Book 10

Usare computer e Internet in sicurezza

Aggiornamenti del sistema operativo e delle applicazioni.

Sapere come funzionano Antivirus e Firewall.

Riconoscere e sapersi proteggere (malware e spyware).

Riconoscere e saper evitare inganni e furti d'identità.

pane e internet

IN RETE È PIÙ FACILE!

Conoscere le minacce che sono presenti su internet e quali sono le difese che possiamo attivare è di fondamentale importanza per tutelare i nostri dati personali e non cadere in truffe.
In questo Book impareremo come verificare che il nostro computer sia sempre aggiornato e che gli strumenti di difesa siano attivi.

CORSO DI ALFABETIZZAZIONE DIGITALE PER CITTADINI

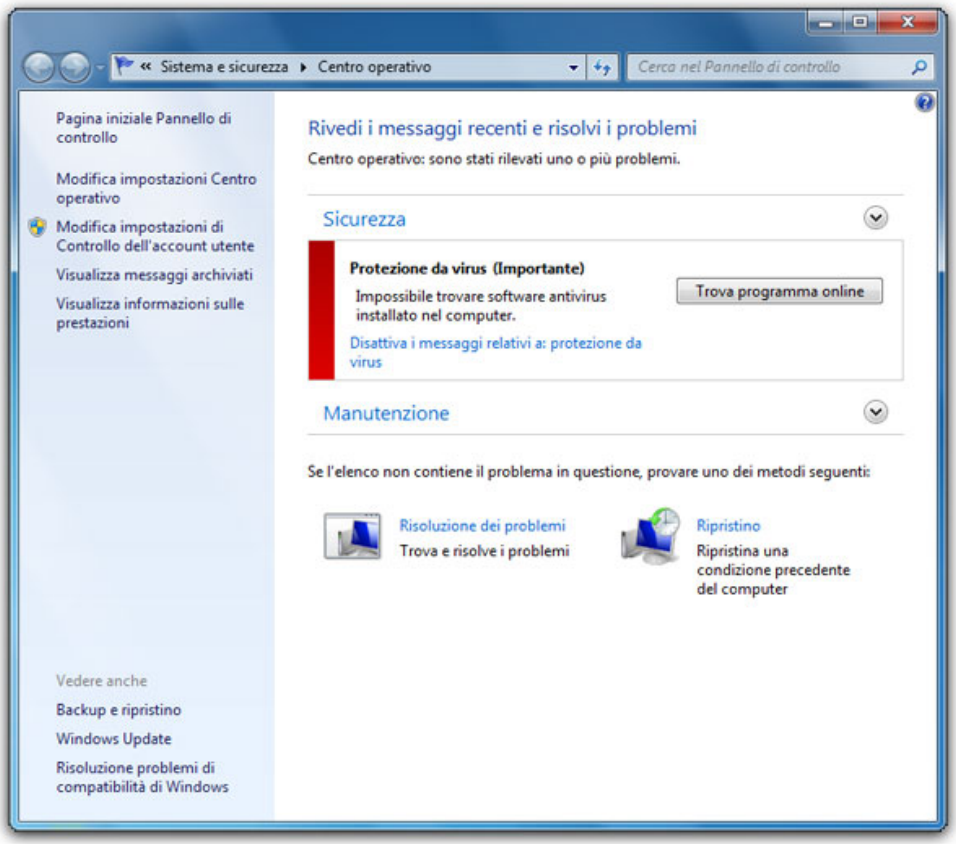
Primo Livello COMPUTER

Book 10: Usare computer e Internet in sicurezza

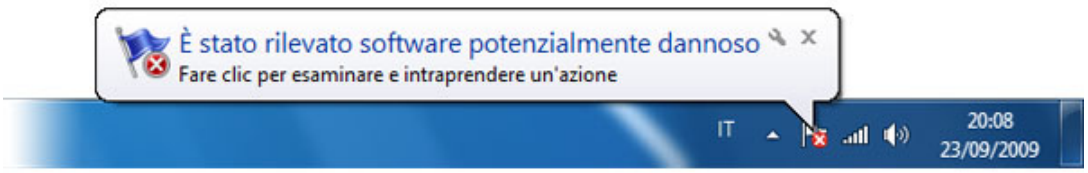
Il Centro Operativo

Il **Centro Operativo** è il punto di partenza per visualizzare gli avvisi e per attivare le funzionalità di sicurezza del sistema operativo (Windows 7).

