Norton Cybercrime Human Impact Report 2010

INDICE

1. Introduzione

Il ruolo di Internet nelle nostre vite continua a crescere e ad evolvere. Proprio come ha rivoluzionato il nostro modo di ricercare informazioni, divertirci e lavorare, sta trasformando anche le nostre relazioni sociali. Tuttavia, accanto ai benefici e agli sviluppi delle tecnologie informatiche, la minaccia del cyber crimine sta aumentando esponenzialmente.

I criminali informatici sono sempre più organizzati e sofisticati e l'impatto delle loro azioni può avere conseguenze poco piacevoli. Da semplici hacker isolati che lavoravano su un PC domestico lanciando attacchi contro singoli computer, si è passati a vere e proprie organizzazioni che perpetrano crimini su scala globale. I ragazzini che facevano gli hacker per hobby e curiosità sono quasi scomparsi per lasciare il campo a nuove generazioni che lo fanno per un profitto e che sono assoldati dalla criminalità organizzata.

Symantec ha pertanto commissionato una ricerca, NCHIR (Norton Cybercrime Human Impact Report), che contiene una sintesi dell'indagine di StrategyOne - società indipendente di ricerche di mercato - sul comportamento online degli adulti a livello globale. L'obiettivo è capire le ultime tendenze associate all'uso di Internet, le differenze più rilevanti nell'approccio alla rete dei diversi paesi, i rischi online che minacciano gli utenti, e i comportamenti più diffusi adottati per difendersi dai potenziali attacchi informatici .

L'indagine è stata condotta in 14 paesi (Australia, Brasile, Canada, Cina, Francia, Germania, India, Italia, Giappone, Nuova Zelanda, Spagna, Svezia, Regno Unito, USA) su un totale di 7066 adulti. Le interviste sono state effettuate tra il 2 e il 22 Febbraio 2010, in tutti i paesi gli intervistati hanno risposto ad un questionario online.

Dallo studio è emerso che il 65% degli intervistati è stato vittima del cyber crime, non sorprende quindi che meno di 1 adulto su 10 si senta sicuro in rete e il 34% ammetta di non sentirsi protetto. Ma quali sono le tendenze analizzate e le particolarità che accomunano o differenziano i diversi paesi?

2. Tendenze principali

2.1 Women do it better

Uomini e donne sembrano arrivare da pianeti lontanissimi e anche in tema di sicurezza informatica le differenze sono evidenti.
Dall'indagine di Symantec, infatti, gli uomini si dimostrano più sprovveduti delle donne nei comportamenti online, lasciandosi sedurre più facilmente da e-mail dal contenuto erotico o che promettono denaro facile che si rivelano poi delle truffe. Inoltre, sono più propensi a condividere, anche con estranei, informazioni riservate: il 62% (contro il 65% delle donne) evita di lasciare il proprio numero di carta di credito su Internet. Quando si parla di shopping, però, si riscattano: sono molto più prudenti infatti rispetto al gentil sesso, dichiarando di utilizzare diverse carte di credito e indirizzi e-mail per effettuare acquisti online in totale sicurezza. Pur di riuscire ad acquistare le scarpe alla moda tanto sognate, le donne si dimostrano invece troppo frettolose nello sfoderare la propria carta di credito e rilasciare informazioni sul proprio conto corrente.
Un dato sorprendente e inaspettato riguarda l'utilizzo di Internet per spettegolare: è emerso infatti che fare gossip online agli uomini piaccia più delle donne, che invece si dimostrano più riservate. Inoltre, mentre il 29% degli uomini pubblica in rete foto imbarazzanti degli amici, il 51% delle donne chiede addirittura il permesso prima di taggare sui social network.

Ma una volta scottati da una brutta esperienza online come si comportano i due sessi?
Le donne non ripetono lo stesso errore due volte: il 54% (contro il 48% degli uomini) dichiara di aver modificato le proprie abitudini per evitare altre esperienze negative, mentre le meno tecnologiche chiedono aiuto ad amici, famigliari o esperti per risolvere il

problema. Gli uomini invece tendono a sottovalutare l'accaduto, senza preoccuparsene troppo: solo il 29% (contro il 34% femminile) si rassegna a cambiare le proprie abitudini di navigazione, evitando di visitare i siti più rischiosi.
Infine, il luogo comune che vorrebbe gli uomini più tecnologici rispetto alle donne sembra avere radici fondate: dall'indagine emerge infatti che sono più propensi ad usare alcuni accorgimenti per la propria sicurezza online, come tenere aggiornato il software di protezione (69%) ed effettuare regolarmente il backup dei dati (33%).

