



G Data

Studio sulla sicurezza 2011

Come vengono valutati i pericoli
di Internet dagli utenti?

Go safe. Go safer. **G Data.**



Sommario

1 Riepilogo.....	2
1.1 Portata e finalità dello studio	2
1.2 Quanto sono conosciuti dai navigatori i pericoli di Internet?	2
2 Metodologia dello studio	3
3 Risultati dello studio sulla sicurezza 2011 di G Data	5
3.1 Ma come si difendono dagli attacchi	6
3.1.1 Come valutano gli utenti le prestazioni delle soluzioni antivirus gratuite?.....	7
3.1.2 Numero di PC non protetti	9
3.1.3 Suite o semplice antivirus?	10
3.2 Quali sono i luoghi dove i navigatori di Internet si aspettano di trovare i maggiori pericoli?.....	12
3.2.1 Le undici tesi della sicurezza di Internet.....	12
3.2.2 Chi è meglio informato: i giovani o gli utenti di Internet più grandi?	17
3.2.3 Qual è paese in cui gli utenti di Internet sono più informati sui pericoli?	19
3.2.4 Sono gli uomini i migliori navigatori?.....	20
3.3 Comportamento nei social network.....	22
3.3.1 Chi utilizza i social network in modo più sicuro uomini o donne?.....	24
3.3.2 Chi utilizza i social network in modo più sicuro: i più giovani o i più anziani?	25
4 Conclusioni	26
Appendice.....	28
G Data Software AG.....	28
Survey Sampling International.....	30
Glossario.....	30

1 Riepilogo

1.1 Portata e finalità dello studio

I mezzi d'informazione riportano ogni giorno notizie di nuovi attacchi agli utenti di Internet e alle aziende, segnalando furti di dati, nuovi virus e le strutture del cartello del crimine elettronico. Gli utenti privati sono ormai costantemente nel mirino degli autori di tali crimini, divenendo sempre più vittime delle bande internazionali di criminali della rete. Nell'era di Internet, la protezione dell'identità digitale riveste dunque un'importanza fondamentale per l'intera società. Per la protezione dei PC, gli utenti hanno a disposizione diverse soluzioni di sicurezza informatica. Ma quanto sono effettivamente informati sui pericoli delle rete e sui metodi utilizzati dai criminali? Ne sanno più i giovani o i più anziani sulla sicurezza IT, sono più informati gli uomini o le donne? Lo studio internazionale sulla sicurezza 2011 condotto da G Data risponde a molte di queste e altre domande, mette alla prova i miti sulla sicurezza IT e illustra in che modo gli utenti valutino effettivamente i pericoli di Internet.

1.2 Quanto sono conosciuti dai navigatori i pericoli di Internet?

Lo studio sulla sicurezza 2011 di G Data ha confrontato i risultati dell'indagine (ovvero la percezione e la stima dei pericoli) con i pericoli effettivi. L'analisi dimostra che, in molti ambiti, le conoscenze degli utenti di Internet sono ancora lacunose o obsolete.

Quasi tutti gli intervistati sono consapevoli dell'esistenza dei pericoli e si impegnano a proteggere il proprio PC. Tuttavia, tale conoscenza raramente rispecchia la realtà effettiva dei pericoli. Nove su dieci utilizzatori di PC credono che un infezione malware venga notata dall'utente. Secondo gli intervistati, tale infezione si manifesta sotto forma di strani pop-up, un rallentamento del computer o il non funzionamento dello stesso. La maggior parte degli intervistati è convinta che si presenti almeno uno di questi sintomi.

I criminali della rete hanno però come obiettivo principale quello di ottenere il massimo profitto economico, dunque l'utente non deve accorgersi di nulla il più a lungo possibile. Di norma, già alla prima infezione vengono rubati dati quali informazioni sulle carte di credito, dati bancari, dati di accesso ai negozi online, account di posta elettronica ecc. Infine, il computer viene di solito inserito nelle reti di bot per affittarlo a insaputa dell'utente nei forum underground, dove potrà essere utilizzato per la distribuzione di spam o per attacchi DDoS.

Per propagare i codici dannosi, i criminali sono presenti ormai da tempo nei social network in cui pubblicano link a pagine Web appositamente predisposte. Anche la diffusione di messaggi spam e di allegati infetti continua a costituire una minaccia, malgrado la maggior parte degli intervistati ritenga il problema ormai superato. Nel progetto di diffusione dei virus, lo spam viene utilizzato per attirare i destinatari su siti Web zeppi di codici dannosi, per poi infettare i PC tramite Drive-by Download (vedere il paragrafo 3.2.1: Undici miti della sicurezza IT e gli errori degli utenti di Internet).

La fiducia che gli utenti ripongono nei social network è immensa. Il 35 per cento si fida dei link, se questi sono pubblicati all'interno della propria rete; un buon 19 per cento seleziona i link indipendentemente dalla loro origine, diventando così facili bersagli dei cybercriminali e dei loro traffici illegali.

Ma come si difendono gli utenti dagli attacchi? La buona notizia: solamente l'undici per cento di tutti gli utenti di Internet naviga senza protezione, affidandosi completamente a soluzioni antivirus o a pacchetti di sicurezza Internet funzionali. Il 48 per cento degli intervistati utilizza dei programmi di sicurezza antivirus gratuiti, rinunciando così all'installazione di un firewall separato, alla protezione http, alla Cloud Security, ai moduli antispyware o antispam. Oltre il 50 per cento di questi utenti crede di aver installato un pacchetto di programmi completo, che include queste indispensabili tecnologie di protezione (vedere il paragrafo 3.1: Ma come si difendono gli utenti dagli attacchi?).

In breve: lo studio sulla sicurezza 2011 di G Data mostra che gli utenti valutano in modo errato i pericoli reali di Internet e che una grossa percentuale di utenti privati non provvede in modo adeguato alla sicurezza del proprio computer. Le conseguenze sono tangibili: troppe persone corrono il rischio che i propri computer vengano involontariamente infettati dal malware. Questo tipo di ignoranza facilita i criminali della rete e gli autori di malware.

2 Metodologia dello studio

Lo studio sulla sicurezza 2011 di G Data "Come vengono valutati i pericoli di Internet dagli utenti?" si basa su un'indagine online internazionale a cui hanno partecipato 15.559 utenti di Internet di 11 paesi, con un'età compresa tra i 18 e i 65 anni. Gli intervistati hanno risposto a domande sul tema dei pericoli virtuali in Internet, sul comportamento durante la navigazione, sull'impiego di soluzioni di sicurezza e sulle loro conoscenze in materia di protezione su Internet. Per ciascun paese è stata approntata una pagina Internet nella lingua locale con un catalogo di domande identiche. Gli intervistati erano tutti provvisti di PC proprio con accesso a Internet. I dati sono stati raccolti nei mesi di febbraio e marzo 2011 da Survey Sampling International¹ per conto di G Data Software AG. La valutazione e l'analisi dei dati sono state eseguite tra aprile e maggio 2011.

Tabella 1: Età e sesso degli intervistati

Età	Uomini	Donne	Totale
18-24	1273	1430	2703
25-34	1636	1796	3432
35-44	1603	1784	3387
45-54	1585	1647	3232
55-64	1381	1424	2805
Totale	1478	8081	15559

¹ Ulteriori informazioni su Survey Sampling International sono disponibili in allegato.

Tabella 2: Intervistati per paese

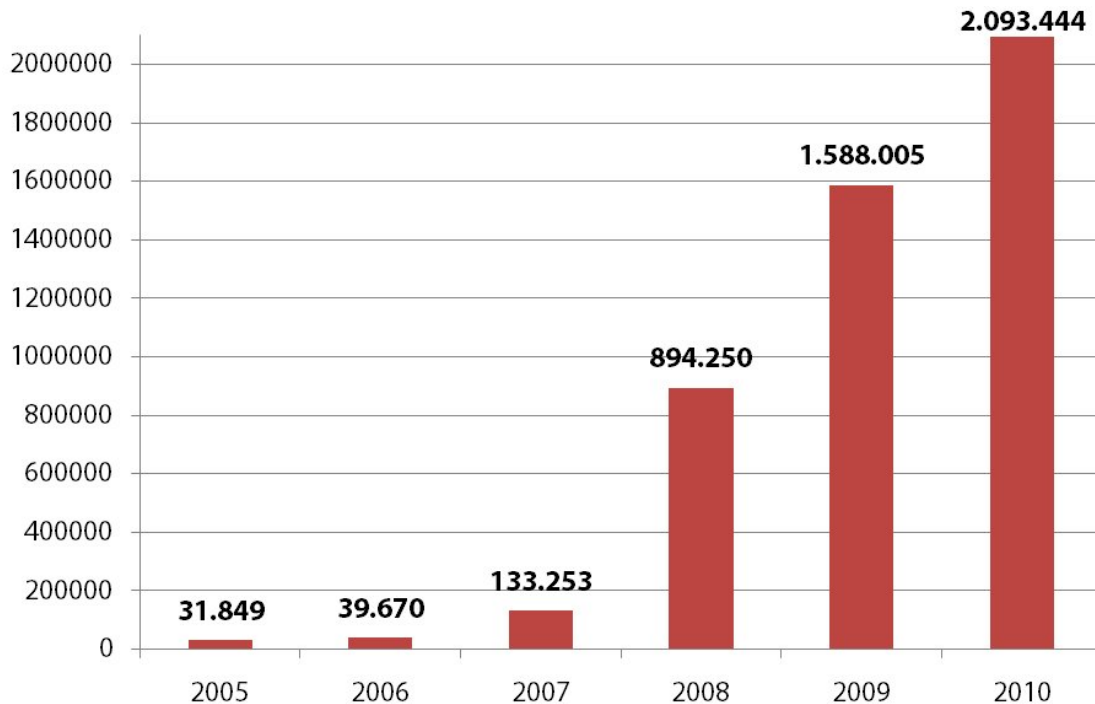
Nazioni	Uomini	Donne	Totale
Belgio	432	496	928
Germania	591	603	1194
Francia	582	622	1204
Italia	575	563	1138
Paesi Bassi	336	367	703
Austria	343	425	768
Russia	503	582	1085
Spagna	579	579	1158
Gran Bretagna	545	561	1106
USA	2646	2958	5604
Svizzera	346	333	679
Totale	7478	8081	15559

3 Risultati dello studio sulla sicurezza 2011 di G Data

Negli ultimi anni, gli attacchi ad aziende e privati sono notevolmente incrementati. La criminalità online è da tempo diventata un commercio molto redditizio: gli autori utilizzano diversi metodi per i loro attacchi, in modo da infettare i computer con i loro virus e rubare così alle vittime tutti i dati possibili, per rivenderli poi con lauti guadagni.

Solo l'anno scorso, G Data ha registrato oltre due milioni di nuovi malware per i sistemi Windows.²

Grafico 1: Numero di nuovi malware all'anno dal 2005



Il codice dannoso viene diffuso dai criminali con modi diversi: il primo prevede la memorizzazione dei programmi dannosi nelle pagine Internet. Anche la semplice visita della pagina Web è sufficiente ad infettare il computer con virus, trojan, spyware e altri malware, tramite i cosiddetti Drive-by Download. L'utente giunge su queste insidiose pagine Internet tramite la semplice navigazione oppure selezionando URL pubblicati dagli autori nei social network o come messaggi nei programmi di messaggistica. I criminali online utilizzano comunque anche i link dei messaggi spam, per attirare gli utenti su pagine appositamente predisposte o per indurli ad aprire allegati di file infetti. In questo caso, l'oggetto del messaggio cita una presunta fattura, un sollecito o fa riferimento alle foto di un evento recente. Se gli utenti rispondono alla sollecitazione, finiscono direttamente nelle pagine con il codice nocivo e vengono infettati a loro insaputa con il virus.

Gli utenti possono proteggersi da questi pericoli solo con delle soluzioni di sicurezza complete e adottando una navigazione su Internet prudente e responsabile.

² Cfr. G Data Malware Report 2/2010, <http://www.gdatasoftware.com/information/security-labs/information/whitepaper.html>

3.1 Ma come si difendono gli utenti dagli attacchi?

Il risultato dello studio sulla sicurezza 2011 di G Data mostra che più del 89 percento dei 15.500 utenti interpellati ha installato un software di sicurezza nel proprio sistema, di cui il 48 percento si affida a programmi gratuiti.

