Enrica Biscaro – Tiziana Gianoglio

TESINA DI INFORMATICA

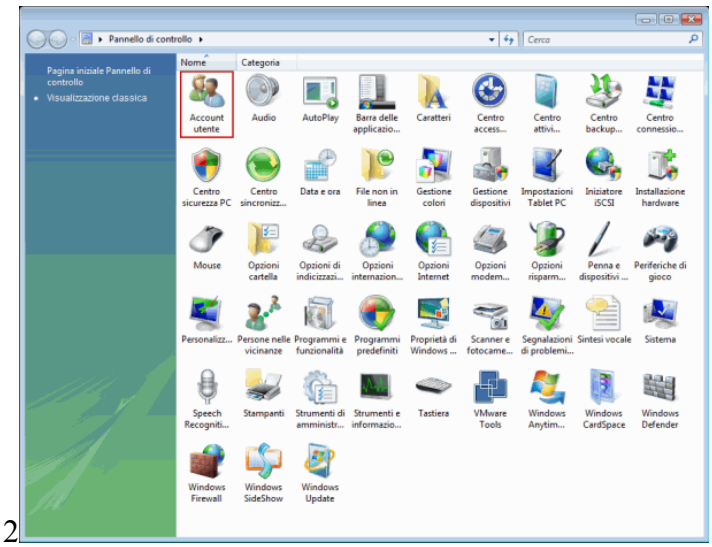
Cenni preliminari sugli account amministratore e account limitato.

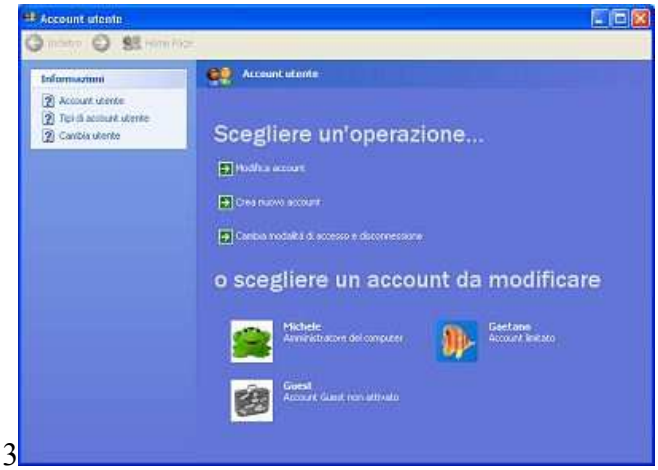
Per un funzionale utilizzo del nostro computer è preferibile usare la funzione che ci permette di creare un account amministratore protetto da password.

Anche se il computer è utilizzato da una sola persona, avere una password per accedervi, è il primo passo per garantire la sicurezza dei nostri dati e della nostra privacy.

Come si fa a creare un nuovo account se il proprio sistema operativo è WINDOWS:
Start → Pannello di controllo → Account utente

1 

2 

3 

La procedura per creare nuovi account o modificare immagine dell'account stesso e modificare la password è molto intuitiva; è sufficiente utilizzare le operazioni automaticamente proposte dal sistema, come mostrato nella schermata num.3.

Una ragione in più per utilizzare questa funzione si verifica quando il computer è condiviso tra più persone. In questi casi è possibile che le impostazioni del computer vengano inavvertitamente modificate dagli altri utenti.

Mediante gli "account utente" è possibile evitare che altre persone possano accedere e modificare i dati sensibili contenuti nel computer. Gli account utente, inoltre, consentono di personalizzare Windows per tutti gli utenti che condividono un computer; non solo è possibile modificare lo sfondo del desktop, la password e la propria immagine personale, ma l'account utente offre anche una visualizzazione personalizzata dei file, un elenco dei siti web preferiti e un elenco delle pagine web visitate di recente.

È importante sapere che i documenti creati o salvati vengono archiviati nella cartella Documenti, in una posizione distinta rispetto ai documenti degli altri utenti che utilizzano il computer.

Per ottimizzare il livello di protezione dei file e assicurarsi che ne venga consentito un utilizzo esclusivamente privato, è quindi opportuno che tutti gli account utenti impostino una password.