2.2 Italiani popolo di santi, navigatori e … bugiardi online

Per gli internauti nostrani il detto "le bugie hanno le gambe corte" non vale. Gli italiani, infatti, cedono al fascino della possibilità di adottare identità false online più degli altri Paesi: il 41% ha ammesso di mentire in rete, e l'abitudine più frequente è quella di usare un nome falso (29%). Gli inglesi, oltre ad essere i più onesti (solo il 12% ha usato un nome falso), sono i più attenti alla netiquette, solo il 18% infatti ha dichiarato di aver finto di essere qualcun altro. In Cina il 22% ha ammesso di falsificare l'età e il proprio status economico, mentre gli indiani mentono soprattutto sulla situazione sentimentale (19%).

Gli utenti ritengono che in rete tutto sia concesso: gli intervistati hanno infatti affermato di non riuscire a resistere alla tentazione di scaricare musica o film gratis, curiosare sul profilo di social network di qualcun altro, acquistare online beni contraffatti come vestiti o medicinali. E come biasimarli? Sono attività diventate ormai quotidiane che non mettono a disagio, per cui spesso non ci sfiora il pensiero che alcune di esse potrebbero essere immorali: a chi non è mai capitato di avere la connessione WiFi temporaneamente fuori uso e di prendere in prestito quella di un ignaro condomino?
La tabella di seguito illustra le attività che gli intervistati ritengono più o meno legali/illegali, morali/immorali:

LEGALITA'

LEGALE	LEGALE MA FARLO METTE A DISAGIO
• Condividere/ritoccare immagini di altri (10%) • Scaricare un singolo musicale gratis (10%) • Scaricare un film gratis (8%)	• Controllare la mail o la cronologia dei siti di qualcun altro senza autorizzazione (22%) • Condividere/ritoccare foto di altri (20%) • Utilizzare lavori/ricerche recuperati online e spacciarli come propri/utilizzare la connessione WiFi di qualcun altro (14%)
ILLEGALE MA NON IMMORALE	**ILLEGALE E IMMORALE**
• Scaricare un singolo musicale gratis (37%) • Scaricare un film gratis (35%) • Scaricare un intero album musicale gratis (33%)	• Utilizzare o vendere online informazioni personali di altri/Compromettere l'account di altri utenti (87%) • Fingere di essere qualcun altro (69%) • Utilizzare lavori/ricerche recuperati online e spacciarli come propri (66%)

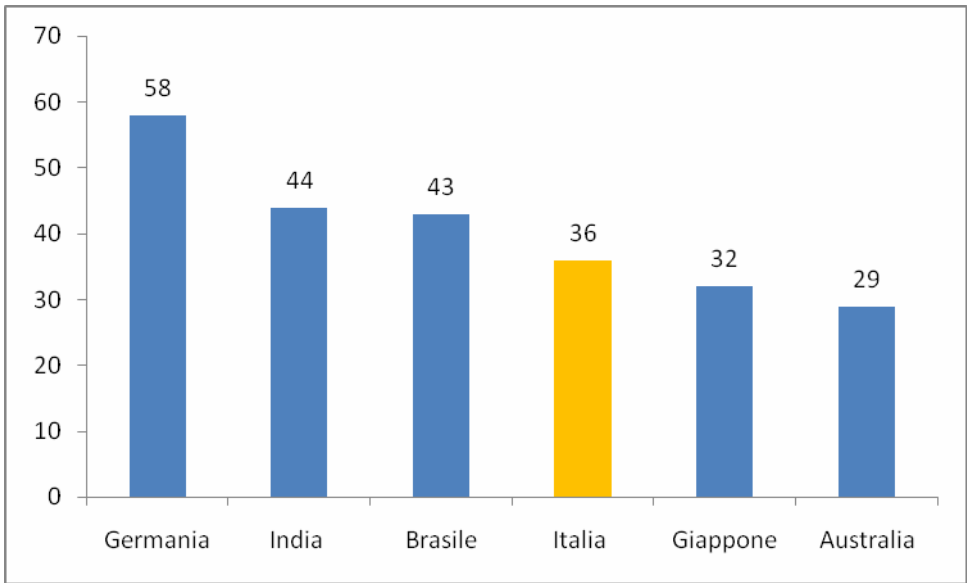
IMMORALITA'

2.3 Cybercrime, ma quanto mi costi?

Una volta diventati vittima di un crimine informatico, tutte le azioni volte a eliminare il problema comportano dei costi in termini sia economici che temporali. Tre vittime su dieci sostengono di non aver mai completamente risolto il cyber crime e per il 28% degli intervistati la più grande seccatura è stata il tempo impiegato per cercare la soluzione, più che la perdita dei dati.