Grafico 2: Quali soluzioni di sicurezza hanno installato gli utenti nei propri sistemi?

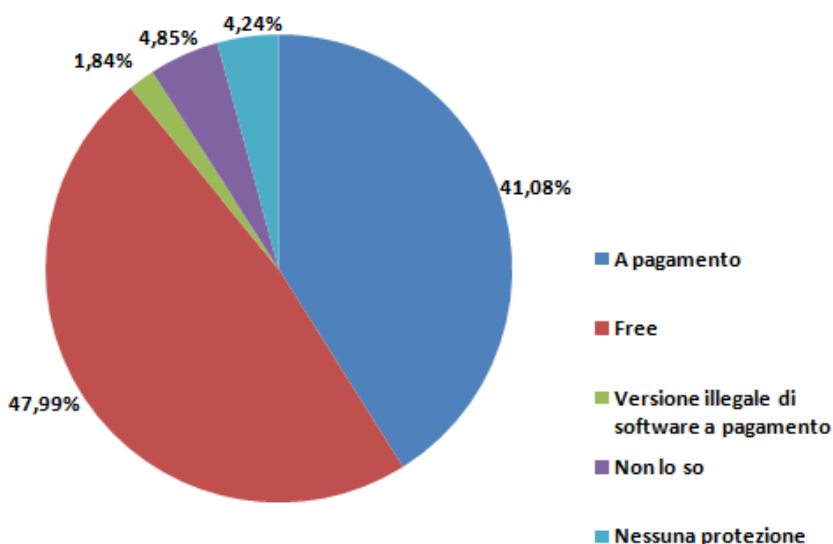
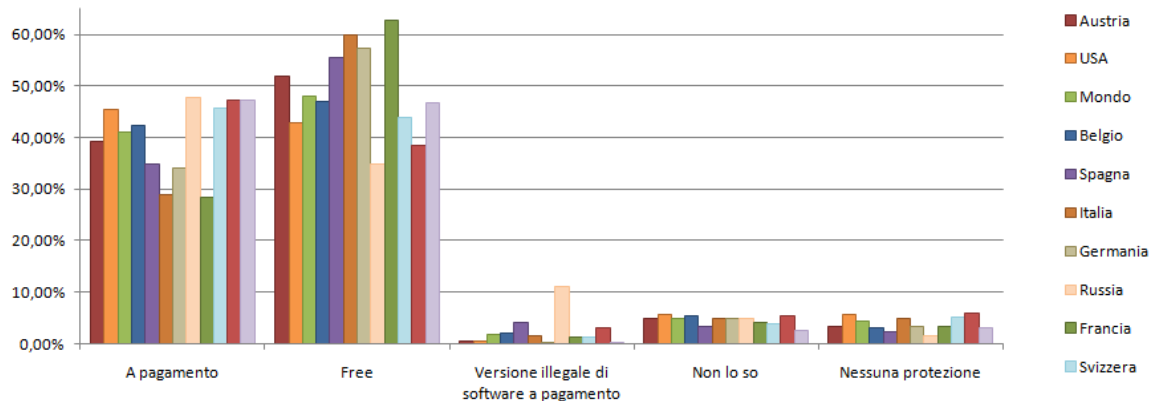


Tabella 3: Risultati alla domanda sulla soluzione di protezione installata dagli utenti

Che soluzione per la sicurezza utilizzi?					
	A pagamento	Free	Versione illegale di software a pagamento	Non lo so	Nessuna protezione
Uomini (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Uomini (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Uomini (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Uomini (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Uomini (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
Totale Uomini	42,55%	47,53%	2,01%	3,40%	4,52%
Donne (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Donne (25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Donne (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Donne (45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Donne (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
Totale Donne	39,71%	48,41%	1,70%	6,20%	3,98%
Totale	41,08%	47,99%	1,84%	4,85%	4,24%

Rispetto al risultato generale dello studio sulla sicurezza, il Regno Unito supera di gran lunga la media: più del 94 percento degli intervistati utilizza soluzioni di sicurezza. La quota più bassa è detenuta dalla Russia, con quasi l'83 percento. Dunque, almeno quattro quinti degli intervistati dei singoli paesi utilizza un software di sicurezza.

Grafico 3: Quali soluzioni di protezione hanno installato gli utenti dei singoli paesi nei propri sistemi?

Tabella 4: Risultati dettagliati dei singoli paesi: Quale soluzione di sicurezza è stata installata dagli utenti?

Che soluzione per la sicurezza utilizzi?					
	A pagamento	Free	Versione illegale di software a pagamento	Non lo so	Nessuna protezione
Mondo	41,08%	47,99%	1,84%	4,85%	4,24%
Austria	39,19%	51,95%	0,52%	4,95%	3,39%
Belgio	42,24%	47,09%	2,16%	5,39%	3,13%
Francia	28,41%	62,79%	1,16%	4,24%	3,41%
Germania	34,09%	57,37%	0,34%	4,77%	3,43%
Gran Bretagna	47,29%	46,84%	0,27%	2,53%	3,07%
Italia	28,82%	60,01%	1,40%	4,92%	4,83%
Paesi Bassi	47,23%	38,55%	2,99%	5,41%	5,83%
Russia	47,83%	34,84%	10,97%	4,79%	1,57%
Spagna	34,96%	55,57%	4,00%	3,22%	2,26%
Svizzera	45,76%	43,80%	1,26%	3,92%	5,26%
USA	45,40%	42,74%	0,55%	5,71%	5,60%

Gli utenti possono abbinare i software antivirus gratuiti con altri strumenti gratuiti. Tuttavia, può risultare problematica una possibile incompatibilità dei singoli programmi con la soluzione di sicurezza in uso.

Per una sicurezza effettiva del proprio computer, oltre all'antivirus sono necessari un firewall personale, un filtro anti-spam ed infine una protezione Web adeguata. A questo scopo, G Data offre G Data Cloud Security, plug-in del browser gratuito e compatibile con tutte le soluzioni antivirus.³

3.1.1 Come valutano gli utenti le prestazioni delle soluzioni antivirus gratuite?

Come detto in precedenza, sul PC vi sono diversi punti di accesso per le infezioni. Le soluzioni di sicurezza moderne dovrebbero essere in grado di fornire protezione da questi pericoli. Ad ogni modo, i programmi antivirus gratuiti non sono in grado di fornire da soli questa protezione, poiché non sono dotati delle tecnologie di sicurezza indispensabili per una protezione completa. Rientrano in questa categoria gli antispam, i filtri Web, i firewall, il riconoscimento dei codici dannosi in base al comportamento e il Cloud Security.

³ Ulteriori informazioni sulla protezione Web gratuita sono disponibili all'indirizzo <http://www.free-cloudsecurity.com>

In questo contesto, è stato chiesto agli utenti di valutare la funzionalità e la qualità dei programmi di sicurezza gratuiti. Quasi il 44 per cento degli intervistati valuta la funzionalità e la qualità dei software di sicurezza gratuiti alla stregua delle soluzioni a pagamento.

Grafico 4: Valutazione dell'efficienza: la qualità dei software di sicurezza gratuiti è la stessa di quelli a pagamento?

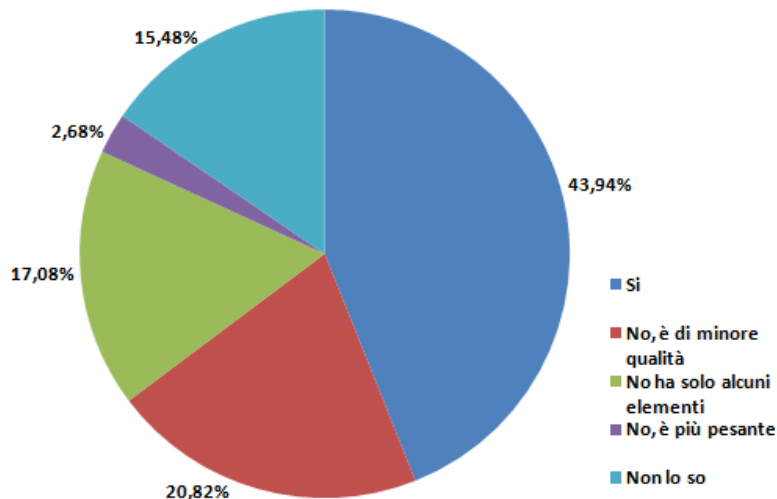
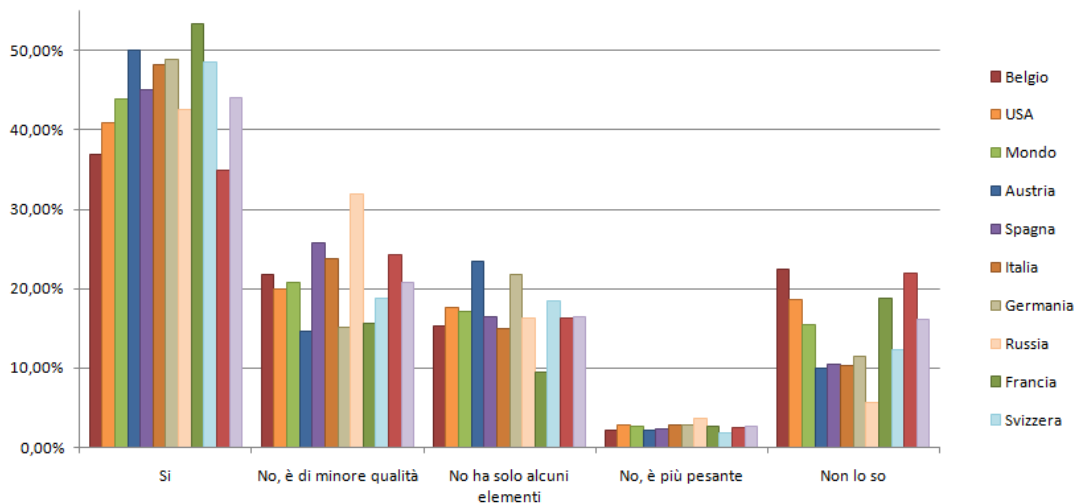


Tabella 5: Risultati dell'indagine in dettaglio: gli utenti ritengono che le soluzioni di sicurezza a pagamento siano uguali da un punto di vista della qualità e della portata di quelle a pagamento?

Un software gratuito è valido tanto quanto un software a paga uominito?					
	Si	No, è di minore qualità	No ha solo alcuni elementi	No, è più pesante	Non lo so
Uomini (18-24)	42,42%	25,69%	17,67%	2,83%	11,39%
Uomini (25-34)	46,03%	23,96%	17,30%	3,30%	9,41%
Uomini (35-44)	45,60%	22,46%	17,90%	2,87%	11,17%
Uomini (45-54)	42,84%	22,02%	19,05%	2,52%	13,56%
Uomini (55-64)	42,87%	20,71%	19,48%	2,32%	14,63%
Totale Uomini	44,06%	22,92%	18,27%	2,78%	11,97%
Donne (18-24)	43,64%	22,10%	17,97%	2,45%	13,85%
Donne (25-34)	44,82%	21,27%	16,31%	3,29%	14,31%
Donne (35-44)	43,39%	20,74%	15,92%	2,30%	17,66%
Donne (45-54)	43,47%	16,03%	15,48%	2,19%	22,83%
Donne (55-64)	43,75%	13,55%	14,26%	2,67%	25,77%
Totale Donne	43,83%	18,87%	15,99%	2,59%	18,72%
Totale	43,94%	20,82%	17,08%	2,68%	15,48%

In questo caso, il leader nel confronto tra paesi è la Francia: per il 53 per cento degli interpellati francesi non esiste alcuna differenza tra le soluzioni di sicurezza gratuite e quelle a pagamento. Al contrario, gli intervistati dei Paesi Bassi hanno ottenuto il valore più basso, ovvero solo il 35 per cento ritiene che i software di sicurezza gratuiti e a pagamento si equivalgano.

Gráfico 5: Valutazione dell'efficienza delle soluzioni di sicurezza gratuite nei diversi Paesi

Tabella 6: Risultati nei singoli paesi: secondo gli intervistati il valore del software di sicurezza gratuito è il medesimo di quello a pagamento?