Per visualizzare il **Centro operativo**, una volta aperto il **Pannello di controllo**, si fa click sulla voce **Sistema e sicurezza.**



Dal **Centro operativo** possiamo controllare lo stato del **firewall** di Windows (un sistema di sicurezza che vedremo più avanti), **l'aggiornamento dell'antivirus**, le funzioni di **Windows Update** (gli aggiornamenti di Windows), lo stato del **backup** (copie di sicurezza) e altro ancora. Il servizio **Segnalazione errori Windows** è il sistema che segnala a **Microsoft** l'esistenza di problemi sul sistema operativo e gli consente di pubblicare le soluzioni su internet.



In dettaglio il **Centro operativo** lo si apre seguendo questo percorso:

Start > **Pannello di controllo** > **Sistema e sicurezza** > **Centro operativo**

Un altro modo è quello di fare click sull'icona a forma di bandierina bianca presente nell'area di notifica (a fianco all'orologio).

Se la bandierina mostra una **piccola "x" bianca su sfondo rosso** significa che il problema evidenziato **è grave**. Con un click sulla bandierina prima e uno successivo su **Apri Centro operativo** potremo leggere i messaggi e le soluzioni proposte per la risoluzione al problema.

La voce **Visualizza messaggi archiviati** presente nel pannello di sinistra ci consente di leggere i vecchi messaggi e le eventuali soluzioni proposte.

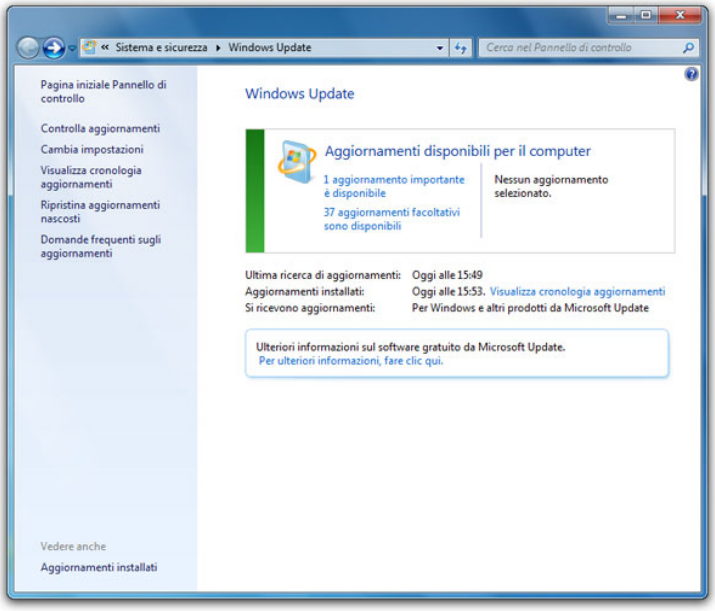
Windows Update

Avere un computer **sempre aggiornato** è di fondamentale importanza per non perdere i dati contenuti a causa di instabilità o difetti del sistema operativo. In **Windows 7** abbiamo a disposizione **Windows Update**, una funzionalità del sistema operativo, che si occupa di verificare lo stato del nostro computer e di scaricare gli ultimi aggiornamenti necessari.

Aggiornare il sistema operativo

Un sistema è tanto più sicuro quanto più è aggiornato: è quindi consigliato verificare e scaricare regolarmente gli aggiornamenti proposti. Per eseguire questa operazione di routine basta configurare correttamente **Windows Update**.

Per aprire il servizio è sufficiente scrivere nella **casella di ricerca** "windows update" e premere **invio**.

