

**E' di alcune ore fa la notizia, rimbalzata in tutto il mondo, di un megaprogetto del governo inglese per la messa a punto, si parla già per la fine dell'anno, di un sistema per l'intercettazione trasparente della posta elettronica da e verso l'utenza inglese. E pare che lo stesso parlamento europeo non sia proprio immune all'attrattiva di questa possibilità.**

# Lontano da sguardi estranei!

## Dall'Inghilterra l'intercettazione trasparente della posta elettronica

*di Raffaello De Masi*

Ovviamente la cosa ha scatenato un putiferio in Gran Bretagna, dove le associazioni in difesa dei consumatori e garanti della libertà di comunicazione si sono fatte, anche energicamente, sentire, in difesa dei loro sacrosanti diritti. Come al solito, la cosa è stata fatta rientrare attraverso una dichiarazione del governo in cui si ammette l'esistenza del progetto (costato un centinaio di miliardi), ma che verrà finalizzato solo a indagini mirate; in altre parole l'uso del sistema sarà possibile solo dietro autorizzazione scritta del giudice. In bel modo per dire tutto e non dire nulla! E poi, come dicevano i romani, "Quis custodiet custodes?", chi controllerà i controllori?

E non basta; ascoltate questa! Pare sia stato definitivamente accertato che il popolare pacchetto RealJukebox abbia contenuto una routine che, arbitrariamente e senza alcuna periodicità, durante l'uso, trasmetteva alla casa produttrice dettagli sull'uso e sulle preferenze musicali dell'utente. Per essere precisi pare che il programma invii un pacchetto di informazioni contenente il tipo di pacchetto MP3 utilizzato, il numero di file MP3 presenti sul disco dell'utente e, se in quel momento si è

connessi a Internet, anche il titolo del brano ascoltato in quel momento. Anche qui, ovviamente, lo scandalo non è tardato a scoppiare, e la compagnia ha assicurato che la nuova versione, già in distribuzione, aprirà una finestra in cui si chiede all'utente se è disposto a trasmettere questi dati che, ipocritamente, si dichiara siano stati finora prelevati a soli fini statistici!

Ormai non si è più sicuri di nulla. Non siamo ancora all'incubo di Orwell, ma non è mica detto che il Grande Fratello debba presentarsi sotto la maschera di spietato persecutore. In Giappone ormai quasi più nessuno usa la carta di credito, che, nessuno ci aveva pensato (vero?), è un ottimo sistema per monitorare l'attività e il movimento di una persona. Ogni giorno, a ogni pie' sospinto, per accedere a servizi offerti gratuitamente (ah, che spirito francescano!) su Internet, occorre fare una lunga trafila, in cui ci viene chiesto di rivelare praticamente ogni nostro dato, e poco ci manca che ci chiedano anche quando abbiamo fatto la prima comunione e la rosolia. Vi domanderete a cosa serva dare tutta questa messe di dati, compreso indirizzo reale, codice fiscale e indirizzo di posta elettronica. Ve

lo spiego subito, in maniera brutale; queste generose persone collezionano un bel portafoglio di indirizzi, bell'e pronto per essere "affittato" a produttori che abbisognano di distribuire materiale pubblicitario, sia elettronico che cartaceo. E la legge sulla privacy? e le profferte di antispamming distribuite a piene mani nelle home page? Campa cavallo...

### **Cerchiamo di difenderci!**

La comunità Internet è piena di persone che credono che la CIA, l'FBI, il KGB e le polizie e i servizi segreti di altro mezzo mondo siano pronti a spiarcì per carpire i nostri segreti; pronti a superare le nostre password, a scoprire i nostri segreti, a leggere la nostra posta o a controllarci mentre facciamo chat. Non siamo proprio a questo, ma quanto ne siamo lontani?