Un software gratuito è valido tanto quanto un software a pagamento?					
	Si	No, è di minore qualità	No ha solo alcuni elementi	No, è più pesante	Non lo so
Mondo	43,94%	20,82%	17,08%	2,68%	15,48%
Austria	50,00%	14,58%	23,44%	2,08%	9,90%
Belgio	36,85%	21,77%	15,30%	2,16%	22,41%
Francia	53,32%	15,70%	9,47%	2,66%	18,85%
Germania	48,91%	15,08%	21,78%	2,85%	11,39%
Gran Bretagna	44,03%	20,71%	16,46%	2,62%	16,18%
Italia	48,15%	23,72%	14,94%	2,81%	10,37%
Paesi Bassi	34,99%	24,32%	16,22%	2,56%	21,91%
Russia	42,58%	31,89%	16,22%	3,69%	5,62%
Spagna	45,04%	25,74%	16,52%	2,26%	10,43%
Svizzera	48,60%	18,85%	18,41%	1,77%	12,37%
USA	40,94%	19,91%	17,68%	2,82%	18,65%

3.1.2 Numero di PC non protetti

Esiste una consapevolezza generalizzata tra gli utenti della necessità di munire i propri personal computer di software per la sicurezza. Tra i partecipanti all'indagine, la percentuale di PC non protetti è piuttosto bassa: solo il 4 per cento, ovvero 659 utenti, e questo è il dato positivo. Un ulteriore 5 per cento degli utenti non era in grado di dire se nel proprio sistema era stata installata una soluzione di sicurezza. L'1,84 per cento degli intervistati dichiara inoltre di essere disposto ad installare delle copie pirata. Si può dunque ritenere che all'incirca il 6 per cento di tutti gli intervistati naviga su Internet senza alcuna protezione. Sembra che gli intervistati incerti sulla presenza o meno di soluzioni per la sicurezza, in realtà non siano protetti.

Gli utenti russi hanno conoscenze limitate in materia di sicurezza

Rispetto agli altri paesi, la Russia risulta essere quello con il maggior numero di computer non protetti. Inoltre, in questo paese viene installato il numero più alto di versioni illegali di soluzioni di sicurezza a pagamento. Tale quota raggiunge l'11 per cento. Nel complesso, il 17 per cento di PC russi

non è sufficientemente protetto dai pericoli insidiosi di Internet. Il leader positivo di questa categoria è invece il Regno Unito: qui solo il 6 per cento degli intervistati rilascia affermazioni che lasciano dedurre l'assenza di protezione nel PC.

3.1.3 Suite o semplice antivirus?

Grafico 6: Quale soluzione di sicurezza è stata installata dagli utenti?

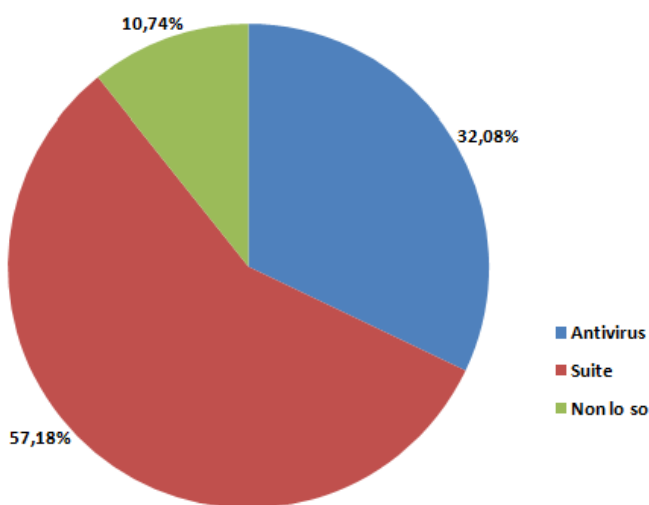


Tabella 7. Risultati dettagliati dell'indagine sulle soluzioni di sicurezza

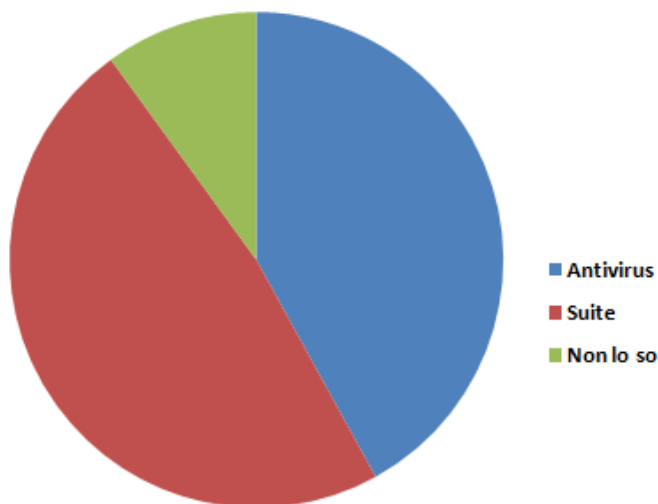
Che tipo di protezione?			
	Antivirus	Suite	Non lo so
Uomini (18-24)	37,00%	55,29%	7,71%
Uomini (25-34)	35,52%	59,52%	4,95%
Uomini (35-44)	32,46%	60,69%	6,84%
Uomini (45-54)	29,55%	63,54%	6,91%
Uomini (55-64)	29,67%	62,93%	7,40%
Totale Uomini	32,73%	60,57%	6,69%
Donne (18-24)	36,03%	52,34%	11,64%
Donne (25-34)	33,86%	53,39%	12,75%
Donne (35-44)	29,92%	56,13%	13,95%
Donne (45-54)	28,71%	56,29%	15,01%
Donne (55-64)	29,23%	51,36%	19,41%
Totale Donne	31,49%	54,05%	14,46%
Totale	32,08%	57,18%	10,74%

Gli utenti di Internet sono consapevoli della presenza di pericoli su Internet e che è necessario proteggersi. O forse no? Ponendo in relazione i risultati alla domanda posta in precedenza (vedere grafico 2) "Che tipo di software di sicurezza è stato installato nel proprio computer" si può notare una notevole contraddizione:

Le soluzioni di sicurezza gratuite sono solamente antivirus e prive di altri tipi di tecnologia, quali firewall, antispam o protezione Web. Attualmente, non esistono sul mercato dei pacchetti di sicurezza gratuiti. La maggior parte degli intervistati (cfr. grafico 7), che in precedenza aveva dichiarato di

essere in possesso di una soluzione antivirus gratuita, ha anche affermato di utilizzare una suite di sicurezza Internet con firewall personale, antispam e protezione Web.

Grafico 7: Soluzione di sicurezza installata dagli utenti che hanno dichiarato di utilizzare una soluzione gratuita



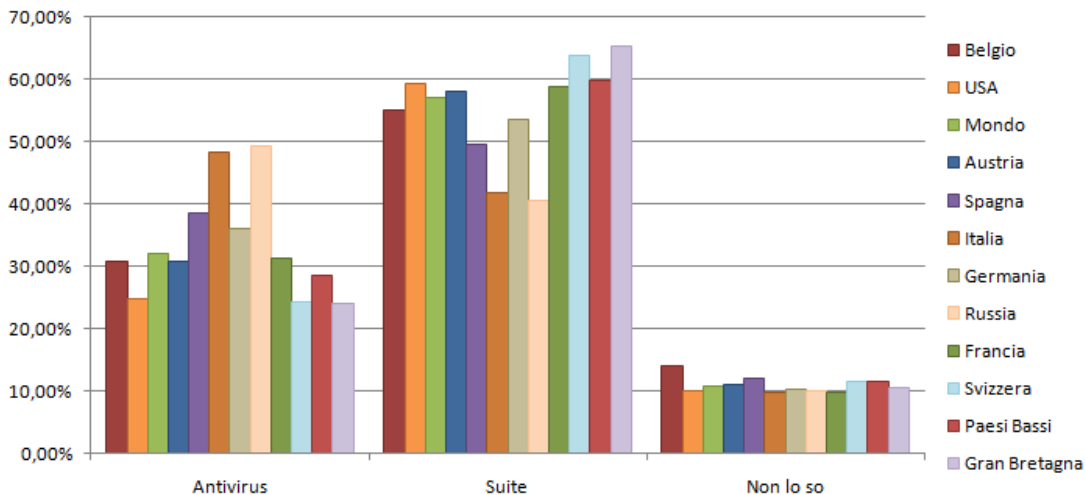
Cosa indica questa apparente contraddizione? La maggior parte degli utenti finali interpellati valuta in modo errato le caratteristiche dei programmi antivirus rispetto alle suite di sicurezza di Internet e sembra non essere sufficientemente informata sulle tecnologia di protezione integrate. Un gran numero di persone giudica dunque l'antivirus e i pacchetti di sicurezza Internet gratuiti come uguali da un punto di vista della qualità, a prescindere dalle differenze di tipo tecnologico. Tale stima errata da parte degli utenti di Internet può costare cara, se si considerano i diversi modi di diffusione dei codici dannosi.

Tabella 8: Soluzioni di sicurezza installate nei singoli paesi

Che tipo di protezione?			
	Antivirus	Suite	Non lo so
Mondo	32,08%	57,18%	10,74%
Austria	30,86%	58,09%	11,05%
Belgio	30,70%	55,17%	14,13%
Francia	31,30%	58,90%	9,80%
Germania	36,17%	53,51%	10,32%
Gran Bretagna	24,04%	65,33%	10,63%
Italia	48,30%	41,92%	9,78%
Paesi Bassi	28,55%	59,82%	11,63%
Russia	49,44%	40,45%	10,11%
Spagna	38,52%	49,47%	12,01%
Svizzera	24,42%	63,92%	11,66%
USA	24,93%	59,35%	10,12%

Tuttavia, nei singoli paesi, la quota di utenti in possesso di un pacchetto di sicurezza supera quella di coloro che utilizzano l'antivirus. L'Italia e la Russia costituiscono un'eccezione. In questo caso il rapporto è invertito (cfr. tabella 8).

Grafico 8: Soluzioni di sicurezza installate: confronto tra paesi

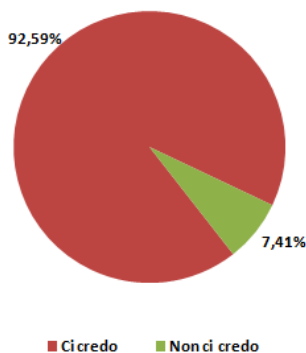


3.2 Quali sono i luoghi dove i navigatori di Internet si aspettano di trovare i maggiori pericoli?

Per ottenere una panoramica di ciò che temono gli utenti della criminalità online, G Data ha posto agli intervistati undici affermazioni errate. Come ci si poteva immaginare, alcuni degli utenti interpellati hanno ritenuto corrette tutte queste affermazioni errate. Per questa ragione, definiamo tali affermazioni le undici tesi della sicurezza di Internet.

3.2.1 Le undici tesi della sicurezza di Internet

Tesi 1: Sarà chiaro se il mio PC è infetto (93 percento).



Solo meno del 7,5 percento è dell'avviso che in caso di infezione non si percepisca niente di strano, anche se è appunto ciò che avviene nella maggioranza dei casi (cfr. tabella 9).

La prima tesi è di gran lunga la più diffusa. Quasi tutti gli utenti di Internet (93 percento) del mondo sono convinti che tutti i programmi dannosi si rendano in qualche modo visibili nel PC. Allo stesso tempo, il 45 percento degli intervistati ritiene che il computer smetta di funzionare non appena viene infettato dal malware. Quasi il 57 percento è dell'opinione che almeno alcune funzioni subiscano dei disturbi o che determinati prodotti software non funzionino più. Il 58 percento è convinto che il computer, una volta infetto, visualizzi diversi pop-up e che emetta strani rumori. Infine, quasi il 57 percento sostiene che il computer diventi molto lento. Solo meno del 7,5 percento è dell'avviso che in caso di infezione non si percepisca niente di strano, anche se è appunto ciò che avviene nella maggioranza dei casi (cfr. tabella 9).

Tabella 9: Secondo gli intervistati, cosa succede quando il computer è infetto? – Gli intervistati potevano scegliere tra diverse risposte.