Comunque è sempre possibile contrassegnare come "condivisi" gli elementi e i file per cui si desidera consentire l'accesso ad altri utenti.

Se invece non si utilizza una password altre persone potranno accedere all'account e visualizzare tutte le cartelle e i file.

Esistono due tipi di account utente:

- Amministratore del computer
- Account limitato.

Gli utenti che dispongono dell'account amministratore possono modificare tutte le impostazioni del computer mentre gli utenti che dispongono dell'account limitato possono modificare solo alcune impostazioni, come illustrato nella tabella sottostante.

Impostazioni	**Amministratore computer**	**Account limitato**
Installazione di programmi e hardware	☺	☹
Modifica impostazioni globali del sistema	☺	☹
Accesso e lettura di tutti i file non privati	☺	☹
Creazione ed eliminazione degli account utente	☺	☹
Modifica degli account di altri utenti	☺	☹
Modifica del nome o del tipo del proprio account	☺	☹
Creazione, modifica e rimozione della propria password	☺	☺
Modifica dell'immagine associata al proprio account	☺	☺

Esistono, inoltre, due tipi di account limitati: l'account Utente Standard e l'account Guest.

Il primo consente ad un utente di utilizzare la maggior parte delle funzionalità del processore, ma è necessaria l'autorizzazione dell'account amministratore se si desidera eseguire modifiche che hanno effetti su altri utenti oppure sulla protezione del computer, come segnalato nella tabella sopra.

Gli account Guest, invece, sono un account destinato ad utenti che non dispongono di un account permanente sul computer. Usare questo account consente ad un utente di utilizzare il computer senza però avere la possibilità di accesso ai file personali di altri utenti. Gli utenti che utilizzano un

account Guest non possono installare software o hardware, modificare impostazioni e creare password. È necessario che si attivi un account Guest prima di poterlo utilizzare, e questo è possibile seguendo i passaggi della creazione degli account utente come visibile nella schermata numero 3.

Non c'è limite al numero di account che è possibile creare nel computer e l'account amministratore dispone dell'accesso completo a tutti gli account possibili.
Nel momento in cui si crea o si modifica la password è possibile digitare un suggerimento utile nel caso la si dimentichi.
I suggerimenti più utili sono composti da parole, frasi e numeri significativi per l'utente.
Questi devo essere chiari per l'utente interessato, ma vaghi per gli altri in modo che questi ultimi non possano risalire alla password.
Se si dispone di un account limitato e, nonostante i suggerimenti non si riesca a ricordare la password, sarà necessario rivolgersi ad un utente che dispone dell' account amministratore per richiedere la creazione di una nuova password.

La sicurezza informatica

Il discorso riguardante gli account ci riporta, a rigor di logica, alla questione della sicurezza informatica.
Il termine **sicurezza informatica** indica la capacità di salvaguardare riservatezza, integrità e disponibilità dell'informazione, sia questa elaborata sul computer, memorizzata su supporti di diversa natura o trasmessa lungo canali di comunicazione.

In questo modo si può ridurre il rischio che qualcuno possa accedere ai nostri dati senza averne l'autorizzazione, si riduce il rischio che i dati possano essere modificati o, addirittura, cancellati in seguito a interventi non autorizzati.

Spesso, noi psicologi, siamo poco informati riguardo ai rischi in cui ci si può imbattere se non si osservano le misure di sicurezza elementari, anche a livello legale. È quindi importante sapere che per quanto riguarda la Legge, questa suddivide la tutela in due parti: da un lato impone una, seppur minima, apposizione di norme di sicurezza al proprio sistema informatico, necessarie ad impedire l'introduzione, nel sistema stesso, di terzi non autorizzati, sempre nell'ottica di prevenire la perdita dei dati e impedirne il trattamento in modi non consentiti dalla Legge stessa.
Dall'altro si occupa di veri e propri crimini informatici come ad esempio l'accesso abusivo ad un sistema informatico o telematico (art.615-ter). Il seguente articolo cita testualmente:
"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti."