Il fatto è che, da quando ci collegiamo al Internet, non facciamo altro che lasciare, a destra e a manca, tracce e impronte del nostro percorso e delle nostre attività. Non è certo molto diffici-

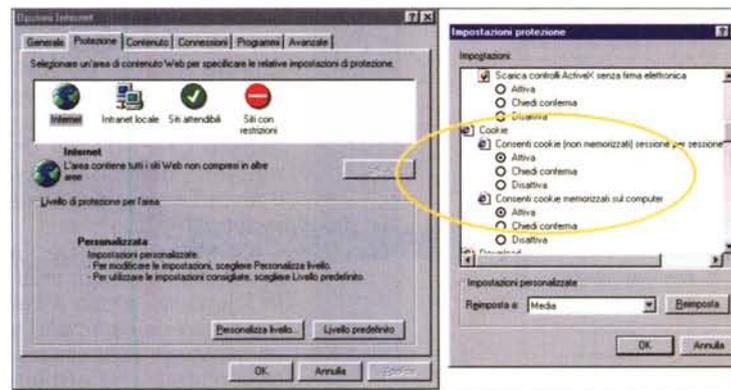
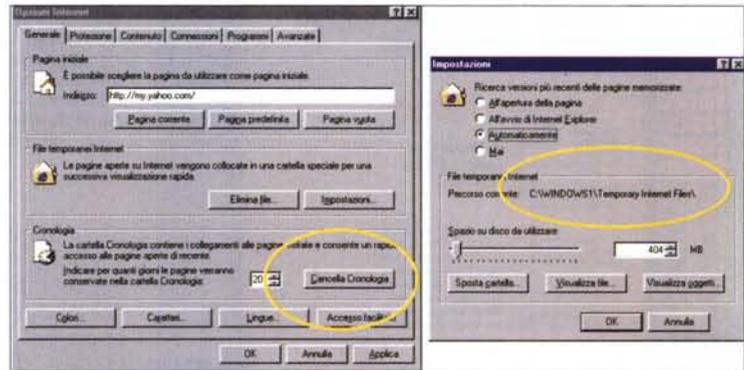
le monitorare la navigazione di un ignaro utente attraverso un semplice controllo continuo della sua connessione. Il solo sistema sicuro per tenere confidenziali i propri dati è di tagliare la linea telefonica, prendere a martellate il cellulare, tagliare la carta di credito, e ritirarsi in una grotta. In caso contrario si è soggetti al pericolo che qualcun altro possa controllare le nostre attività. Tutto sta a ridurre i danni il meno possibile. In altre parole, usare, per battere questi indiscreti occhi tecnologici, esattamente le stesse armi, la tecnologia. E un poco di sale in zucca!

Perdonatemi la banalità, ma è inutile dotare la propria casa dei più sofisticati sistemi d'allarme, se poi si ha l'abitudine di lasciare le finestre spalancate. In altri termini, non dimentichiamo le basi più semplici della sicurezza, prima di adottare le più potenti e sofisticate tecnologie di protezione, con chiavi a centinaia di bit e connessioni più sicure di Fort Knox.

Ad esempio, non lasciare mai, in computer che possono essere utilizzati da altri (ad esempio quello dell'ufficio), informazioni riservate personali, come numeri di carta di credito o di conto corrente; e non culliamoci sulla falsa sicurezza di averli custoditi con una password! Si potrebbero avere amare sorprese! Lo stesso vale quando si usa un computer a disposizione anche di altri per operazioni come credito in linea o acquisti; non inserire mai dati "sensibili" in un sito non dotato di "secure server", e, se proprio si è costretti, assicurarsi di cancellare la cache e la cronologia dopo l'uso, e a conclusione della navigazione (in Explorer, Strumenti# Opzioni Internet# Generali# Cancella Cronologia).