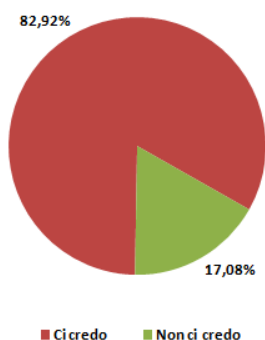
Cosa accade quando il Pc è infetto?					
	Il PC va in crash	Alcune cose smettono di funzionare	Ci sono strani pop up e suoni	Il PC rallenta	Niente di speciale
Uomini (18-24)	43,52%	52,24%	56,64%	58,84%	10,45%
Uomini (25-34)	43,52%	57,46%	58,31%	59,96%	8,37%
Uomini (35-44)	46,35%	56,33%	58,58%	57,70%	7,99%
Uomini (45-54)	41,83%	54,57%	58,36%	57,03%	8,83%
Uomini (55-64)	37,44%	57,42%	54,89%	55,10%	7,10%
Totale Uomini	42,65%	55,71%	57,46%	57,77%	8,50%
Donne (18-24)	48,46%	58,18%	64,06%	62,52%	6,43%
Donne (25-34)	50,17%	59,30%	64,37%	58,13%	5,57%
Donne (35-44)	47,48%	57,51%	57,12%	55,27%	7,29%
Donne (45-54)	46,81%	57,86%	56,22%	53,25%	5,65%
Donne (55-64)	46,00%	57,23%	50,56%	48,17%	7,16%
Totale Donne	47,85%	58,05%	58,62%	55,53%	6,40%
Totale	45,35%	56,93%	58,06%	56,60%	7,41%

In passato, i virus venivano scritti da sviluppatori che volevano dimostrare le loro capacità tecniche. Se l'infezione aveva successo, la vittima se ne accorgeva poiché apparivano dei pop-up, diminuiva la funzionalità oppure il PC cessava di funzionare. A quanto pare, molte persone lo ricordano ancora molto bene. Ma adesso i codici dannosi vengono programmati da criminali molto esperti, con lo scopo di guadagnare quanto più denaro possibile. Un malware ben programmato può valere molto sul mercato nero online. Il codice del programma viene acquistato dai criminali che lo utilizzano, ad esempio, con lo scopo di ingrandire la rete di bot per raggiungere i PC infetti a livello mondiale con la massima potenza di calcolo possibile. Queste cosiddette reti di bot possono ad esempio essere utilizzate per il lancio di attacchi DDoS, per l'invio dello spam o la diffusione dei virus. Tale tipo di economia sommersa è ampiamente sviluppata: gli sviluppatori e gli amministratori delle reti di bot offrono le loro conoscenze e servizi come prestazioni speciali nei forum underground specializzati. Altri criminali acquistano prestazioni o codici dannosi in queste piattaforme, come ad esempio l'attacco ad un sito Web di una determinata azienda o l'avvio di un'azione di spam di massa. Per eseguire queste operazioni, non è necessario disporre di una conoscenza tecnica.⁴

Pertanto, gli sviluppatori e gli amministratori delle reti di bot si impegnano a rendere la rete di bot il più estesa e stabile possibile. Ciò significa che ogni PC scollegato, ad es. quando viene scoperta ed eliminata l'infezione presente, costituisce per i cybercriminali una perdita economica. I programmi dannosi sono dunque costruiti dagli autori di malware in modo tale che l'infezione non sia individuata. Per questo è piuttosto improbabile che al giorno d'oggi un'infezione del PC si manifesti con il crash del computer, funzionalità limitate, finestre di pop-up sospette o altri sintomi. Questo sviluppo è piuttosto pericoloso per gli utenti di PC poiché solo le infezioni che si manifestano velocemente possono essere anche rapidamente eliminate. Non è certo d'aiuto il fatto che ancora nove su dieci utenti ritengano che il malware sia facilmente individuabile. Questi utenti deducono dunque che se il computer non presenta problemi di performance non è di certo infetto. Tale tesi fa dunque il gioco dei cybercriminali.

⁴ Per ulteriori informazioni sull'economia sommersa, consultare il G Data Whitepaper Underground Economy all'indirizzo: <http://www.gdatasoftware.co.uk/security-labs/information/whitepaper.html>

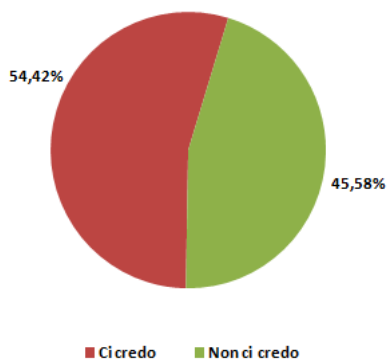
Tesi 2: I software antivirus gratuiti offrono la stessa sicurezza di quelli a pagamento (83 per cento).



Questa affermazione viene confermata dall'83 per cento, ovvero dalla maggioranza degli intervistati. Sebbene la maggior parte di coloro che hanno partecipato all'indagine, il 56 per cento degli intervistati, alla domanda sulle differenze di qualità tra le soluzioni di protezione a pagamento e quelle gratuite (cfr. tabella 6) dubiti che si possano effettuare paragoni nella qualità dei due tipi di software di protezione, gli stessi non sono poi però in grado di descrivere queste differenze in dettaglio. Il 15 per cento degli intervistati ha ammesso di non avere alcuna idea della differenza di funzionalità tra i due tipi di prodotto, gratuito e a pagamento. Quasi il 3 per cento ha risposto che la differenza fosse nell'impiego delle risorse del sistema: i prodotti gra-

tuiti risultano più pesanti rispetto alle soluzioni commerciali. La differenza principale tra le offerte gratuite e quelle a pagamento è invece costituita dalla tecnologia di sicurezza offerta. Il software di protezione gratuito fornisce solamente una protezione antivirus, mentre quello a pagamento comprende diversi elementi di sicurezza. Oltre alla protezione antivirus, queste soluzioni di norma comprendono un filtro http, un firewall, un modulo antispam ed un riconoscimento dei codici dannosi basato sul comportamento. Solo il 17 per cento degli intervistati ha risposto correttamente a questa domanda.

Tesi 3: La maggior parte del malware è diffusa via email (54 per cento).

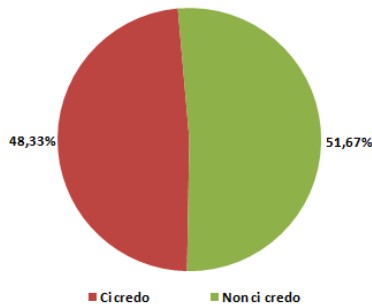


Questa affermazione, come la precedente, è ormai obsoleta, ma il 54 per cento degli utenti è ancora convinto della sua correttezza. Tra tutti i messaggi di posta degli ultimi anni dello scorso millennio, i messaggi "Melissa" e "I love you" sono stati senza dubbio lo strumento di maggior diffusione del malware. Le infezioni si trasmettono tramite allegati, che vengono resi accattivanti grazie al Social Engineering. Molti si ricorderanno ancora dei messaggi che promettevano le foto nude della tennista russa Anna Kurnikova. All'apertura di tale allegato, il PC veniva però infettato da un virus. Da circa sei anni, gli allegati ai messaggi sono stati superati di numero dai link a file che rimandano a siti Web (anche se negli ultimi mesi gli allegati stanno riprendendo piede).

Questa tattica permette agli autori di aggirare gli efficienti filtri antispam e di recapitare il messaggio agli ignari utenti. Allo stesso tempo però molti sono diventati prudenti con i messaggi provenienti da mittenti sconosciuti e li cancellano immediatamente, senza nemmeno aprirli. Nella maggioranza dei casi, i link all'interno dei messaggi rimandano a siti Web dannosi. Esistono comunque anche altre possibilità di trovare vittime: ad esempio nei social network (cfr. paragrafo 3.3), tramite l'ottimizzazione delle richieste di ricerca, i domini risultanti da errori di battitura ecc. I programmi nocivi si sono spostati nei siti Web, questi ultimi sono divenuti il principale vettore di infezione.

Tesi 4: Non puoi essere infettato soltanto visitando un sito infetto (48 per cento).

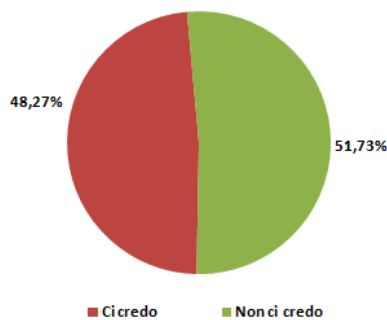
È scioccante sentire che quasi la metà degli utenti di Internet ritiene questa affermazione corretta. Tramite Drive-by Download, da anni ormai è possibile infettare il proprio computer con codici nocivi. Per questo tipo di infezione è veramente sufficiente la visita di un determinato sito Internet. La supposizione che il caricamento della pagina non sia sufficiente è una pericolosa falsa conclusione, poiché questo tipo di attacco viene praticato quotidianamente in modo diffuso.



Esistono due varianti di infezioni Drive-by: da un lato esistono i siti Web sviluppati con il fine di infettare i PC. Mediante la pubblicazione di link interessanti nei social network, oppure utilizzando banner o messaggi in cui è incluso il link, i cybercriminali tentano di attirare la vittima nel sito Web infetto.

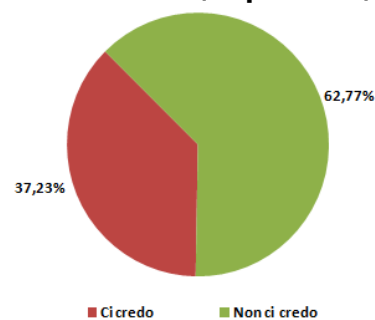
L'altra variante è più raffinata: il codice dannoso viene infiltrato in una pagina Internet fidata e considerata tra le preferite. Così, ad esempio si apre una finestra di 0x0 pixel, invisibile all'utente. Tale finestra avvia però un download nel PC del visitatore, infettandolo di nascosto con programmi nocivi. Il vantaggio principale di questo secondo metodo è che così i cybercriminali non sono tenuti a fare alcuna pubblicità al sito Web. Gli autori però devono essere in grado di accedere a tale sito per poterlo manipolare. Se è ben protetto, cosa molto rara tra le pagine Web su Internet, il lavoro diventa molto difficile.

Tesi 5: La maggior parte del malware è diffusa attraverso il download tramite siti di peer2peer e torrent (48 per cento).



È innegabile che tramite le piattaforme di scambio, come le pagine Web Torrent e le reti di scambio Peer-2-Peer si diffondono i programmi dannosi e di conseguenza non c'è da stupirsi che il 48 per cento degli intervistati ritenga che questo sia il metodo più importante di diffusione del malware. Probabilmente, un utente ha già infettato il proprio sistema con codici dannosi visitando tali pagine ma questa tesi rimane comunque errata e dunque un mito, poiché la maggior parte dei programmi dannosi si diffonde (come già illustrato) tramite pagine Web dannose.

Tesi 6: Il mio PC è più probabile che trovi malware su un sito pornografico che su un sito di corse di cavalli (37 per cento).



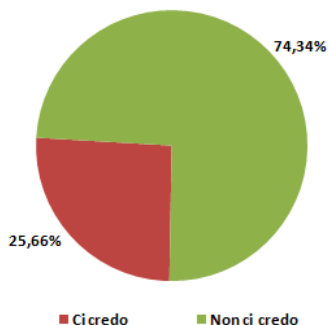
La pornografia ha una dubbia reputazione. Nemmeno in questo caso dunque c'è da stupirsi che molte persone (37 per cento) sospettino la presenza di un legame con la criminalità online. C'è da domandarsi però se effettivamente le pagine porno siano più frequentemente infette di altre pagine Internet, come quelle sull'equitazione o sui temi del tempo libero. Nel settore della pornografia i guadagni sono ingenti. Per i possessori di queste pagine Web, la pagina Internet di per sé costituisce la fonte di introito principale. Per questo vengono normalmente sviluppate, aggiornate e rese

sicure da professionisti. Un cliente pagante, il cui PC viene infettato con malware durante la visita, è un cliente perso, con conseguente danno finanziario. Il gestore di pagine Web relative agli hobby non è probabilmente un Web designer e non si preoccupa di caricare regolarmente gli aggiornamenti del software o le patch che permetterebbero di chiudere le falle di sicurezza. Per i criminali è dunque molto più semplice accedere a questi siti Web e infettarli con codici dannosi piuttosto che ai siti Web pornografici resi sicuri da professionisti. Tali pagine Web sono facilmente individuabili tramite Google: è sufficiente inserire il nome dell'applicazione e conoscerne una falla di sicurezza. In questo modo, è possibile scovare tutti i siti Web che possono facilmente essere manipolati. I siti Web

pornografici costituiscono comunque in generale un rischio maggiore se sono gestiti da fornitori ambigui, nel caso di pagine porno più serie il pericolo potenziale non è così alto.