Conclusa questa breve digressione sugli aspetti legali della sicurezza del pc, torniamo agli aspetti prettamente informatici.
Per determinare una politica di sicurezza è necessario individuare le componenti del sistema che devono essere protette:

- ✓ Hardware → componente fisico di una periferica o di una apparecchiatura elettronica.
- ✓ Software → è un programma o un insieme di programmi in grado di funzionare su un computer
- ✓ Dati → informazioni gestite dai programmi
- ✓ Supporti memorizzazione
- ✓ Reti → che permettono l'interconnessione di vari sistemi e, quindi, lo scambio di informazioni
- ✓ Accessi → la possibilità data all'utente di accedere a determinate risorse.

Inoltre per adottare le opportune misure di sicurezza bisogna sapere da chi proteggersi. A riguardo possiamo distinguere hacker e cracker. I primi sono coloro che entrano nei sistemi operativi altrui per divertimento o per dimostrare di saperlo fare, nella maggioranza dei casi per non arrecare danni al sistema; al contrario i cracker sono coloro che violano i sistemi informatici con lo specifico intento di provocare danni al sistema.
Un'ulteriore distinzione è tra outsider e insider, rispettivamente coloro che operano all'esterno rispetto al network che vogliono attaccare e coloro che sono effettivamente autorizzati all'uso della rete e che cercano di abusarne

Accenniamo, ora, alle modalità attraverso cui vengono realizzati gli attacchi informatici. Le "tecniche" sono svariate, ricordiamo ad esempio:

- ❖ Virus
- ❖ Trojan
- ❖ Spyware
- ❖ Worm
- ❖ Phishing

I **virus** sono dei programmi, ovvero una seria di istruzioni che sono state scritte da un programmatore ed eseguibili da un computer per "inglobarsi" e confondersi con le istruzioni di altri

programmi; chi l'ha scritto ha previsto la possibilità che il virus sia in grado di replicarsi e copiare le istruzioni che lo compongono, in altri programmi. La caratteristica fondamentale di un virus è che, dopo un determinato tempo nel quale si replica, comincia a compiere l'azione per la quale è stato scritto, azione che varia dal distruggere dati e programmi presenti nel processore al far comparire nello schermo un messaggio di infezione.
Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di "contagio" era lo scambio di floppy disk contenenti file infetti; oggi, il veicolo preferenziale di infezione è rappresentato dalle comunicazioni e-mail e dalle reti peer-to-peer.

Un **trojan**, in italiano, cavallo di troia,è un tipo di malware (si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito). Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.

Uno **spyware** è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente, come ad esempio i siti visitati e gli acquisti fatti in rete, senza il suo consenso; non si replica ma richiede l'esecuzione inconsapevole da parte dell'utente.
La diffusione avviene, sfruttando la vulnerabilità del browser, o visitando pagine web o mediante tecniche di social engeneering.
Le conseguenza della diffusione sono la ricezione di pubblicità non richiesta (spam), la modifica della pagina iniziale del browser e la modifica della lista dei preferiti del web.

Un **worm** è una particolare categoria di malfare in grado di autoreplicarsi; molto simile ad un virus, a differenza di questo non necessita di legarsi ad altri programmi eseguibili per diffondersi. Tipicamente il worm modifica il computer che infetta, in modo da essere eseguito ogni volta che si avvia il processore e rimane attivo finche questo non viene spento. Il worm tenta di replicarsi sfruttando la connessione internet e la posta elettronica: il maleware ricerca indirizzi e-mail memorizzati sul computer e invia una copia di se stesso come file allegato a tutti, o parte, degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm spesso utilizzano tecniche di social engeneering per indurre il destinatario ad aprire l'allegato.

Le principali modalità di difesa dagli attacchi informatici

Per evitare attacchi informatici, o almeno per limitarne le conseguenze, vanno prese delle contromisure; calcolatori e reti necessitano di protezione.
L'unico computer a prova di attacco informatico è quello spento, non collegato ad Internet e chiuso a chiave in una cassaforte.

Come in qualsiasi ambiente la sicurezza assoluta non è realizzabile, però sono stati sviluppati degli strumenti per limitare i rischi, permettendo così di mantenere un appropriato livello di sicurezza. Innanzitutto è molto importante mantenere continuamente aggiornati sia il sistema operativo che i programmi applicativi, installando programmi appositi ("updates"), in modo particolare quelli relativi alla sicurezza. Così facendo si protegge il calcolatore dalle vulnerabilità che di mano in mano vengono identificate e che prima o poi saranno sfruttate da qualche meccanismo di attacco. Qualsiasi computer deve essere seguito in modo appropriato; il proprietario dovrebbe sapere bene quello che sta facendo, per ridurre al minimo le "porte" aperte a possibili intromissioni. Non si devono usare password ovvie (che possono essere facilmente intuite) ed è consigliabile limitare allo stretto indispensabile gli eventuali servizi che un calcolatore connesso in rete offre ai suoi utilizzatori.

