto di messaggi di posta elettronica.
- 8 - Non pubblicare messaggi stupidi o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione. Leggere sempre le FAQ (Frequently Asked Questions) relative all'argomento trattato prima di inviare nuove domande.
- 9 - Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito.
- 10 - Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso:

A - La rete è utilizzata come strumento di lavoro da molti degli utenti. Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.

B - Qualunque attività che appesantisca il traffico o i servizi sulla rete, quali per esempio il trasferimento di archivi voluminosi o l'invio di messaggi di posta elettronica contenenti grossi allegati ad un gran numero di destinatari, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in modo da ridurre il più possibile l'impatto sulla rete.

In particolare si raccomanda di:

- Effettuare i trasferimenti di archivi in orari diversi da quelli di massima operatività (per esempio di notte), tenendo presenti le eventuali differenze di fuso orario;
- Non inviare per posta elettronica grandi quantità di dati; indicare (ove possibile) la locazione (URL) dei dati nel messaggio, rendendoli disponibili per il prelievo o la consultazione sulla rete.

C - Vi sono sulla rete una serie di siti server (file server) che contengono, in copia aggiornata, documentazione, software ed altri oggetti disponibili sulla rete. Informatevi preventivamente su quale sia il nodo server più accessibile per voi. Se un file è disponibile su di esso o localmente, non vi è alcuna ragione per prenderlo dalla rete, impegnando inutilmente la linea e impiegando un tempo sicuramente maggiore per il trasferimento.

D - Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o re-distribuirlo in qualunque modo e sotto qualunque forma.

E - Comportamenti palesemente scorretti da parte di un utente, quali:

- Violare la sicurezza di archivi e computer della rete;
 - Violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
 - Compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente;
- costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge.