di Pier Francesco Piccolomini[1]

Se hai iniziato da poco ad usare un computer e a navigare in internet, è molto probabile che tu ti stia ponendo delle domande sulla sicurezza. E cercando informazioni sull'argomento ti sarai di certo imbattuto in un fiume di parole incomprensibili.

In questo capitolo della nostra guida informatica ti daremo qualche strumento che ti consentirà, quando sentirai parlare di "virus" o di "spyware", di sapere di cosa si tratta. E la conoscenza di un problema è la chiave per sapere come difendersi, giusto? E allora, **immergiamoci nel grande mare della sicurezza informatica**.

Quali sono i rischi?

I pericoli a cui sei esposto quando usi un computer e navighi in Internet sono tanti, ma possono tutti essere ricondotti a due categorie:

- perdita di dati: virus ed altri programmi malevoli possono danneggiare il tuo sistema operativo o cancellare documenti per te importanti;

- furto di dati personali e truffe: alcuni criminali tentano con ogni mezzo di sottrarti informazioni private (dall'indirizzo email al numero della carta di credito passando per le tue password per accedere a vari servizi in internet) per ricavarne profitto.

Come puoi proteggerti?

Il primo passo è capire quali sono e come agiscono i nostri "nemici", in particolare il famigerato virus, l'indiziato numero uno.

[1] Da un post originale di OnSoftware ES: http://onsoftware.softonic.com/guia-seguridad-basica

Un virus informatico somiglia ad un virus vero e proprio perché produce danni agli organismi che colpisce (nel nostro caso si tratta di computer) ed è in grado di riprodursi infettando altri organismi.

I virus sono programmi, esattamente come quelli che installi nel tuo PC per scrivere documenti o ascoltare la musica. La differenza è che si installano senza che il proprietario del computer se ne renda conto, sfruttando falle di sicurezza del sistema operativo o la disattenzione dell'utente.

Gli accorgimenti essenziali per evitare di venir contagiati da un virus informatico sono i seguenti.

1. Installa un software antivirus. Ce ne sono moltissimi, e ne esistono anche di ottimi totalmente gratuiti. Alcuni dei più blasonati tra quelli free sono Panda Cloud Antivirus, avast! Free Antivirus, AVG Anti-Virus 2012 Free Edition e Avira AntiVir Personal. Tra gli antivirus a pagamento i più usati sono Kaspersky Anti-Virus 2012, MacAfee AntiVirus Plus 2011, Norton AntiVirus 2012 e NOD32 Antivirus.

2. Fai attenzione a ciò che installi. Innanzitutto è buona (anzi, ottima) norma leggere con attenzione tutto quello che trovi scritto durante il processo di installazione dei programmi, per evitare di autorizzare cambiamenti o installazioni extra che in realtà non desideri. Ancora più attento devi stare a non installare programmi ingannevoli, cioè che promettono cose che non mantengono.

Un caso tipico è quello degli **scareware**, programmi inutili che però i truffatori cercano di convincerti ad acquistare. La categoria degli antivirus è una delle preferite da questi personaggi, che mettono insieme qualche riga di codice per creare qualcosa che somigli a un programma che protegge il PC e cercano di venderlo per qualche decina di euro a qualche ignaro utente.

Su questo argomento scriveremo presto un post specifico. Per ora ti consigliamo di stare lontano da siti che vendano programmi a pagamento con queste caratteristiche:

- nome del prodotto generico (per esempio, semplicemente Antivirus)

- grafica molto generica

- promesse esagerate o troppo astratte

- scarsa informazione sull'autore del software

- manca una comunità di utenti o un forum su cui si parla del prodotto

- testimonianze generiche e non verificabili di presunti utenti soddisfatti

Fortunatamente oggi è difficile capitare in siti del genere, perché **i sistemi operativi hanno dei meccanismi di difesa in grado di riconoscere con una certa precisione i siti truffaldini**, segnalandoteli quando cerchi di accedervi.

3. Non fidarti di persone che non conosci. Specialmente nelle chat e nelle reti sociali, diffida di chi ti consiglia link (in questo devi usare la diffidenza del buon padre di famiglia, che ti permetterà di intuire se un consiglio di uno sconosciuto sia sospetto o no) e soprattutto non accettare file da nessuno che non sia fidato: potrebbero contenere virus.

4. Tieni il tuo computer sempre aggiornato. Le versioni più recenti del sistema operativo e dei programmi che usi (soprattutto quelli che hanno più a che fare con internet) correggono spesso falle nella sicurezza dei computer e li rendono quindi meno attaccabili. Quando Windows ti offre la possibilità di installare aggiornamenti, fallo. È sempre la scelta migliore.

E contro le truffe, come si fa?

Internet è un luogo di libertà, e come tale è pieno di cose buone ma anche di cose cattive. I truffatori, ad esempio, ci si muovono molto bene. Con qualche accorgimento, però, non riusciranno ad avere la meglio su di te.

Il consiglio più importante è **scegliere sempre password sicure** per proteggere l'accesso a tutti i tuoi account (posta elettronica, siti che visiti e account Facebook, ad esmpio).

Una password solida deve avere alcune caratteristiche: deve essere lunga almeno 7 caratteri (ma di più è molto meglio), deve contenere lettere maiuscole, lettere minuscole, numeri e caratteri speciali (ad esempio £, &, %) e non deve esistere nel vocabolario. Da evitare come la peste sono le password con il nome del nipote, della moglie, del gatto, la data di nascita propria o di una persona cara e le password tipo "1234567890", facili da ricordare tanto quanto da rubare.

In secondo luogo, non devi credere a tutto quello che leggi in internet. **Chiunque può aprire una pagina web in pochi minuti**, scriverci qualunque cosa e metterla online. Per questo, quando cerchi informazioni cercale su fonti affidabili, e se hai la sensazione che una non lo sia, probabilmente hai ragione.

Ecco dunque alcune regole pratiche riassuntive per navigare in internet in sicurezza ed evitare le truffe:

- **Non credere a tutto quello che ti arriva per posta elettronica**. Ti capiterà di certo, se non ti è già capitato, di ricevere email di sconosciuti che ti offrono milioni di dollari in cambio di un piccolo aiuto. Il 100% di quei messaggi sono truffe che non solo non ti porteranno un euro in tasca, ma te ne sottrarranno. Garantito. Un discorso simile vale per le cosiddette **catene di Sant'Antonio**, in cui qualcuno di dice di girare l'email che hai ricevuto a un tot di amici, guadagnando qualcosa per questo. Anche queste sono

truffe. Non rispondere mai alle catene di Sant'Antonio, e **non cedere alla tentazione al pensiero di "lo faccio lo stesso, non si sa mai"**. Hai solo da perderci;

- installa e mantieni sempre aggiornato un antivirus;

- Non comprare online su siti che non ti diano totale fiducia;

- Non rivelare mai più dati personali di quelli che sono necessari per godere del servizio che stai cercando. Se ti viene chiesto di più, quasi sicuramente c'è qualcosa di poco pulito di cui rischi di rimanere vittima.