Molti servizi, a cominciare dal collegamento iniziale, si basano sull'uso di password (ad esempio e-mail, drive virtuali personali, servizi bancari on-line, ecc.). Bisognerebbe avere password diverse per ognuno di essi (salvo riunire sotto una stessa stringa quelli di scarsa importanza) e cambiarle con una certa frequenza, se non tutte almeno quelle di importanza vitale. Quando si sceglie un nome, cerchiamo di essere creativi e non usiamo dati facilmente prevedibili, come nomi di mogli e figli, date di nascita, numeri telefonici o targa della macchina, anche se scritti al contrario, e con una lettera sì e una no. Una combinazione senza significato di lettere maiuscole, lettere minuscole e nu-

Per non lasciare traccia della nostra navigazione, ricorriamo alle opzioni del nostro browser!



I cookie sono utilissimi, ma possono nascondere qualche insidia! Impariamo come difenderci!

meri è poco facilmente prevedibile da una persona diversa da chi l'ha creata (ovviamente saremo tanto furbi da evitare di tenere nel portafogli un foglietto

di promemoria; non ridete, molti si portano appresso, accanto alla tessera del Bancomat, il foglietto con il numero di accesso. O magari fanno un bel file di testo, e lo conservano sul desktop!)

## Password, sempre password.

Molte persone usano continuamente il loro PC, magari un portatile, come compagno di lavoro e come diario-segreteria personale. Mai come

Anonymizer, <http://www.anonymizer.co> vi permetterà di viaggiare su Internet senza essere intercettati

*http://www.privacy.org è una organizzazione dedicata alla difesa della privacy, che indice ogni anno un concorso per l'assegnazione degli Orwell d'oro alle persone, siti o organizzazioni che si sono distinte nel violare la privacy delle persone. Bel riconoscimento!*

questa rubrica il mese passato. Se i bambini sono piccoli, forse la soluzione più interessante è rappresentata da Kid-Desk Internet Safe, che crea quello che viene definito un "walled garden", un giardino circondato da mura, vale a dire un'area dove il bambino si può muovere ma da cui non può sconfinare. Pregevole e affidabile; lo trovate da <http://www.ionasoft.com/>.

particolare documento), e anche molti clienti di posta elettronica sono dotati di chiave delle rispettive cartelle. Non credere di poter proteggere il PC ricorrendo alla password di Windows. Come abbiamo già diverse volte fatto notare su queste pagine, essa riguarda solo le preferenze d'uso e, a meno di non essere legati a un network, basta premere il tasto Esc per superare lo sbarramento.

Se il vostro PC è utilizzato da altre persone nel vostro ufficio, e desiderate che la vostra attività, una volta conclusa, non sia più raggiungibile da alcuno, tenete bene da conto che non basta gettare nel cestino il materiale elaborato e poi "tirare la catena". I dati sarebbero facilmente recuperabili con la più stupida delle utility di "undelete" reperibile in commercio.

Lo stesso vale per la password sul BIOS; inutili fidarsi, superarla è come rubare le caramelle a un bambino. Basta togliere la batteria che alimenta i servizi interni e il gioco sarà fatto; col vantaggio di non sentirne neppure piangere il ragazzino.

Se avete necessità di gestire la cosa proprio in questo modo, usate un'utility che sovrascrive ripetutamente l'area occupata dal file cancellato; la trovate in McAfee Office (<http://www.mcafee.com>) e in System Mechanic (si chiama Incinerator, <http://www.iolo.com>)

Molti dischi rigidi di qualità e molti PC di marca vengono forniti di utility destinati al recupero di dati, in caso di crash del sistema.

Questi pacchetti, come Nasp'N'Shot e GoBack, possono essere utilizzati anche per recuperare dati frettolosamente cancellati; quindi disinstalliamoli. Inoltre, teniamo in considerazione che usare il PC del posto di lavoro per usi personali potrebbe non essere compatibile con le direttive del nostro datore di lavoro, e che, nonostante tutta la privacy di questo mondo, ci sono diversi sistemi di monitoraggio dell'attività dei dipendenti.

in questo caso l'uso delle password è indispensabile (pensate solo allo smarrimento o al furto del portatile!).

La maggior parte dei word processor, spreadsheet e, ovviamente, database includono questa opzione (alcuni possono essere protetti anche con una doppia password, in modo da legare a due persone differenti l'apertura di un

Se il PC viene utilizzato anche dai nostri figli, potrebbe essere il caso di utilizzare un pacchetto come CyberSitter (<http://www.cybersitter.com>) o CyberPatrol (<http://www.cyberpatrol.com>), o ancora NetNanny (<http://www.netnanny.com>) di cui abbiamo parlato in

**C**osa è PGP? Semplice, è un programma di cifratura della nostra posta che permette di spedire e ricevere messaggi che non possono essere letti durante il transito in rete. Il pacchetto si recupera da <http://www.pgpi.org> e, una volta installato, si aggiunge automaticamente a Outlook, creando in questo anche nuovi bottoni.

Per utilizzarlo occorre creare, la prima volta, la nostra chiave PGP. Schiacciamo il bottone appena creato, e ci troveremo di fronte a una finestra che ci chiederà una serie di dati, tra cui anche l'indirizzo di posta elettronica (stare molto attenti a digitare quest'ultimo dato; se si dispone di diversi indirizzi di posta, digitare esattamente quello che poi verrà gestito da PGP; la precisione è necessaria, altrimenti la chiave PGP sarà inutilizzabile). Ci verrà chiesto poi di digitare una password (in gergo passphrase) che terrà nascosta a occhi indiscreti la nostra chiave - ri-

## PGP, l'angelo custode della nostra posta

cordiamoci che più lunga è la password più è difficile da violare. Andiamo avanti e il programma ci chiederà alcune personalizzazioni riguardo all'ambiente; all'inizio lasciare tutto com'è, ci sarà tempo poi per provare le altre personalizzazioni. Ci verrà chiesto infine se si desidera fare l'upload della nostra chiave pubblica su un server PGP; la cosa è conveniente, in quanto non saremo costretti poi a inviare la stessa chiave a ogni utente

ci invieremo posta.

A questo punto è finito tutto; usiamo Outlook nel solito modo e, se desideriamo inviare un messaggio cifrato, schiacciamo il nuovo bottone Encrypt; o, se si vuole dimostrare che il messaggio arriva proprio da parte nostra, schiacciare Sign. Pochi minuti, insomma, per poi usare la nostra posta in sicurezza.

**Intel's Online Privacy Policy**

Your right to privacy is very important. We recognize that when you choose to provide us with information about yourself, you trust us to act in a responsible manner. We believe this information should only be used to help us provide you with better service. That's why we have a policy in place to protect your personal information. Intel Corporation is a Premier Sponsor and member of the TRUSTe Privacy Program.

This policy covers Intel's terms of corporate web sites, which include [www.intel.com](http://www.intel.com), [www.intel.com/usa](http://www.intel.com/usa), [www.intel.com/usa/privacy](http://www.intel.com/usa/privacy), and [www.intel.com/usa/privacy/usa](http://www.intel.com/usa/privacy/usa). This statement is not applicable to the following subsidiary web sites: [www.intel.com/usa/privacy/usa](http://www.intel.com/usa/privacy/usa), [www.intel.com/usa/privacy/usa](http://www.intel.com/usa/privacy/usa), [www.intel.com/usa/privacy/usa](http://www.intel.com/usa/privacy/usa), and [www.intel.com/usa/privacy/usa](http://www.intel.com/usa/privacy/usa), which each have their own posted privacy policies. We encourage you to take the time to read the local privacy policy and those of any web site you visit.

Below is a summary of Intel's online privacy policy.

**What personal information do we collect?**  
In general, when you visit our web sites and access information you remain anonymous. Before we ask you for information, we will explain how this information will be used. We will not provide any of your personal information to other companies or individuals without your permission.

Some of our web sites require registration to access, although typically all that's required is your e-mail address and some basic information about you, such as job function.

There are occasions when we will ask for additional information. We do this to be able to better understand your needs, and provide you with services that we believe may be valuable to you. Some examples of information our web sites collect include name, address and phone number. We give you the opportunity to elect not to receive material from us. If you sign up for an Intel electronic newsletter or e-mail list, each message will include instructions on how to "unsubscribe" from that list.