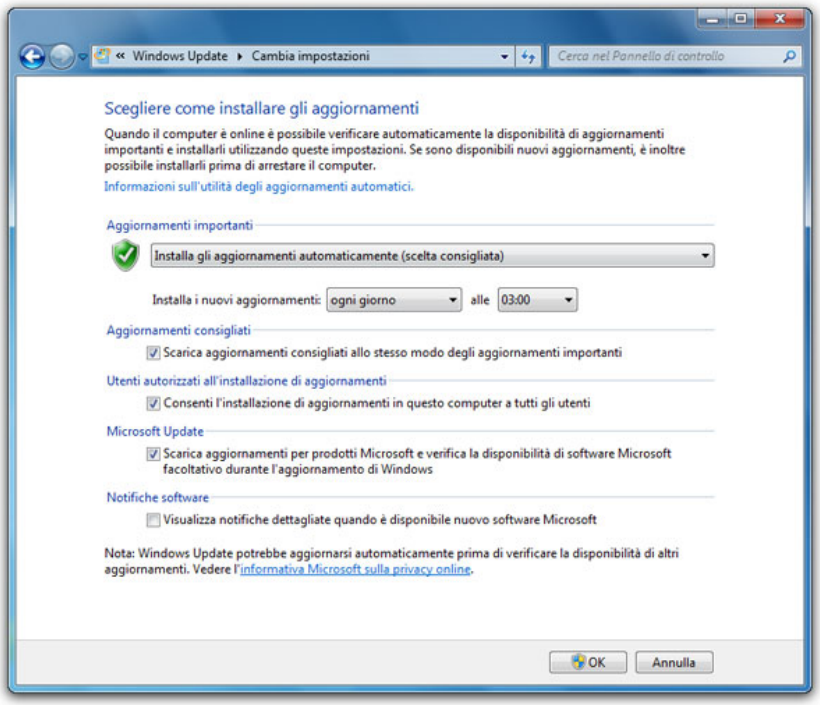


Controlliamo che **Windows Update** abbia le impostazioni per verificare, scaricare e installare **automaticamente** gli aggiornamenti.

Nella finestra del programma cerchiamo la voce **Cambia impostazioni** dal **pannello di sinistra.** Il menu a tendina presente come prima opzione deve essere settato sulla voce **"Installa gli aggiornamenti automaticamente (scelta consigliata)"**. Verifichiamo inoltre che le prime tre caselle di controllo siano spuntate, in particolare:

- Scarica aggiornamenti consigliati allo stesso modo degli aggiornamenti importanti.
- Consenti l'installazione di aggiornamenti in questo computer a tutti gli utenti.
- Scarica aggiornamenti per prodotti Microsoft e verifica la disponibilità di software Microsoft facoltativo durante l'aggiornamento di Windows.

La quarta voce è opzionale e ci consente di ricevere informazioni su nuovi software di Microsoft.



Windows prevede due livelli di aggiornamenti:

- gli **aggiornamenti importanti** che sono **automaticamente rilevati e installati**;
- gli **aggiornamenti facoltativi** che vengono **solo segnalati** lasciando a noi la decisione se procedere o meno alla loro installazione.

Per installare uno o più aggiornamenti facoltativi è sufficiente selezionarli dall'elenco proposto marcando la casella di controllo e procedere con un click sul **OK**.

Nota: Microsoft rilascia gli aggiornamenti di sicurezza ogni secondo martedì del mese; in genere alle 19 ora italiana.

Se volessimo controllare la presenza di nuovi aggiornamenti, sarà sufficiente fare click sul collegamento **Controlla aggiornamenti** (nel **pannello di sinistra**). La voce **Visualizza cronologia aggiornamenti** ci permette di controllare la cronologia degli aggiornamenti

installati mentre con **Ripristina aggiornamenti nascosti** controlliamo eventuali aggiornamenti che non sono stati eseguiti e nascosti.

Gli aggiornamenti non importati possono essere rimossi nel caso che abbiano causato problemi di funzionamento al computer. Per farlo, partendo dal **Pannello di controllo**, clicchiamo sulla voce **Disinstalla un programma** (nel gruppo Programmi), e una volta entrati nella finestra che visualizza l'elenco dei programmi installati, individuiamo il collegamento **Visualizza aggiornamenti installati** dal **riquadro di sinistra** e facciamo click sopra. Ora dovremo scegliere quale aggiornamento rimuovere **selezionandolo con un click** e, infine, un ulteriore click su **Disinstalla** nella barra degli strumenti.