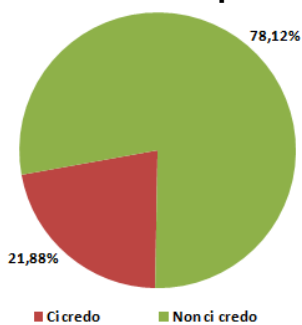
Tesi 7: Un firewall può proteggere il mio PC da attacchi di tipo drive-by (26 per cento).

Questa affermazione è stata confermata da circa il 26 per cento degli interpellati. Anche questa tesi è



falsa. I firewall sono senza dubbio un componente importante del piano di sicurezza di un computer, ma non possono proteggere efficacemente il PC dalle infezioni Drive-by. Per una protezione efficace e sufficiente, l'utente di Internet deve munirsi di una soluzione di sicurezza completa con protezione Web integrata. Infatti, in caso di infezione, il firewall non può sempre impedire al programma dannoso di eseguirsi e, come nel caso dei programmi spyware, di inviare i dati sensibili ai criminali.

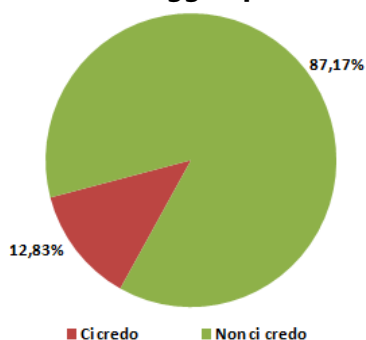
Tesi 8: Se non si apre un file infetto non puoi essere infettato (22°per cento).



Anche questa affermazione, come alcune delle precedenti, si basa su convinzioni derivanti da fatti obsoleti, che si sono tramandati fino ad oggi come leggende e nei quali ancora crede quasi il 22 per cento degli intervistati. Naturalmente, le infezioni avvengono ancora in seguito all'apertura di file pericolosi da parte dell'utente, ma l'esecuzione automatica dei file dannosi può verificarsi solo se le falle di sicurezza esistenti possono essere sfruttate dagli autori dell'attacco. In questo caso, il codice dannoso può attivarsi automaticamente, anche senza che l'utente selezioni il file infetto. Per questo motivo, è preferibile dedurre

che i file infetti siano sempre pericolosi per gli utenti dei PC e che si possono eseguire anche indipendentemente dal comportamento dell'utente.

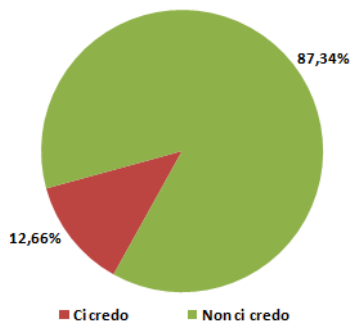
Tesi 9: La maggior parte del malware è diffuso tramite chiavi USB (12,83°per cento).



Nel frattempo, è ormai assodato che i programmi dannosi si diffondono in maggioranza tramite siti Web infetti ma che esistono comunque altri veicoli di infezione. Negli anni ottanta e novanta, durante i quali Internet non era ancora così onnipresente, i dischetti costituivano spesso una fonte di infezione. Negli ultimi anni invece è cresciuta notevolmente tra i cybercriminali la popolarità delle chiavette USB e di altri mezzi di scambio USB. Viene così manipolata la funzione autostart dei supporti di dati, affinché lancino programmi dannosi una volta inseriti nel PC. Ne è un esempio eclatante il worm Conflicker. Per questo, si consiglia vivamente di disattivare la

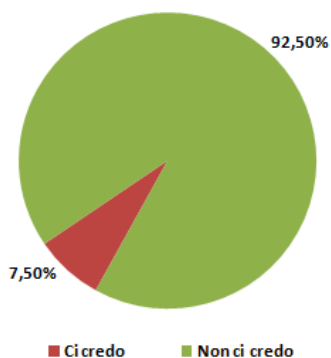
funzione di esecuzione automatica del sistema operativo. Solo così si può evitare che il worm si installi automaticamente all'inserimento della chiavetta USB.

Tesi 10: Non visito siti non sicuri, quindi sono al riparo da drive-by-downloads (3°percento).



Questa affermazione può essere confutata allo stesso modo della sesta tesi (Il mio PC è più portabile che trovi malware su un sito pornografico che su un sito di corse di cavalli). I cybercriminali non badano al tema della pagina Web. Sono unicamente interessati a trovare siti in cui possono infettare il maggior numero di computer possibili con il minimo sforzo. Tale risultato può essere ottenuto con la manipolazione di banner pubblicitari e con l'attacco continuo di grandi domini. Se i criminali riescono nei loro intenti e ottengono l'accesso, vi possono installare codici dannosi anche senza le conoscenze tecniche necessarie, semplicemente utilizzando i cosiddetti Web exploit toolkit. Siti Web che per anni sono risultati estremamente affidabili possono essere improvvisamente attaccati e diventare un potenziale pericolo di infezioni. Questa tesi è stata confermata solo da circa il 13 per cento degli interpellati.

Tesi 11: I cyber criminali non sono interessati ai PC degli utenti privati (8°percento).



Fortunatamente, questa tesi viene sposata dal numero più basso di persone, ovvero solo dall' 8 per cento. Anche questa è un'affermazione errata. È indiscutibile che le reti aziendali destino grande interesse tra i cybercriminali ma in generale, sono anche più difficili da infettare. I computer privati al giorno d'oggi sono piuttosto potenti, dunque sono particolarmente adatti a diventare componenti delle reti di bot. Inoltre, in questi computer sono spesso memorizzati dati personali interessanti che possono essere utilizzati dai cybercriminali, quali dati di accesso di negozi online, di social network, di account di posta elettronica o le informazioni delle carte di credito. Non è dunque da sottovalutare l'interesse che i computer privati possono destare nei criminali online.

3.2.2 Chi è meglio informato: i giovani o gli utenti di Internet più grandi?

Gli utenti di Internet di un'età compresa tra i 18 e i 25 anni sono senz'altro cresciuti con il computer e Internet e questo gruppo è indubbiamente molto attivo in rete. Diversa è invece la situazione degli intervistati più maturi di un'età compresa tra i 55 e i 64 anni. L'indagine è stata condotta esclusivamente online e dunque gli intervistati sono tutti navigatori di Internet. Il mezzo è però relativamente nuovo per gli intervistati più grandi. Si dovrebbe dunque presumere che la generazione più giovane ne sappia di più dei pericoli di Internet della generazione più matura. Ma un'altra ipotesi fa pensare che la generazione più matura, poiché dotata di una confidenza minore con Internet e i computer, fiuti pericoli da tutte le parti e per cui naviga sicuramente con più cautela.

Per scoprire il livello di informazione dei più giovani e dei più anziani intervistati, si è investigato su quanto questi due gruppi credessero alle tesi illustrate. La seguente tabella fornisce una panoramica a riguardo.

Tabella 10: Chi crede maggiormente alle tesi presentate: gli utenti più giovani o più anziani?

Tesi	18-25 anni:	55-64 anni:	Totale risposte
1) Sarà chiaro se il mio PC è infetto	91,68%	92,87%	92,59%
2) I software antivirus gratuiti offrono la stessa sicurezza di quelli a pagamento	82,17%	83,17%	82,92%
3) La maggior parte del malware è diffusa via email	46,54%	61,46%	54,42%
4) Non puoi essere infettato soltanto visitando un sito infetto	53,42%	46,67%	48,33%
5) La maggior parte del malware è diffusa attraverso il download tramite siti di peer2peer e torrent	53,42%	45,67%	48,27%
6) Il mio PC è più probabile che trovi malware su un sito pornografico che su un sito di corse di cavalli	39,18%	35,40%	37,23%
7) Un firewall può proteggere il mio PC da attacchi di tipo drive-by	32,89%	17,47%	25,66%
8) Se non apri un file infetto non puoi essere infettato	22,42%	25,13%	21,88%
9) La maggior parte del malware è diffuso tramite chiavi USB	16,91%	9,02%	12,83%
10) Non visito siti non sicuri, quindi sono al riparo da drive-by-downloads	14,39%	13,69%	12,66%
11) I cyber criminali non sono interessati ai PC degli utenti privati	10,03%	6,77%	7,50%

Se nella tabella si prende in considerazione la colonna dei più giovani, in un primo momento il risultato è positivo. I giovani sono meno convinti della veridicità delle 3 tesi più importanti, ma si distaccano solo in parte dalla media degli intervistati. Per quanto riguarda però la quarta tesi, che costituisce l'errore più pericoloso poiché mette in dubbio l'esistenza e l'efficienza delle infezioni Drive-by, i giovani sono quelli che la accettano in numero maggiore. Ciò vale anche per la quinta tesi sul malware e sulle borse di scambio, come le pagine Torrent e le reti Peer-2-Peer. Probabilmente ciò è dovuto al fatto che i giovani scaricano un numero enorme di file da questi siti Web e sicuramente sono già incappati in file infetti. Rispetto agli altri utenti, gli intervistati più giovani temono inoltre una possibilità maggiore di infezioni nei siti Web pornografici. La generazione più giovane inoltre più disinformata rispetto alle funzioni dei firewall. Questo contraddice l'ipotesi che gli utenti più giovani conoscano a fondo le tecnologie con cui sono cresciuti. I giovani sembrano essere meno consci del fatto che il computer si possa infettare anche senza necessariamente dover aprire il file. Allo stesso tempo, gli intervistati più giovani crede più della media che le chiavette USB siano la fonte più importante di infezioni da malware. Inoltre, questo gruppo sopravvaluta le proprie conoscenze su come evitare i Drive-by Download ed è convinto più degli altri che il proprio computer privato non sia interessante per i cybercriminali.

Tutto sommato, i giovani non ottengono un buon risultato. La loro conoscenza è più limitata della media degli utenti di Internet, sfatando il mito che i giovani conoscano Internet meglio della media della popolazione poiché sono cresciuti con questa tecnologia.

Spostando la nostra attenzione sulla colonna degli intervistati più maturi notiamo chiaramente che questo gruppo crede in numero ancora maggiore rispetto alla media che le tre tesi più importanti siano vere. Per quanto riguarda la quarta, relativa agli attacchi Drive-by Download, lo scenario che ne risulta è diverso. Gli intervistati più vecchi sono meglio informati sulla pericolosità di questi attacchi rispetto ai giovani, soprattutto nel caso degli utenti più giovani in assoluto. Ciò non è comunque di sollievo, visto che anche tra loro, uno su due non crede all'esistenza dei Drive-by Download. Un

numero sopra la media degli intervistati è d'accordo con la tesi che le pagine di file sharing siano la fonte maggiore di infezioni di malware. La differenza rispetto alla media è però esigua. Lo stesso dicesi per le pagine Web di pornografia, che destano meno sfiducia in questo gruppo di persone rispetto alla media. Gli utenti più grandi si fidano notevolmente meno delle funzioni di protezione fornite dai firewall nei confronti dei Drive-by Download di quanto non facciano i giovani e anche rispetto alla media. I più anziani sono però più convinti dell'impossibilità di un'infezione in assenza di apertura di un file, il che contraddice la convinzione palesata in precedenza sul pericolo di infezioni Drive-by. Gli utenti più maturi non ritengono, giustamente, che le chiavette USB siano la fonte principale della diffusione di malware. Meno giustificata è la fiducia superiore alla media sulla sicurezza delle proprie abitudini di navigazione, che dovrebbe proteggere i più anziani dagli attacchi Drive-by Download. In realtà sono solo un po' meno sprovveduti rispetto ai giovani. Riteniamo comunque positivo che, rispetto alla media, i più anziani siano maggiormente consapevoli del fatto che il proprio computer possa essere interessante per i cybercriminali.

In definitiva, anche questa fascia di età non esce vincente da quest'indagine, anche se mostra di avere più coscienza dei pericoli di Internet rispetto ai giovani. L'analisi porta dunque a concludere che le persone della fascia di età compresa tra i 25 e i 54 anni siano le più informate sui pericoli di Internet. È necessario però sottolineare che anche queste persone sono convinte della correttezza di numerose delle tesi elencate su questo argomento e che pertanto anche la loro conoscenza non è sufficiente.