**Protecting your privacy**  
We will take appropriate steps to protect your privacy. We will also take reasonable security measures to protect your personal information in storage. For example, if you create an account with your credit card information to make an online purchase, we encrypt the card number. Additionally, access to personally identifiable information is limited to individuals needing such access to perform their job function.

We will not provide any of your personal information to other companies or individuals without your permission. However, we may need to provide your name and delivery address to third parties that are used for the purposes of delivering specific services to you (e.g., customer support, or a shipping company) if you have asked us to send something to you. Likewise, we will share your credit card information with the appropriate subscription and processing companies, in the event you wish to purchase something via credit card. These companies will not use this information for any other purpose and will not disclose the information to anyone else.

We provide links to third party sites. Since we do not control these web sites, we encourage you to review the privacy policies posted on these third party sites.

**Children's privacy**  
None of the Web sites covered by this policy knowingly collect personally identifiable information from children under age 13. If we discover that a child under the age of 13 has provided us with any personally identifiable information, we will delete that information from our systems.

Intel encourages parents to go online with their children. Parents should understand the sites their kids are visiting and which sites are appropriate. There are parental control tools available such as browsers and filtering software that prevent children from accessing inappropriate sites. Children should never give out personal information on the internet, such as name, address, phone number, or name of a school, unless supervised by a parent or responsible adult. Look for a privacy policy on a web site and find out how information collected from children is treated. Parents should teach their children to look for that policy that displays a privacy policy.

**Use of cookies**  
Intel web sites use cookies for various reasons. Cookies enable us to provide you with a better experience by allowing us to understand and tailor areas of our web site area of interest to our visitors. Intel also uses cookies when you register for one of our web programs. In this situation, a cookie will store useful information that enables our web site to remember you when you return to visit us. Intel can only read cookies from Intel web sites. If you choose to disable cookies in your browser, you can still access most of our web sites.

**Data storage and processing in the United States**  
Many of our web sites that collect information will process and store that information in databases located in the United States.

**How can you update the personal information you have provided to Intel?**  
You can help Intel maintain the accuracy of your information by notifying Intel of any changes to your address, site, phone number or e-mail address. Most of our programs allow you to make the changes yourself by following the instructions on the program's membership profile page.

If you need assistance in updating your information, please contact the Customer Support team ([customer@intel.com](mailto:customer@intel.com)). To aid the agents in processing your request, please include our contact information (name, address, e-mail), the name of the Intel program or service you need the changes applied to, and the details of the change (e.g., update email address, unsubscribe from a newsletter). This information you provide to Intel Customer Support will also be covered by this policy.

**How to unsubscribe from email newsletters**  
If at any time you wish to stop receiving an electronic newsletter from Intel you can unsubscribe as explained in the newsletter.

**Newsgroups / Forums / Message Boards**  
Keep in mind that information posted to an internet forum is public.

**Overview**  
Intel Corporation is a Premier Sponsor and member of the TRUSTe Privacy Program. TRUSTe is an independent, nonprofit industry whose mission is to build user trust and confidence in the internet by enforcing the principles of disclosure and informed consent. Because this site may be demonstrable to consumers as your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

By participating in the TRUSTe program, Intel Corporation agrees in the negligence of nothing you if the following:

1. What information of yours is collected.
2. How the information is used.
3. With whom the information may be shared.

**Questions?**  
If you have comments or questions on this policy, we are dedicated to protecting your personal information, and will make every reasonable effort to keep that information secure. Due to the rapidly evolving technologies on the internet, we may occasionally update this policy. All revisions will be posted to this site.

Questions regarding this statement should be directed to [privacy@intel.com](mailto:privacy@intel.com). If we have not responded to your inquiry or your inquiry has not been satisfactorily addressed, please contact TRUSTe. Intel is committed to user privacy in our products and services. Read Intel's "Privacy Policies".