Antivirus

Quasi non ci accorgiamo della presenza dell'Antivirus nel nostro computer, resta lì buono, da una parte, e sembra quasi addormentato, ma in realtà compie una serie di operazioni che **proteggono il nostro computer** dagli attacchi dei **virus** di tutti i tipi.

Ne esistono molti tipi, con caratteristiche differenti: quelli che utilizziamo comunemente sui nostri computer sono in perenne ricerca di virus sia all'interno della memoria RAM (memoria di lavoro), sia nel disco rigido, ma soprattutto nel flusso di dati che entrano ed escono nel nostro computer.

Come fa un antivirus a riconoscere un virus? Per semplificare il tutto possiamo affermare che ogni virus porta con sé **una firma**, ovvero una sequenza di caratteri univoca per quel virus, che lo identifica e distingue da tutti gli altri. Gli antivirus **effettuano controlli specifici alla ricerca di queste firme**.

Ogni famiglia di antivirus conserva un archivio di firme che individuano i file pericolosi. Ogni volta che una **firma viene riconosciuta** all'interno di un file o di un processo in esecuzione, l'antivirus ci avvisa. Nei casi non particolarmente gravi ci è lasciata la facoltà di decidere se tentare di **pulire il file** o di **buttarlo nel cestino**. In caso di **minaccia più grave** l'antivirus **cestina automaticamente** il file prima che possa causare danni al computer.

È lampante come sia fondamentale avere un **antivirus sempre aggiornato** con l'ultimo elenco disponibile delle firme dei virus per poter riconoscere le nuove minacce. Un antivirus non aggiornato è pressoché inutile.

Non sempre però il riconoscimento delle firme è una sistema che ci mette al sicuro. I moderni antivirus hanno messo in campo un'altra strategia di controllo, il metodo è chiamato **euristico**. Con questo metodo l'antivirus controlla il funzionamento di qualsiasi programma e nel caso in cui venga rilevato un malfunzionamento, o un comportamento anomalo, viene inviato un allarme all'utente per informarlo che probabilmente un virus sta tentando o, nel peggiore dei casi, è riuscito a infettare il computer.

Quello **euristico** è sicuramente il **metodo migliore di difesa** per tutti quei virus sconosciuti di cui non si conosce ancora la firma.

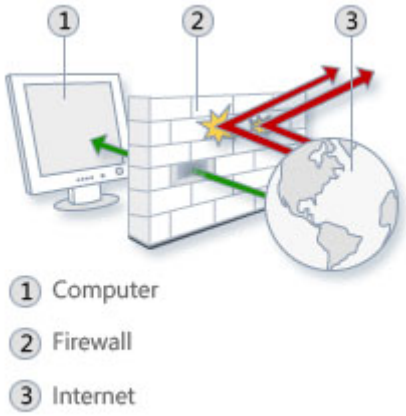
I programmi antivirus hanno prezzi decisamente abbordabili e ne esistono diverse versioni con funzionalità di base gratuiti. Ricordiamoci che la lotta contro la propagazione dei virus in rete comincia proprio dall'installazione e dall'aggiornamento del nostro antivirus.

Firewall di Windows

Il **firewall** è un programma (software) o un dispositivo (hardware) che **controlla le informazioni** provenienti da internet o da un altro tipo di rete. Il firewall può **bloccare** o **consentire** l'accesso al computer, a seconda delle opzioni impostate.

Un firewall impedisce a **pirati informatici** o **programmi dannosi** (ad esempio i 'trojan', cavalli di Troia) di accedere al computer tramite una rete locale o internet, nonché di bloccare l'invio di programmi dannosi ad altri computer.

Il firewall funziona come in questa immagine, dove le frecce rosse sono gli accessi indesiderati mentre la verde rappresenta quelli consentiti (navigazione nelle pagine web, le email, ecc.).



Precisiamo che un firewall si occupa di monitorare le attività da e verso il computer e **non un programma antivirus**. Un buon livello di protezione prevede l'uso contemporaneo di **un firewall,** di un **programma antivirus** e di un **antimalware**.(il malware è un programma dannoso).