In Italia, risolvere un problema di cyber crimine costa a ciascun utente circa 93 euro e il tempo che occorre è il quarto più lungo esaminato, circa 36 giorni. Fanno meglio di noi gli svedesi che riescono ad eliminare la minaccia in solo 9 giorni, un vero e proprio record rispetto alla media globale di 28. I tedeschi invece sono delle tartarughe in confronto, impiegandone ben 58!

GIORNI IMPIEGATI PER RISOLVERE IL CYBERCRIME: I 6 PAESI PIU' LENTI



Il 36% degli italiani ha affermato di non aver mai completamente risolto il cyber crimine, ma non lamentiamoci troppo visto che in Giappone è il 60% degli utenti a non aver raggiunto la soluzione. Gli spagnoli invece sono i più virtuosi: solo il 14% ha sperimentato difficoltà.

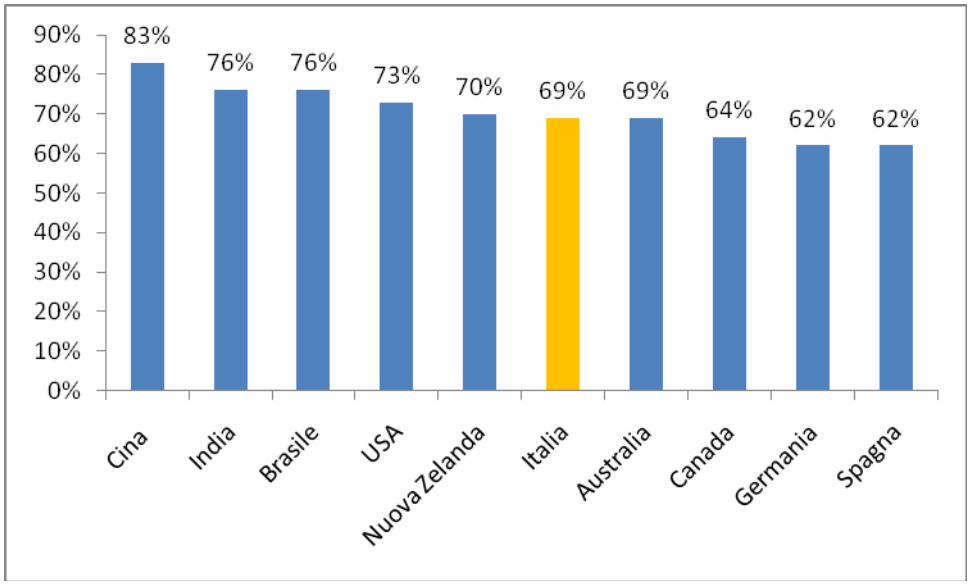
Inoltre, il 79% degli intervistati ritiene che le possibilità di identificare e punire i criminali siano davvero poche o addirittura nulle. Poca fiducia nella giustizia, ma non solo: alla difficoltà oggettiva di eliminare i problemi causati da un attacco informatico, si aggiunge la

complessità del panorama del cyber crimine. L'hacking oggi sta assumendo sempre più le sembianze del crimine organizzato ma solo il 21% degli intervistati è cosciente di questo fenomeno, con l'eccezione di una buona percentuale di brasiliani (34%) che invece ha dichiarato di sospettare che dietro un’azione di cyber crime si nasconda più di un criminale.

2.4 Tutto il mondo NON è paese

La Cina si conferma capitale mondiale del cyber crime, con l'83% degli utenti che ha affermato di essere stato vittima di un attacco informatico, mentre è in Giappone il tasso più basso di vittime, solo il 36%.

PERCENTUALI DI VITTIME COLPITE DA ATTACCHI ONLINE: LA TOP TEN DEI PAESI



Gli atteggiamenti nei confronti della criminalità variano da paese a paese: i giapponesi, ad esempio, ritengono che virus e malware siano legati al cybercrime più di quanto lo pensino i brasiliani. In Cina le molestie virtuali, i predatori sessuali online, il phishing e il furto d'identità sono considerate attività criminali, ma meno gravi di altre, proprio perché sono minacce non molto diffuse, al contrario invece dei virus e dei malware che colpiscono ben il 65% dei cinesi.

Nonostante conoscano molte delle attività perpetrate dai cyber criminali, le persone hanno dichiarato di seguire solitamente poche regole volte a difendersi dagli attacchi, che sono utili ma di certo non sufficienti.

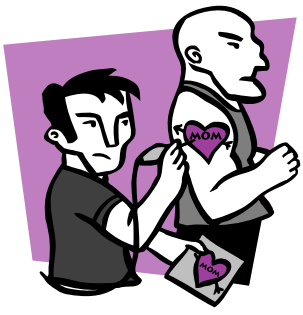
Per proteggere le proprie informazioni personali dagli hacker, gli intervistati hanno dato risposte differenti: ad esempio, la maggior parte degli australiani (89%) ha dichiarato di eliminare le mail con allegati sospetti, mentre i tedeschi hanno dimostrato meno superficialità, affermando di aggiornare spesso i software di sicurezza (79%); in India, il 76% evita di lasciare dettagli come il numero della carta di credito o gli indirizzi e-mail, e il

74% degli statunitensi ha affermato di non scaricare applicazioni software da siti che non conoscono; inglesi e francesi (66%) controllano spesso l'estratto conto bancario.