[Back to top](#)

Legal Information and Privacy Policy © 2000 Intel Corporation

*aAnche Intel è molto attenta alla privacy dei suoi clienti, come membro della TRUST Privacy Program. I nostri bambini vogliono navigare con noi; accontentiamoli, partecipando alle loro avventure!*

**The International PGP Home Page**

**Download the latest version**  
Here you may download the latest freeware PGP version for your platform, whether you want the international or the US variant.

**Latest news**  
2000/2/10 - New mirror site opened in Hungary  
2000/1/31 - PGP 6.5.1 available for download  
1999/1/13 - US web PGP support begins  
1999/1/19 - German lock body PGP development  
1999/1/11 - PGP 6.2 available for download  
1999/1/07 - PGP 6.5 available for download  
1999/1/04 - PGP 6.5 is released by IAI  
1999/1/01 - PGP 6.5 is released by PGP  
1999/1/01 - PGP 6.5.1 beta 2 for Linux released  
1999/0/29 - New mirror site opened in CT  
1999/0/29 - PGP Home Page site 1.0 online beta  
1999/0/23 - Summary of PGP 6.5.1 completed  
1999/0/16 - USA life support control on credit  
1999/0/14 - Mail Essentials with PGP support

Search:

[PGPI Home](#)

**b2bnow.com 62 product categories**

**PGP Interactions Page**

Click here for the French version Click here for the German version  
Click here for the Sp. March version Click here for the Italian version  
Click here for the Slovene version

[Go to Index](#) [Go to Chart](#)  
[Go to my homepage](#) [Go to my address](#)

**Status of the PGP-Users List (updated 3/26/00)**

Those of you subscribe to the [pgp-users@milos.stevanovic.net](mailto:pgp-users@milos.stevanovic.net) mailing list may have noticed that a mess to have led. The Rsvetov.net servers seem to be offline, and Fred (the moderator) is missing. Anyone with information, please let us know!

*La pagina della <http://www.pgpi.org>. Il più popolare pacchetto di crittografia di posta è disponibile in diverse versioni dedicate ai più differenti sistemi operativi, dal Windows al Mac all'Amiga e perfino allo Psion e al BeOS*

Forse la cosa migliore è proprio non usare il PC dell'ufficio!

## Biscottini da uno sconosciuto.

Indipendentemente dalla manipolazione dei dati personali conservati sul PC, occorre tenere presente che navigare nella rete è sempre fonte di espo-

sizione, magari anche per dati non proprio riservati. Navigando è facile essere monitorati riguardo al nostro accesso e a una serie di altri dati e valori, come tipo di browser usato, IP address, e perfino risoluzione del nostro schermo. Non ci credete? Provate a collegarvi a <http://www.anonymizer.com>, per una dimostrazione in linea e, eventualmente, per prendere le opportune precauzioni.

I "cookie", i biscottini che riceviamo quando visitiamo molti siti, sono una grande comodità e, poiché sono facilmente editabili, ben difficilmente eventuali "pirati" ricorrono ad essi per attaccare il nostro sistema. Comunque, se il baco del sospetto vi rode fin nell'intimo, chiedete al vostro browser di non accettarne; andare sempre in Opzioni

Internet e scegliendo Protezione Personalizza Livello. Qui, oltre a disabilitare l'accettazione dei cookie, potremo ulteriormente personalizzare altre scelte, come quella relativa ai plug-in ActiveX, agli applet Java e così via. La contropartita è rappresentata dalla continua richiesta, però, di riempimento di finestre di accesso. C'è da dire, però, che i cookie possono essere usati anche per scopi, non diciamo illeciti, ma non proprio corretti. Ad esempio quelli depositati dai banner pubblicitari servono per determinare certe abitudini dell'utenza che, anche se non investono informazioni personali, possono essere usate a scopo di marketing.

E così abbiamo concluso. Non avremo certo sconfitto il grande fratello, ma almeno non siamo state vittime prone; a presto!