Per verificare le impostazioni del Firewall eseguiamo il **Pannello di controllo** e facciamo click sul collegamento **Sistema e sicurezza**, nella nuova scheda selezioniamo con un click la voce **Firewall.**

Le impostazioni consigliate per un buon funzionamento del Firewall sono le seguenti:

- Firewall attivato per tutte le connessioni di rete.
- Blocco di tutte le connessioni in entrata, tranne quelle consentite in modo esplicito.

- Firewall attivato per tutti i tipi di rete (privata, pubblica o di dominio).

Se dovessimo avere dei dubbi sulla configurazione del Firewall sarà sufficiente fare click sulla voce **Ripristina impostazioni predefinite** nel riquadro di sinistra.

Malware (virus, spyware, adware e phishing)

Malware è una parola composta, originata dall'unione dei due termini "**mal**icious soft**ware**" (programma dannoso).

È considerato malware **qualsiasi programma** creato apposta per danneggiare un sistema operativo, compromettere funzioni del computer, o compiere a nostra insaputa azioni illegittime con il nostro computer, i nostri dati, le nostre connessioni (come, per esempio, rubare dati personali o inviare automaticamente email con il nostro indirizzo, senza autorizzazione).

I virus sono dunque **solo una categoria di malware**.

La famiglia dei **malware** raggruppa diverse tipologie di minacce, per citarne alcune ricordiamo: **worms**, **trojans**, **bots**, **spyware**, **adware**, **rootkits**, **keyloggers**.

Conoscere **la differenza** tra tutte queste forme di software maligno ci serve per adottare specifiche forme di difesa: per proteggere meglio il computer da minacce diverse abbiamo infatti bisogno di protezioni diverse. Proprio come per le **infezioni nel mondo reale**, è necessario adottare diverse terapie ecurarsi con medicinali diversi a seconda del tipo di malattia.

Virus

Un **virus** è un tipo di malware capace di **autoreplicarsi** (si moltiplica da solo) e diffondersi nel computer e poi in altri computers, attaccandosi a un altro programma (legittimo), attivandosi quando l'utente avvia quel dato programma.

Un virus informatico può **restare nascosto nel computer**, attaccato a un programma o file, inattivo fino a quando l'utente avvia quel dato programma o apre il file infettato. Se non curiamo l'infezione, il virus può infettare diversi file, cartelle, il registro di sistema, ecc.

I virus si diffondono attraverso file infetti trasmessi da computer a computer **con chiavette USB**, oppure **scaricati da Internet** attraverso **file-sharing** (condivisione di file), **email** o anche **allegati** in programmi di **messaggistica istantanea**.

I **virus non sono tutti uguali e possono creare danni di diversa gravità**: talvolta provocano un leggero rallentamento del sistema operativo ma spesso riescono a danneggiare i dati e programmi fino a **bloccare completamente il computer**.

I nuovi virus sono concepiti non tanto per **creare danni** quanto **per sottrarre informazioni**, danneggiare reti, rubare denaro, creare pubblicità come fanno gli **adware** (software sovvenzionato da pubblicità), ecc.

La cura contro i **virus** è costituita dai programmi **antivirus o antimalware**.

Foto di mariotto52 via Flickr
(https://flic.kr/p/FC16U - CC BY-NC 2.0)

Spyware

Gli **spyware** spiano quello che facciamo sul computer e su Internet.

Uno spyware può anche prendere **parziale controllo del computer** (ad esempio per dirottarci su determinati siti web quando navighiamo), ma in genere raccolgono dati ed informazioni personali senza che ce ne accorgiamo.

Gli spyware raccolgono i dati monitorando le nostre attività, anche **accedendo a particolari file** chiamati logs, che contengono informazioni sull'uso del computer. Possono **registrare quello che digitiamo sulla tastiera** oppure fare una **scansione del computer** per trovare file e cartelle contenenti **dati personali**.