3.2.3 Qual è il paese in cui gli utenti di Internet sono più informati sui pericoli?

Esistono diversi preconcetti su quali siano i paesi in cui gli utenti siano più o meno informati. Molti ritengono infatti che gli americani e gli inglesi siano piuttosto ben informati sui pericoli di Internet e che lo siano meno gli italiani e i russi. Per scoprire se effettivamente esistono dei paesi in cui gli utenti di Internet sono molto o poco informati sui pericoli effettivi di Internet, abbiamo riportato i risultati percentuali degli intervistati che credono a questi miti nella tabella 11. Il verde indica i paesi in cui tale tesi è ritenuta meno valida. Il rosso, al contrario, indica i paesi in cui la tesi è maggiormente accettata.

Tabella 11: In quale paese viene dato più credito a queste tesi?

Tesi	Paesi Bassi	Belgio	Francia	Spagna	USA	Italia	Germania	Russia	Gran Bretagna	Austria	Swizzera	Mondo
1) Infezione apparente	86,63%	93,97%	92,28%	95,30%	94,29%	94,38%	83,17%	97,88%	91,40%	86,46%	90,13%	92,59%
2) Antivirus gratuiti	83,78%	83,19%	90,53%	83,48%	82,32%	85,06%	78,22%	83,78%	83,54%	76,56%	81,59%	82,92%
3) E-mail infette	58,89%	62,18%	57,64%	58,61%	52,37%	58,88%	52,85%	38,80%	52,89%	55,47%	57,73%	54,42%
4) Siti Internet infetti	51,49%	49,03%	49,25%	57,83%	40,95%	63,44%	62,90%	48,48%	42,85%	60,68%	54,93%	48,33%
5) Torrent&peer2peer	43,53%	46,76%	48,17%	52,43%	52,73%	45,52%	35,26%	49,49%	48,73%	41,02%	44,48%	48,27%
6) Siti Porno infetti	25,32%	34,27%	31,89%	32,43%	40,13%	32,25%	30,65%	60,18%	35,80%	34,11%	36,23%	37,23%
7) Firewall	31,44%	28,34%	18,77%	26,78%	24,32%	28,03%	29,31%	17,05%	24,95%	28,26%	29,16%	25,66%
8) File infetti	16,50%	26,29%	23,59%	30,78%	18,18%	30,67%	13,32%	38,53%	20,43%	14,06%	18,56%	21,88%
9) Chiavette USB infette	8,11%	10,67%	17,28%	20,09%	9,92%	15,38%	8,38%	30,05%	10,49%	8,72%	8,98%	12,83%
10) Siti Internet non sicuri	18,07%	13,69%	14,78%	14,00%	10,79%	17,84%	11,81%	11,89%	9,67%	12,50%	14,14%	12,66%
11) Pc Utenti privati	5,12%	6,90%	5,98%	8,87%	7,50%	8,35%	7,20%	6,54%	8,77%	9,90%	6,63%	7,50%

Questa tabella mostra che gli intervistati tedeschi sono spesso i più informati sugli insidiosi pericoli di Internet. La Germania è il paese dove si dà meno adito alle tre tesi più importanti. Lo stesso vale per i Paesi Bassi. Tuttavia, è bene notare che gli olandesi sono due volte più distanti dalla verità nella valutazione delle tesi. È interessante notare che gli americani, dai quali ci si aspettava probabilmente il miglior risultato, hanno ottenuto il numero più basso di sostenitori solo nella quarta tesi. Gli americani intervistati in particolare credono alla tesi secondo cui le borse di scambio siano il mezzo di diffusione più comune dei codici dannosi. Non sono comunque gli americani quelli meno informati sui pericoli di Internet: il fanalino di coda è la Russia. Tra tutte le nazionalità, i russi credono nella maggioranza delle tesi. Il fatto che siano quelli che credono meno a due altri miti, non toglie che siano gli ultimi in classifica.

3.2.4 Sono gli uomini i migliori navigatori?

La convinzione che gli uomini siano tecnicamente più esperti delle donne è profondamente radicata in molte persone (inconsiamente). Se questo fosse vero gli uomini dovrebbero essere anche più informati delle donne su dove si insidiano realmente i pericoli di Internet e quali sono le paure antiquate e irrealistiche. È effettivamente così? La tabella seguente mostra la valutazione di uomini e donne riguardo ai miti di Internet.

Tabella 12: Chi è più propenso a credere alle tesi: uomini o donne?

Tesi	Uomini	Donne	Totale
1) Sarà chiaro se il mio PC è infetto	91,50%	93,60%	92,59%
2) I software antivirus gratuiti offrono la stessa sicurezza di quelli a pagamento	84,01%	81,73%	82,92%
3) La maggior parte del malware è diffusa via email	54,53%	54,31%	54,42%
4) Non puoi essere infettato soltanto visitando un sito infetto	48,19%	48,46%	48,33%
5) La maggior parte del malware è diffusa attraverso il download tramite siti di peer2peer e torrent	49,13%	47,47%	48,27%
6) Il mio PC è più probabile che trovi malware su un sito pornografico che su un sito di corse di cavalli	43,88%	31,07%	37,23%
7) Un firewall può proteggere il mio PC da attacchi di tipo drive-by	26,02%	25,32%	25,66%
8) Se non apri un file infetto non puoi essere infettato	22,65%	21,16%	21,88%
9) La maggior parte del malware è diffuso tramite chiavi USB	13,47%	12,24%	12,83%
10) Non visito siti non sicuri, quindi sono al riparo da drive-by-downloads	11,74%	13,51%	12,66%
11) I cyber criminali non sono interessati ai PC degli utenti privati	8,75%	6,35%	7,50%

La tabella indica che le donne sono molto spesso più vicine alla verità di quanto non lo siano gli uomini. Solo in tre casi di affermazioni sbagliate le donne rispondono più spesso in modo errato. Tuttavia, è dubbio che questo sia sufficiente a concludere che le donne siano degli utenti migliori. Solitamente, i dati di percentuale si differenziano per meno del 2 per cento.

Le differenze più evidenti tra uomini e donne si manifestano nella tesi "Il pericolo di imbattersi in malware è maggiore nei siti porno di quanto non lo sia nella visita a pagine Web sull'equitazione o sui viaggi". Il motivo per cui questa affermazione viene condivisa dagli uomini potrebbe essere lo stesso per cui i giovani intervistati sono quelli che credono in maggior numero all'affermazione: "La maggioranza dei virus e dei malware si diffonde tramite file infetti nelle borse di scambio, come le reti Peer-2-Peer e i siti Web Torrent". Se un gruppo di utenti ha più esperienza di frequentazione di questi siti Web è probabilmente successo più spesso che siano incappati nei malware in detti siti. Ciò non significa però che la credenza sia corretta. Gli uomini intervistati hanno visitato i siti di equitazione con la stessa frequenza? Se anche questo fosse il caso e non fosse mai accaduto che in questi siti siano stati infettati da software dannosi, non potrebbe trattarsi di una semplice coincidenza se in nessuno di questi casi si sia verificata un'infezione Drive-by? Le donne hanno probabilmente meno dimestichezza con i siti Web pornografici ed evidentemente non sono state vittime di attacchi Drive-by Download in questi siti. Da un punto di vista femminile, dunque, un sito Web pornografico può essere altrettanto pericoloso come ogni altro sito Internet. Un'altra spiegazione per questa differenza di valutazione potrebbe essere di carattere psicologico. La pornografia è vista e percepita dalla

maggioranza delle persone come disdicevole e negativa, ovvero come qualcosa da tenere segreto. Quando le persone hanno la sensazione di fare qualcosa di sbagliato mettono in conto la possibilità di ricevere una punizione per il loro comportamento, in questo caso un'infezione malware. È un dato di fatto statistico che gli uomini consumano più pornografia delle donne e che dunque pensino di incappare in codici dannosi nei siti Web porno.

Oltre alla domanda sui siti Web, esiste un'altra credenza per la quale la valutazione degli uomini e delle donne è piuttosto diversa. Gli uomini credono più spesso che il computer privato non sia interessante per i cybercriminali. Le donne sono meno convinte di questo. Ciò può essere dovuto al fatto che le donne sono più prudenti nell'uso del PC in generale perché si sentono meno sicure e dunque che gli uomini sono più pronti al rischio. Forse questa affermazione indica soprattutto una speranza da parte degli uomini.

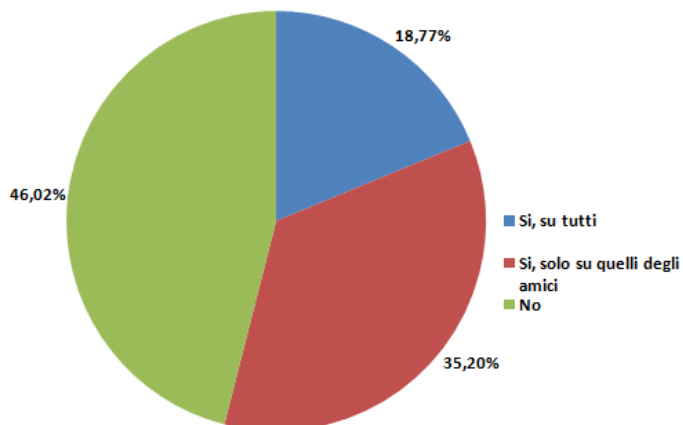
3.3 Comportamento nei social network

La popolarità dei social network è in continua crescita e sono diventati ormai una componente solida dell'infrastruttura di Internet. Gli utenti presentano sé stessi su Facebook, Twitter, etc. dove mantengono una rete di amicizie internazionali, spesso anche ampia. Il successo di questi social network richiama però sempre più anche l'attenzione dei criminali, che tentano di utilizzare i portali di carattere sociale per i loro scopi fraudolenti.

I truffatori hanno diverse possibilità per danneggiare gli utenti: di solito, i dati di accesso alla rete degli utenti possono essere ottenuti tramite il "classico" phishing tramite siti Web falsi, copie molto simili agli originali oppure con il furto delle banche dati di accesso dei fornitori. Una delle ultime invenzioni dei criminali sulle piattaforme sociali è la diffusione degli indirizzi Internet pericolosi sulle bacheche, nei messaggi di chat o nei messaggi personali. Viene ad esempio promesso il link ad un video.

Gli indirizzi Web pubblicizzati sono spesso abbreviati in modo così sostanziale, grazie ad un servizio di abbreviazione URL, che l'utente non ha sentore alcuno del rischio che corre. Facendo clic su questi link l'utente viene dirottato su pagine Internet esterne, infettate da codici dannosi, che rubano i dati tramite phishing o che utilizzano il Clickjacking per trasformare la vittima in spammer sui social network. In questo modo, l'utente diffonde il link alla sua rete di amici, a sua insaputa e senza che il link sia visibile a lui. In caso di link inviati da sconosciuti è necessario essere estremamente prudenti, ma anche gli amici possono diffondere questi tipi di indirizzi Internet, per es. se l'account dell'utente viene violato ed utilizzato dal criminale. Poiché il pericolo potenziale è molto elevato, lo studio sulla sicurezza G Data 2011 conteneva la domanda se gli utenti fanno clic sui link presenti nei social network.

Grafico 9: Comportamento rispetto ai clic negli URL dei siti Web nei social network

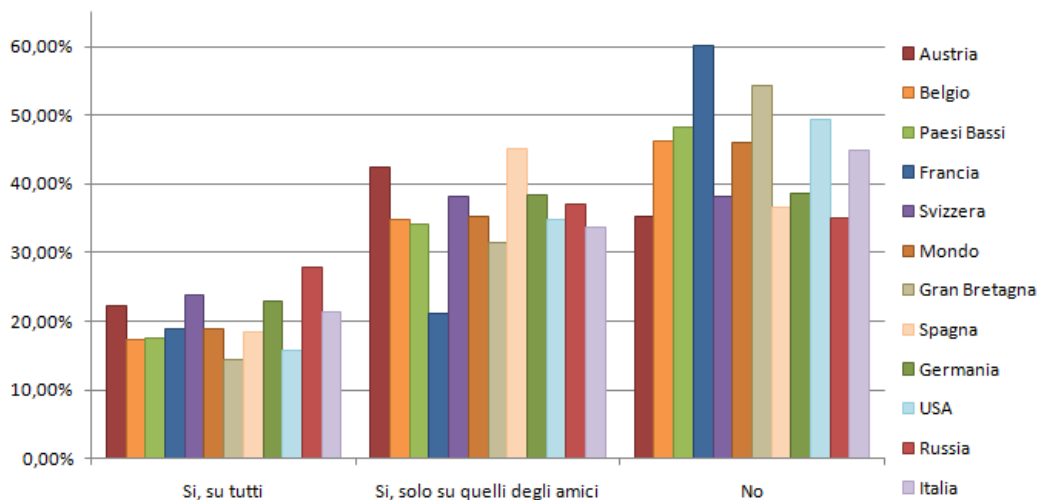


La maggioranza dei partecipanti all'indagine usa i link offerti nei social network. Il 46 per cento degli intervistati non esegue clic su URL di siti Web, sia che siano di amici o di sconosciuti. Più di un terzo si fida degli indirizzi Internet pubblicizzati da amici della propria rete. Solo un 19 per cento seleziona i link indipendentemente dalla loro origine, diventando così facili bersagli dei cybercriminali e dei loro traffici illegali.