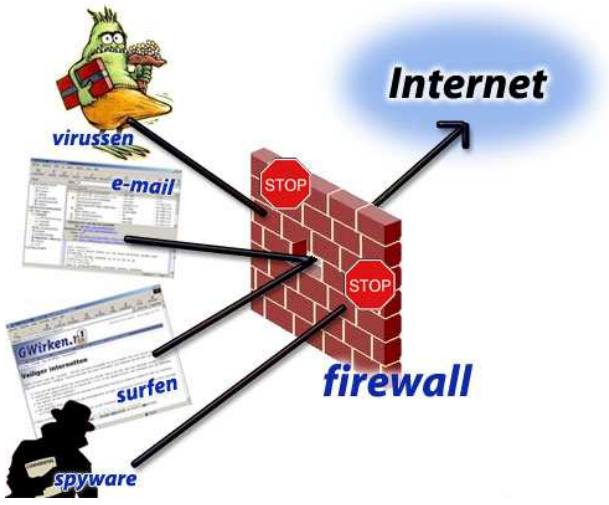
Per quanto concerne i virus, è bene utilizzare dei programmi "antivirus" che sono in grado di identificare e spesso rimuovere, o comunque rendere inoffensivi, la maggior parte dei virus circolanti in rete.

Sicuramente un buon antivirus deve avere un buon motore di scansione, in grado di effettuare una scansione approfondita, che riesca a rilevare e segnalare la presenza di eventuali codici sospetti.

Le principali funzioni di un antivirus sono quelle di scansione dei file del disco rigido in tempo reale, scansione di periferiche esterne, della memoria, del registro e anche della posta elettronica (con scansione completa degli allegati e della posta indesiderata).

L'antivirus deve essere anche in grado di classificare i file infetti in base alla dannosità ed evidenziare gli eventuali elementi che non è riuscito ad esaminare.
I file infetti interessati vengono automaticamente e direttamente eliminati dall'antivirus che, inoltre offre la possibilità di metterlo in quarantena, per monitorare eventuali movimenti sospetti o isolare completamente il file.

Per rendere la protezione del personal computer ottimale è buona norma accompagnare l'antivirus ad un buon firewall.



Ma che cos'è un **<u>firewall</u>**?

Sono una risorsa software o hardware che controlla le informazioni provenienti da Internet o da un altro tipo di rete, bloccandole o consentendone l'accesso al computer, a seconda delle opzioni impostate.
Usando una metafora è come se questi dispositivi rappresentassero i punti di un muro: la loro funzione principale è quella di agire come dei filtri controllando tutto il traffico di rete che proviene dall'esterno, nonché quello che viene generato dall'interno, e permettendo soltanto quel traffico che risulta effettivamente autorizzato.
L'obiettivo di questo tipo di programmi e' quello di controllare il flusso di informazioni che partono ed arrivano al computer per verificare se le informazioni scambiate seguono o meno criteri

legittimi. Non appena una comunicazione esce da questi criteri il firewall entra in azione e consente di scegliere se bloccare o meno un particolare scambio di dati.
Sorveglia, inoltre, tutte le operazioni durante una connessione avvisando quando, ad esempio, un sito su cui si sta navigando tenta di accedere ad informazioni sensibili, come l'indirizzo di posta elettronica, i documenti personali archiviati sul computer, le password ed altri dati riservati.
I firewall più evoluti permettono anche di selezionare le informazioni da proteggere che risultano essere prioritarie rispetto ad altre , come il numero della carta di credito, le proprie password eccetera. La conseguenza è che quando si tenta di inviare queste informazioni ad un sito che non offre adeguate garanzie (ad esempio non utilizza un livello sufficiente di cifratura dei dati) il firewall avverte della situazione permettendo di operare una scelta.