Tutte le informazioni raccolte vengono inviate ad aziende che li usano per pubblicità, sondaggi e altre forme di **spam** (posta indesiderata e ingannevole). I dati possono essere usati da **hackers** (pirati informatici), che fanno parte di organizzazioni criminali diffuse in tutto il mondo e che li usano per attività illegali molto più dannose della pubblicità non richiesta, come ad esempio accedere al conto bancario e trasferire del denaro.

Gli spyware spesso arrivano al nostro computer quando scarichiamo programmi gratuiti da determinati siti **poco attenti alla sicurezza**, o quando facciamo scansioni online in posti poco sicuri, installando **add-ons** o **plugins infetti** (estensioni per i programmi per abbellirli o aggiungere funzionalità) o **visitando siti maligni.**

Gli spyware, per essere rimossi, necessitano di specifici programmi.

Adware

Anche **Adware** è la fusione di due termini inglesi: **ad**vertisement (pubblicità) e mal**ware**.

Gli adware quindi sono concepiti per **mostrare pubblicità** ogni volta che usiamo specifici programmi.

Questo avviene frequentemente con alcune versioni gratuite di programmi a pagamento, per spingerci all'acquisto del programma anche con falsi messaggi allarmistici.

Un'altra modalità con cui gli adware mostrano pubblicità sono le **pop-up** (finestre indesiderate) o **nuove finestre** del **Browser**, aperte automaticamente durante la normale navigazione in Internet.

L'adware non è particolarmente pericoloso, anche se è evidentemente fastidioso e rappresenta un'intrusione nel nostro computer.

Succede però che un adware si accompagni a uno spyware e in questo caso, come abbiamo visto, la pericolosità cresce notevolmente.

Gli adware si eliminano con specifici programmi di rimozione.