Nel confronto tra i paesi si distingue in particolare la Francia:

Il 60 per cento dei francesi non seleziona i link nei social network. Rispetto a tutti gli altri paesi, è il valore più alto. Il 18 per cento seleziona le pagine Internet di qualunque utente. Tale valore coincide con il valore medio del confronto tra Paesi. Solo il 21 per cento dei partecipanti all'indagine seleziona i siti Web che sono stati pubblicati sulla piattaforma sociale da individui che fanno parte della propria rete di amici. Rispetto ad altri paesi ed anche al valore medio, è il valore più basso. I francesi si dimostrano dunque essere i più sensibili ai pericoli costituiti dai collegamenti a siti Web nei social network.

Grafico 10: Confronto tra paesi riguardo al comportamento rispetto ai clic negli URL dei siti Web nei social network



La consapevolezza più bassa dei pericoli che nascondono i link la detengono gli intervistati della Russia: più di un quarto degli interpellati afferma di selezionare URL di tutti gli utenti, conosciuti e non, del social network e sono dunque i primi in classifica per quanto riguarda questa possibilità di risposta. Solo il 35 per cento non seleziona nessun URL di siti Web. Il 37 per cento degli intervistati russi si limita a selezionare indirizzi Internet di amici.

Tabella 13: Comportamento rispetto ai clic negli URL dei siti Web nei social network dei singoli paesi

Clicchi sui link dei social networks?			
	Si, su tutti	Si, solo su quelli degli amici	No
Mondo	18,77%	35,20%	46,02%
Austria	22,27%	42,45%	35,29%
Belgio	17,34%	34,80%	46,17%
Francia	18,77%	21,01%	60,22%
Germania	22,95%	38,36%	38,69%
Gran Bretagna	14,29%	31,46%	54,25%
Italia	21,44%	33,66%	44,90%
Paesi Bassi	17,50%	34,14%	48,36%
Russia	27,74%	37,14%	35,12%
Spagna	18,43%	45,04%	36,52%
Svizzera	23,71%	38,14%	38,14%
USA	15,79%	34,80%	49,41%

3.3.1 Chi utilizza i social network in modo più sicuro: uomini o donne?

Dallo studio sulla sicurezza di G Data si può effettivamente evincere una differenza tra donne e uomini in relazione all'utilizzo dei link nei social network. Ciò non sorprende, poiché le donne si muovono comunque con più prudenza nelle community virtuali.

La differenza anzi è minima: il 47 per cento delle donne evita i link nelle piattaforme di social network, mentre la percentuale di uomini è solo leggermente inferiore: il 45 per cento. Gli uomini però selezionano con maggior disinvoltura i link di persone che non sono parte della rete di amicizie. Le donne selezionano con una frequenza doppia gli URL di amici rispetto a quelli di altri utenti della piattaforma del social network. Per quanto riguarda gli uomini, un terzo degli intervistati privilegia la selezione degli indirizzi Internet proposti da amici piuttosto che quelli di altri utenti.

Tabella 14: Risultati dettagliati della domanda (risultati generali di tutti i paesi)

Clicchi sui link dei social networks?			
	Si, su tutti	Si, solo su quelli degli amici	No
Uomini (18-24)	26,24%	38,02%	35,74%
Uomini (25-34)	25,92%	38,63%	35,45%
Uomini (35-44)	21,09%	33,56%	45,35%
Uomini (45-54)	18,23%	31,10%	50,66%
Uomini (55-64)	15,93%	26,21%	57,86%
Totale Uomini	21,46%	33,55%	44,99%
Donne (18-24)	21,54%	45,38%	33,08%
Donne (25-34)	20,43%	40,92%	38,64%
Donne (35-44)	15,41%	35,59%	48,99%
Donne (45-54)	13,72%	31,27%	55,01%
Donne (55-64)	9,83%	30,48%	59,69%
Totale Donne	16,29%	36,73%	46,99%
Totale	18,77%	35,20%	46,02%

Fatta eccezione per Italia, Belgio e Austria, i risultati dei singoli paesi mostrano un quadro molto simile:

anche in questi paesi le donne si muovono con molta più prudenza nei social network ed evitano di selezionare URL in generale oppure di cui non conoscono il mittente. Questo succede molto di più rispetto agli uomini, ma la differenza tra i sessi non è solitamente così grande. I risultati degli studi sulla sicurezza condotti in Italia, Belgio e Austria indicano invece un rapporto opposto. Qui sembra siano gli uomini ad essere leggermente più sensibili ai pericoli che derivano dai link nei social network. La discrepanza è minima anche in questo caso.

Ne risulta dunque che sebbene le differenze tra uomini e donne esistano, sono assai esigue ed è dunque difficile concludere che uno dei due sessi sia più prudente nella navigazione nei social network.

3.3.2 Chi utilizza i social network in modo più sicuro: i più giovani o i più anziani?

Gli utenti di Internet più giovani sono notoriamente più presenti nei social network e li utilizzano in modo molto più intenso rispetto ai navigatori più anziani. Malgrado ciò, la generazione precedente è più attenta a muoversi nelle piattaforme di social network, come dimostrato dal risultato generale dello studio sulla sicurezza di G Data. Particolarmente prudenti sono gli uomini e le donne ed in ugual misura, delle fasce di età comprese tra i 45 e i 54 e dai 55 ai 64 (cfr. tabella 14).

Più della metà degli intervistati di queste fasce di età rifiuta categoricamente di selezionare gli URL nei social network. Le donne di questa generazione sono leggermente più critiche rispetto ai loro coetanei maschi. Le tre fasce di età dei più giovani (fino ai 44 anni) privilegiano, come prevedibile, la selezione di siti Web pubblicati, sia di persone conosciute sia di sconosciute.

Conclusione: vince la generazione "silver surfer"

Più sono anziani gli intervistati, maschi e femmine, meno sarà frequente la selezione di link a pagine esterne inserite nei social network. Qui non è rilevante se tali link derivano da persone conosciute o meno. Se da un lato gli uomini di età compresa tra i 55 e i 64 rinunciano alla selezione con una percentuale del 58 per cento, solo il 36 per cento degli uomini di età compresa tra i 18 e i 24 anni, fa altrettanto. Nel caso delle donne la differenza è ancora maggiore. Nelle categorie di età più grandi, il 60 per cento si rifiuta di selezionare rispetto ad un terzo delle donne comprese tra i 18 e i 24 anni. Per contro, il numero delle intervistate che selezionano link di conosciuti e sconosciuti aumenta con il diminuire dell'età. Lo stesso vale per i link di persone conosciute facenti parte della cerchia di amici virtuali.

La prudenza degli utenti più vecchi può avere diverse ragioni: sicuramente la generazione più vecchia è più insicura nei confronti dei social network. Questa forma di Web collaborativo e comunicativo non è per loro così consueta come per la giovane generazione. Per alcune persone più grandi potrebbe però trattarsi di un'insicurezza nell'utilizzo dei portali di social network. I più anziani non fanno uso (come detto in precedenza) dei social network con la stessa intensità dei giovani e non vi passano certo la stessa quantità di tempo. Inoltre, è anche possibile che i contatti nelle reti di questo gruppo di età non pubblicino link esterni o solo in modo limitato e di conseguenza gli intervistati non sono molto a conoscenza della tematica. Un aspetto ulteriore è dato dal fatto che i giovani utenti di Internet lo considerano, insieme ai social network, come una sorta di strumento: è possibile mantenere i contatti o crearne di nuovi, passare del tempo ed esporre fatti personali.

4. Conclusioni

L'indagine indica almeno un fatto estremamente positivo: la maggior parte degli utenti di Internet è a conoscenza del fatto, indipendentemente dalla loro età o sesso, che su Internet ci sono dei pericoli. Tale conoscenza è però per molti di essi limitata a questo ed infatti solo pochi di loro sono in grado di indicare correttamente i pericoli attuali di Internet. Anche la cognizione degli intervistati di come ci si può difendere dai virus è ridotta. Solo pochi sanno come ci si può proteggere dai pericoli insidiosi in modo efficace. Si nota anche come siano ritenute corrette molte affermazioni errate sui pericoli di Internet. Quasi tutti erano convinti di conoscere il significato dei virus e dei codici dannosi ma si basavano su fatti ormai obsoleti. Esistono ancora paure di pericoli che oggi giorno si presentano di rado, come sul malware che si diffonde via posta elettronica (il 54 per cento crede che i virus si diffondono principalmente in questo modo), oppure la credenza che il malware influenzi in qualche modo l'attività del PC (il 92 per cento ne è convinto). Sebbene questo fosse ancora vero negli anni novanta e anche nella primissima parte di questo secolo, ormai non corrisponde più a verità. La maggior parte dei programmi dannosi è ormai programmata in modo così intelligente da risultare invisibili agli utenti di PC, fatta eccezione per i programmi di protezione falsificati, i cosiddetti rogueware. Per quanto riguarda l'illusione che la maggior parte di malware viene inviata per posta elettronica, questa non crea alcun problema. Si consiglia sempre di agire con prudenza con i messaggi di posta elettronica. La selezione di un link o l'apertura di un allegato è sempre un'operazione che comporta dei rischi. Una buona dose di vigilanza non può mai guastare in queste situazioni. L'altro esempio di credenza, ovvero che i virus causino l'arresto dei computer, crea maggiori problemi: finché l'utente non si accorge di nulla, si illude erroneamente di essere al sicuro. Come già in precedenza discusso, le infezioni con codici dannosi al giorno d'oggi non sono visibili all'utente. Il virus è dunque in grado di adempiere il suo compito a lungo, mentre l'autore guadagna da tali risultati.

Un'altra scoperta che fa riflettere è il fatto che i pericoli derivanti dai siti Web siano relativamente sconosciuti. Quasi la metà degli intervistati non crede all'esistenza dei Drive-by Download. Il 48 per cento dei partecipanti all'indagine non ritiene possibile un'infezione del computer con la semplice visita di un sito Web infetto. Questa modalità di infezione rappresenta tuttavia il metodo più utilizzato dai cybercriminali per diffondere il malware. Gli utenti che hanno sentito comunque parlare di Drive-by Download o che lo conoscono hanno delle opinioni precise su dove si possono trovare questi siti Web infetti. In particolare, gli uomini credono (quasi il 44 per cento) che i siti Web pornografici siano più pericolosi della media. Ciò implica anche che i siti Web infetti non siano distribuiti casualmente all'interno del Web. Questa affermazione lascia dunque intendere che i siti Web degni di fiducia non possano essere violati e infettati con codici dannosi. Quasi ogni settimana i mezzi di informazione riportano siti Web di famosi marchi che sono stati violati, e questi sono solo quelli di cui i mezzi di informazione vengono a conoscenza. Chissà quanti sono i casi che non vengono scoperti? In breve: per gli utenti le infezioni Drive-by, dal nome nome esplicito ("infezione durante il passaggio"), non esistono. Di conseguenza, non è possibile che solo in virtù del proprio comportamento, nessuna di queste venga in contatto con il proprio PC.

L'unico modo veramente efficace per proteggere i PC dai Drive-by Download è l'utilizzo di una soluzione di sicurezza completa che contenga un filtro HTTP per la scansione dei siti Web, così da individuare i malware prima che siano caricati. Le soluzioni antivirus gratuite non contengono questa tecnologia di protezione e i loro utilizzatori non sono di conseguenza sufficientemente protetti. Come lo studio ha dimostrato, spesso questi utenti sono dell'opinione che la loro soluzione contenga una protezione globale dai pericoli di Internet. Questo errore può anche rivelarsi fatale e portare ad un'infezione che presenta codice dannoso pericoloso.