Analizzando i dati italiani, è emerso che il 67% dichiara di non comunicare informazioni personali, anche se poi il 76% non effettua il backup dei file regolarmente, il 74% non utilizza carte di credito e indirizzi mail differenti per gli acquisti online, e il 71% non ha un sistema di controllo del browser per identificare siti pericolosi.

I più negligenti sono i giapponesi: solo il 9% degli intervistati, infatti, cambia le password di frequente e solo il 20% effettua il backup dei file; seguono i cinesi, più della metà infatti non si preoccupa nemmeno di eliminare le e-mail con allegati sospetti.

In caso di attacco informatico, solo il 51% degli intervistati cambierebbe il proprio modo di agire online; i più fiduciosi nella giustizia sono gli italiani, infatti il 51% chiamerebbe la polizia, mentre il 63% degli inglesi preferirebbe rivolgersi alla propria banca o ad altre istituzioni finanziarie. I brasiliani invece preferiscono farsi giustizia da soli (38%), cercando di identificare il criminale senza l'aiuto di nessuno, mentre in Giappone si sentirebbero più sicuri chiamando il proprio internet service provider (32%).



2.5 Nessuna chirurgia al laser può cancellare un tatuaggio digitale

Le attività in rete tendono a lasciare un segno: sia che si tratti di una foto imbarazzante pubblicata senza il nostro permesso, di un post di cui ci si è pentiti, o di un pettegolezzo dannoso, la maggior parte della popolazione intervistata (45%) crede che sia impossibile ripristinare completamente una reputazione online negativa. I più pessimisti sono i canadesi (57%) seguiti dagli spagnoli (54%) e dagli australiani (51%), mentre gli italiani si collocano in una posizione intermedia (42%). I più ottimisti sono invece i cinesi, solo il 26% crede infatti che la reputazione di una persona possa essere messa in pericolo online.

Essere un buon cittadino virtuale

Esiste un galateo anche online, e dallo studio emerge che le regole della “netiquette” sono condivise dalla maggior parte degli intervistati e solo il 2% dichiara di non adottare comportamenti che non danneggino gli altri utenti. L’80% evita di perseguitare e di minacciare altre persone, il 77% ritiene che sia scorretto diffondere lo spam, il 74% evita di divulgare foto imbarazzanti, il 69% chiede il permesso prima di divulgare dati riservati, il 62% non spettegola online.

3.I consigli di Symantec

Per una efficace protezione dagli attacchi informatici, Symantec suggerisce di seguire alcuni consigli di seguito elencati:

- Utilizzare una soluzione per la sicurezza Internet che combini antivirus, firewall, rilevamento delle intrusioni e gestione delle vulnerabilità per proteggersi il più possibile dalle minacce a tecnica mista e da altre tipologie di malware.

- Accertarsi che le patch per la sicurezza siano aggiornate e che vengano applicate tempestivamente a tutte le applicazioni vulnerabili.
- Assicurarsi che le password contengano sia lettere sia numeri, modificandole di frequente. Le password non dovrebbero corrispondere a parole presenti nei dizionari.
- Non consultare, aprire o lanciare in esecuzione alcun allegato di posta elettronica inaspettato e di cui non sia nota la funzione.
- Aggiornare le definizioni dei virus con regolarità. In questo modo è possibile proteggere i propri computer contro le più recenti tipologie di virus in circolazione.
- Evitare di divulgare informazioni personali o finanziarie a meno che la richiesta non provenga legittimamente da una fonte confermata.
- E’ fondamentale essere consapevoli dei rischi che possono automaticamente crearsi con l'installazione di programmi per file sharing, download gratuiti e versioni di programmi freeware e shareware. Selezionare link e/o allegati all'interno di messaggi di posta elettronica (o IM) può esporre i computer a inutili rischi. Accertarsi che sui desktop vengano installate solamente le applicazioni approvate dall'azienda.
- Leggere le licenze EULA (End-User License Agreement) e con attenzione comprenderne le clausule. Alcuni rischi possono verificarsi dopo che l'utente ha accettato la licenza EULA o in conseguenza di tale accettazione.
- Diffidare dei programmi che evidenziano inserzioni pubblicitarie all'interno dell'interfaccia utente. Molti programmi spyware tengono traccia di come un utente reagisce alle varie pubblicità, e la loro presenza è indice di potenziali minacce.