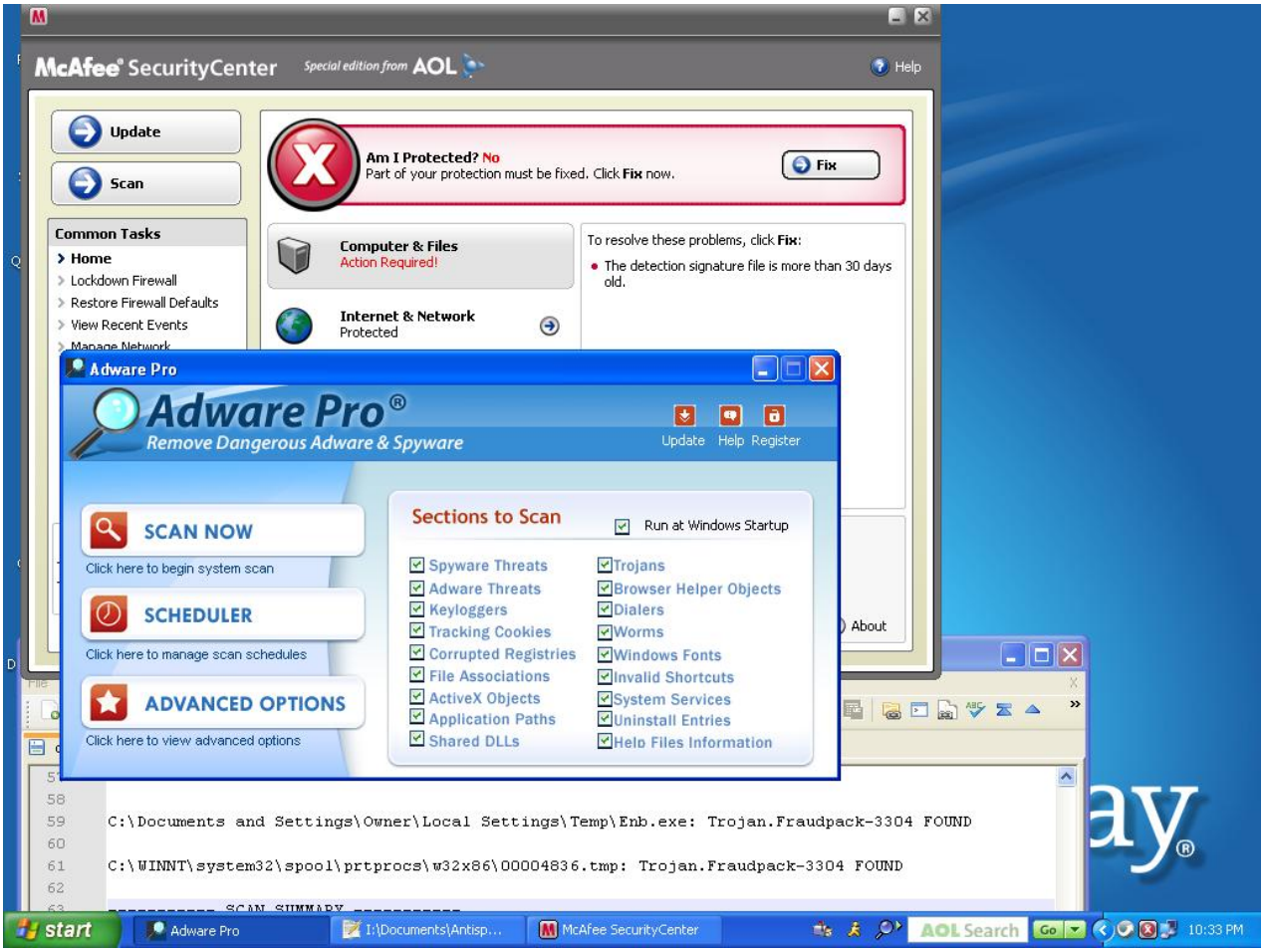


Foto di Ron A. Parker via Flickr (https://flic.kr/p/7L5cPH - CC BY-NC-SA 2.0)

Phishing

Il **phishing** è una **truffa via Internet** attraverso la quale ci vengono **trafugati dati personali**.

Tra le diverse pratiche di pirateria, il phishing è tra le più ambigue mai messe in atto. Questo tipo di truffa sfrutta la buona fede delle persone per entrare in possesso di loro dati sensibili (come quelli di accesso a conti correnti bancari o postali).

Foto di betacontinua via Flickr
(https://flic.kr/p/5aT7yF - CC BY-NC-SA 2.0)

Perché la truffa riesca sono necessari diversi passaggi:

1. **Vengono inviate migliaia di email** che imitano alla perfezione, nella grafica e nel contenuto, comunicazioni da parte di un istituto bancario, di un servizio web, di un famoso sito di aste online o altre istituzioni note e quindi considerate attendibili.
2. Nel messaggio si annuncia che è stato **riscontrato un possibile problema**, spesso legato alla sicurezza, e che c'è la necessità di verificare l'account del ricevente, cliccando sul **collegamento (link)** presente nel testo dell'email.
3. Questo collegamento **non porta però al sito dell'istituzione** indicata, bensì ad una **copia perfetta** dello stesso, creato appositamente per indurre il malcapitato ad effettuare un tentativo di login inserendo lo username e la password negli appositi campi che, in questo caso, vengono automaticamente copiati in un data base del truffatore.
4. La truffa ha avuto successo e il suo autore è ora in possesso dei dati per accedere ai servizi del truffato!

Questo che segue è uno dei tanti esempi di improbabili mail (di false Poste Italiane) che possiamo ritrovarci nella posta in arrivo. Molto spesso è sufficiente leggere il testo della mail per individuare grossolani errori di ortografia o indirizzi compilati stranamente. È comunque importante non cliccare su questi messaggi perché possono comunque rimandarci a siti che tentano di installarci automaticamente dei malware, anche senza che l'utente arrivi alla compilazione dei campi di login.

Prestiamo quindi molta attenzione.

Le nostre armi di difesa contro questa forma di truffa informatica **partono dal buon senso**.

Un'istituzione seria non ci richiederà mai i nostri dati personali attraverso una semplice email.

La maggior parte di questi messaggi vengono catalogati come **spam** dai sistemi di sicurezza dei provider di posta elettronica. Può accadere che alcune di queste email riescono a sorpassare il sistema antispam. In questo caso e in generale è dunque necessario fare comunque molta attenzione: **il superamento dei sistemi di sicurezza** non è affatto **sinonimo della veridicità del mittente**.