Non meno del 62,58 per cento dei possessori di soluzioni antivirus gratuite è convinto che il prodotto possa proteggere il PC da Drive-by Download. Il 25,39 per cento degli utilizzatori crede (erroneamente) che il PC sia invece protetto da Drive-by Download grazie al firewall. Questi utenti, viste le loro convinzioni, non andranno in cerca di filtri HTTP per proteggersi dalle pagine Web infettate.

Tale protezione è di importanza cruciale anche per gli utenti dei social network. In queste piattaforme vengono costantemente pubblicati link a pagine Internet esterne con contenuti spiritosi o informativi oppure con video. Tra l'altro, sono queste le funzioni che rendono così interessanti i social network, come Twitter e Facebook. Sarebbe dunque un peccato dover ignorare totalmente questi link per motivi di sicurezza: tale misura viene comunque adottata dal 46 per cento di coloro che hanno partecipato all'indagine. A questo proposito, è comunque anche necessario menzionare che gli URL abbreviati rappresentano un rischio aggravato, non solo nelle piattaforme di social network. Lo scopo dell'abbreviazione dei link non è subito comprensibile. Con servizi online come <http://longurl.org> è possibile risalire all'indirizzo Internet originario. Questo tipo di servizi, abbinati ad un buon filtro HTTP, rendono un po' più sicura per l'utente la selezione dei link pubblicizzati nei social network.

Rimane difficile giungere a delle conclusioni su chi è più informato sui pericoli di Internet. È evidente che la categoria di persone intervistate di età compresa tra i 25 e i 54 anni è quella più cosciente dei pericoli di Internet, ma comunque spesso ha dubbi anche su situazioni innocue. Per questo è incerto concludere che siano i più saggi utenti di Internet.

La differenza tra uomini e donne appare minima anche se le donne risultano essere leggermente più informate, secondo il risultato generale dello Studio sulla Sicurezza 2011 di G Data. Non è dunque possibile stabilire con certezza quale dei due sessi sia più informato sui potenziali pericoli di Internet. Lo stesso si può dire sulla questione delle nazionalità, anche qui è impossibile decretare un vincitore universale. In Germania, Gran Bretagna e Irlanda del Nord gli utenti sono decisamente più informati su quali siano o non siano i pericoli reali di Internet, ma anche in questo caso la differenza con il dato medio è minima. Un risultato è comunque certo: in Russia l'ignoranza sui pericoli di Internet è maggiore, ma allo stesso tempo fortunatamente i navigatori russi sono quelli che, rispetto agli altri paesi, posseggono in maggior numero una suite di sicurezza a pagamento. C'è anche da sottolineare che in Russia viene utilizzato il maggior numero di copie pirata delle suite di sicurezza, che sono meno stabili e affidabili delle versioni legali.

In definitiva, lo Studio sulla sicurezza 2011 di G Data rivela che malgrado la diffusione ampia dell'utilizzo di Internet, la maggior parte degli utenti conosce poco i pericoli e di conseguenza anche le strategie per evitare che il PC venga infettato con codici dannosi.



Appendice

G Data Software AG

G Data Software, con sede legale a Bochum, è una delle case produttrici di software più innovative e in rapida espansione, specializzata in soluzioni di sicurezza IT. Come specialista della sicurezza su Internet e pioniera nel settore della protezione antivirus, l'azienda fondata a Bochum nel 1985 ha sviluppato il primo programma antivirus già oltre 20 anni fa.

G Data è dunque una delle aziende di software di sicurezza più vecchie del mondo. Da più di cinque anni nessun altro produttore di software europeo di software di sicurezza ha vinto con maggior frequenza premi e certificazioni internazionali e nazionali di G Data.

Il portafoglio di prodotti comprende soluzioni per la sicurezza per il cliente finale di aziende di medie e grandi dimensioni. Le soluzioni di sicurezza G Data sono disponibili a livello mondiale in oltre 90 paesi.

Ulteriori informazioni sull'azienda e sulle soluzioni di sicurezza G Data sono disponibili all'indirizzo www.gdata.it

Pietre miliari di G Data

1986

Il CeBIT prende il volo: in occasione della prima fiera, G Data presenta il primo progetto di protezione antivirus per computer ATARI.

1987

G Data sviluppa numerosi programmi innovativi per ATARI ST, tra cui anche il primo programma antivirus a livello mondiale: G DATA AntiVirusKit.

1990

La diffusione dei Personal Computer avanza rapidamente. G Data inizia lo sviluppo di software per MS Dos. Il primo progetto è la conversione dell' AntiVirusKit per PC, all'epoca una novità: la propria interfaccia utente grafica.

1991

G Data continua a crescere e offre un ampio spettro di diversi programmi software per ATARI ST.

1992

Oltre ai programmi antivirus, G Data sviluppa una serie di software applicativi per MS-DOS e Windows. Particolarmente innovativo: il pianificatore d'itinerari GeoRoute, il primo pianificatore di itinerari per PC con mappe interattive.

1995

Apertura della prima succursale estera in Polonia

1998

PowerRoute, con il suo milione di copie vendute, è il pianificatore d'itinerari per PC più di successo della Germania



2000

Trasformazione in società per azioni: i dipendenti di G Data acquistano la partecipazione alla società. Fino ad oggi, la maggioranza dei dipendenti è socio fondatore della ditta.

2001

Entrata nel mercato di rete e di business con i G Data AntiVirus Business e AntiVirus Enterprise.

2002

G Data sviluppa la tecnologia DoubleScan ed è il primo tra i produttori di software ad installare due motori antivirus in parallelo nei suoi prodotti.

2003

Going International: entrata nel mercato giapponese

2004

G Data presenta al CeBIT la prima generazione di pacchetti di sicurezza completi G Data InternetSecurity.

2005

All'avanguardia: G Data è una delle prime ditte al mondo ad integrare nei suoi programmi di protezione la tecnologia di Cloud Security. OutbreakShield protegge da spam e virus indipendentemente dal contenuto e in tempo reale.

La Stiftung Warentest (organizzazione a tutela dei consumatori tedesca) giudica G Data InternetSecurity come miglior pacchetto di sicurezza.

Going International: apertura delle succursali in Francia e Italia

2006

Il numero di virus aumenta, G Data reagisce: grazie agli aggiornamenti dei database a cadenza oraria, i clienti di G Data sono prontamente protetti da nuovi malware.

2007

Stiftung Warentest: per la seconda volta di seguito, G Data InternetSecurity 2010 si aggiudica il primo posto nei test di confronto effettuati dalla rivista specializzata tedesca più famosa.

CeBit Premiere 2007: G Data TotalCare

2008

Introduzione sul mercato di una soluzione di sicurezza pensata per i possessori di portatili: G Data NotebookSecurity unisce antivirus, backup e tecnologia di cifratura, tutto in una soluzione all in one.

2009

Le soluzioni di sicurezza G Data sono disponibili in più di 60 paesi. Con l'entrata sul mercato in Sud America, Russia, Sudafrica e Cina, G Data prosegue con successo la sua politica di espansione.

2010

G Data festeggia il 25° anniversario di fondazione della ditta

CeBIT Premiere: G Data EndpointProtection

2011

CeBIT Premiere G Data CloudSecurity: plugin del browser per la protezione della navigazione su Internet

Protezione intelligente per smartphone Android e Tablet PC: G Data MobileSecurity

Survey Sampling International

Nel 1977 SSI ha inventato il mercato commerciale dei sondaggi statistici negli USA. Da più di tre decenni determiniamo lo standard delle conoscenze tecniche, della qualità di servizi alla clientela e delle indagini statistiche nell'area delle ricerche di mercato.

SSI offre accesso a più di 6 milioni di partecipanti all'indagine in 54 paesi. Tra le nostre fonti annoveriamo comunità di gruppi di consultazione SSI in 27 paesi, un numero in forte crescita guidato dalle nostre società controllate e dalla nostra ampia rete mondiale di aziende affiliate. SSI utilizza 400 dipendenti appartenenti all'impresa di 50 paesi diversi che parlano 36 lingue, per un totale di 1800 clienti della ricerca di mercato e tre quarti delle più grandi società di ricerche di mercato.

La società dispone a livello mondiale di 17 sedi locali: Pechino, Francoforte, Londra, Los Angeles, Madrid, Città del Messico, Parigi, Rotterdam, Seul, Shanghai, Shelton (CT), Singapore, Stoccolma, Sydney, Timisoara (Romania) Tokyo e Toronto. Vi sono inoltre dei rappresentanti SSI anche a Hong Kong.

Per maggiori informazioni su Survey Sampling International si consiglia di visitare il sito www.surveysampling.com

Glossario

Bot: i bot sono piccoli programmi che in genere vengono eseguiti in background sul computer della vittima senza essere notati e che qui svolgono varie funzioni in base alle loro caratteristiche: da attacchi DDoS a invio di e-mail di spam, fino alla registrazione dei tasti digitati sulla tastiera, e altro ancora. La funzionalità dipende principalmente da quanti soldi si è disposti ad investire per un bot. I bot dotati di molte funzionalità sono naturalmente più costosi dei bot più semplici, in grado di eseguire poche azioni. Vengono venduti anche nei forum underground.

Reti di bot: una rete bot è una comunità di cosiddetti PC zombie. Per gestire una rete di bot vengono utilizzati i server di comando e controllo (server C&C). Le reti di bot servono anche per lanciare attacchi di overload ai server Web (attacchi DoS e DDoS) e per inviare spam.

DoS (Denial of Service): nel caso di un attacco Denial of Service (DoS), ovvero negazione del servizio, i computer, e in particolare i server Web, vengono bombardati con richieste mirate e/o in grandissima quantità. A causa di questo attacco diventa impossibile eseguire i servizi che si bloccano per il sovraccarico.

DDoS (Distributed Denial of Service): un attacco Distributed-Denial-of-Service si basa sullo stesso principio dei normali attacchi DoS con la sola differenza che in questo caso di tratta di un attacco distribuito. Spesso questi attacchi vengono eseguiti con molte migliaia di PC zombie.

Infezione Drive-by (Drive-by Download): l'infezione drive-by si verifica quando, al momento della visita di determinati siti Web predisposti, viene eseguito il download e l'esecuzione inconsapevole di codici dannosi sul proprio PC. Gli autori utilizzano per questi attacchi le falle di sicurezza dei browser e dei loro plugin. Gli aggressori prestano un'attenzione particolare ai punti deboli delle funzioni per l'esecuzione di contenuti attivi (ad es. JavaScript, Flash o Java).



Exploit: programma che sfrutta una falla nella sicurezza esistente nel computer bersaglio per eseguire un qualunque codice di programma.

Phishing: viene detto phishing il tentativo fraudolento di impossessarsi di dati personali come credenziali di login, password, numeri di carte di credito, dati di accesso a conti bancari, ecc., attraverso pagine Web contraffatte o messaggi e-mail indesiderati. I tentativi di phishing si rivolgono principalmente a clienti di banche con offerte di online-banking (CityBank, Postbank), servizi di pagamento (Paypal), Internet Service Provider (AOL) o shop online (eBay, Amazon). Spesso l'utente viene così reindirizzato mediante una mail o Instant Messenger a pagine Web contraffatte che riproducono molto fedelmente le pagine imitate.

Social engineering: il social engineering adotta tattiche di persuasione con cui un pirata informatico induce un utente a fornirgli informazioni che potranno essere usate per recare danno all'utente stesso o alla sua azienda. Spesso l'hacker finge di essere un ente autorevole per ottenere dati di accesso o password.

Spam: a metà degli anni 90 la parola spam descriveva la diffusione esagerata di uno stesso messaggio nei forum Usenet. Il concetto risale ad uno sketch dei Monty Python. Attualmente, il termine ha assunto diversi significati. Come significato generale, si riferisce a tutte quelle e-mail inviate ma non richieste. In senso più stretto il termine spam è limitato alle e-mail pubblicitarie, ovvero worm, hoax, mail di phishing, di risposta automatica non sono considerati tali.

PC zombie: viene detto zombie un PC che diventa controllabile a distanza tramite una backdoor. Riprendendo l'analogia cinematografica, il PC zombie ubbidisce soltanto a chi lo controlla segretamente e esegue le attività, spesso illecite, che gli viene ordinato di compiere. Molti zombie vengono raggruppati nelle cosiddette reti di bot.