

Modulo 1 – Computer Essentials

Lezione 6 - Sicurezza e benessere

*In questa lezione si impareranno le tecniche di **Protezione dei dati su computer e dispositivi elettronici** (6.1), cioè a riconoscere politiche corrette per le password, quali crearle di lunghezza adeguata, con un'adeguata combinazione di caratteri, evitare di condividerle, modificarle con regolarità. (6.1.1), a definire il termine firewall e identificarne gli scopi (6.1.2), a comprendere lo scopo di creare con regolarità copie di sicurezza remote dei dati (6.1.3), a comprendere l'importanza di aggiornare regolarmente i diversi tipi di software, quali anti-virus, applicazioni, sistema operativo (6.1.4), a riconoscere il **Malware** (6.2), cioè a definire il termine "malware", identificare diversi tipi di malware, quali virus, worm, trojan, spyware (6.2.1), a sapere come un malware può infettare un computer o un dispositivo (6.2.2), ad usare un software antivirus per eseguire una scansione in un computer (6.2.3), a curare la **Tutela della salute e "informatica verde"** (6.3), cioè a sapere quali sono i principali modi per assicurare il benessere di un utente durante l'uso di un computer o di un dispositivo, quali effettuare pause regolari, assicurare una corretta illuminazione e postura (6.3.1), a conoscere le opzioni di risparmio energetico che si applicano ai computer e ai dispositivi elettronici: spegnimento, impostazione dello spegnimento automatico, dell'illuminazione dello schermo, della modalità di sospensione (6.3.2), a sapere che i computer, i dispositivi elettronici, le batterie, la carta, le cartucce e i toner delle stampanti dovrebbero essere riciclati (6.3.3), ad identificare alcune delle opzioni disponibili per migliorare l'accessibilità, quali software di riconoscimento vocale, screen reader, zoom, tastiera su schermo, contrasto elevato (6.3.4).*

6.1 Protezione dei dati su computer e dispositivi elettronici

6.1.1 Riconoscere politiche corrette per le password, quali crearle di lunghezza adeguata, con un'adeguata combinazione di caratteri, evitare di condividerle, modificarle con regolarità.

Abbiamo già parlato in precedenza dell'utilizzo della password, ossia di un codice segreto che certifica l'autenticità dell'utente di risorse hardware e software e di informazioni e dati protetti.

L'efficacia della password è strettamente legata alla sua segretezza, e quindi agli opportuni accorgimenti da prendere perché non venga scoperta. Innanzitutto la password deve essere personale e non condivisa con altri utenti. Deve essere memorizzata dal proprietario e non devono esistere copie scritte. Perché questo sia possibile occorre che sia di media lunghezza, non troppo lunga in modo che il proprietario la possa ricordare e nello stesso tempo non troppo corta perché non sia facile da individuare per tentativi. Non deve essere prevedibile, pertanto non deve fare riferimento a dati personali che possono essere conosciuti facilmente (esempio nome dell'utente, data di nascita, targa della vettura, ecc.). E' opportuno che sia formata da combinazioni di cifre e lettere dell'alfabeto, possibilmente maiuscole e minuscole.

Inoltre è bene che venga cambiata con frequenza e che la nuova chiave non abbia un legame logico con la precedente (esempio 456701, 456702, 456703, ecc.).

Alcuni programmi e siti Internet permettono di attivare l'inserimento automatico della password, quando viene digitato l'identificativo utente. Utilizza questa possibilità solo se sei sicuro che il computer è di tuo utilizzo esclusivo e non è accessibile ad altri, o quando il programma o il sito non forniscono informazioni e servizi che devono essere protetti.

Quando digiti la password, quanto scrivi viene mascherato con una serie di asterischi, in modo che non possa essere letto da estranei. Tutto ciò funziona se hai l'accorgimento di evitare di essere visto quando premi i tasti della tastiera.

6.1.2 Definire il termine firewall e identificarne gli scopi.

Si è già detto che Internet è diventato non più solo uno strumento per fornire informazioni e servizi di pubblico accesso, ma anche un canale di comunicazione a basso costo per accedere al sistema informativo delle aziende da locazioni

remote. Nasce quindi l'esigenza di riconoscere gli utenti che si connettono al sito Internet aziendale, dando l'accesso alle informazioni e ai servizi interni all'azienda solo agli utenti autorizzati.

Lo stesso problema si può avere a livello personale se si vogliono proteggere i propri dati riservati da accessi non voluti via Internet.

La soluzione a questo problema è il firewall (in italiano porta tagliafuoco), cioè un software, in alcuni casi installato su un sistema informatico dedicato, che controlla il traffico tra Internet e i sistemi aziendali, impedendo gli accessi non autorizzati.

Il sistema funziona in ingresso, bloccando le richieste di utenti non abilitati, e in uscita, impedendo il collegamento a determinati siti esterni.

In definitiva, il firewall difende il proprio sistema da accessi indesiderati provenienti dalla rete e impedisce l'accesso a siti che non si vuole siano accessibili.

Di fatto viene creato un filtro sul traffico entrante ed uscente, garantendo un buon livello di sicurezza, mediante operazioni di controllo, di verifica ed eventualmente di modifica sui pacchetti gestiti dal protocollo di Internet.

Il firewall può essere inserito tra la rete Internet ed il sistema informatico interno all'azienda, ma, per aumentare il livello di sicurezza, viene normalmente posto tra il sito Web aperto a tutti gli utenti ed i sistemi informatici che gestiscono le applicazioni accessibili agli utenti autorizzati.

6.1.3 Comprendere lo scopo di creare con regolarità copie di sicurezza remote dei dati.

Abbiamo già detto che per conservare i dati in modo permanente li memorizziamo nelle memorie di massa; questi dati potrebbero però essere danneggiati in caso di malfunzionamento di un programma, di guasti di un dispositivo, o di danneggiamento fisico dell'intero computer, come nel caso di incendi, inondazioni, terremoti.

Inoltre gli archivi possono essere rovinati da accessi fraudolenti e da virus informatici.

Per evitare di perdere i dati è necessario fare delle copie di sicurezza, copie di backup, su altre memorie ausiliarie rimovibili, quali chiavette USB, CD, DVD, hard disk esterni, da conservare in luoghi sicuri, quali ad esempio armadi ignifughi.

Nel caso di reti, i singoli utenti possono salvare i propri dati sui dischi dei server di rete, sistemi che forniscono servizi agli utenti della rete, mentre è compito del gestore della rete effettuare il salvataggio dei dischi del server.

A fronte di eventi catastrofici, è opportuno che le copie di backup non siano conservate nello stesso luogo o in prossimità degli archivi originali, in quanto potrebbe andare distrutte insieme a questi. Il massimo livello di sicurezza si ha quando il backup viene effettuato sulle memorie di massa di un server remoto, trasferendo i dati tramite la rete.

Al verificarsi di danni agli archivi originali vengono ripristinati i dati, prelevandoli dalle copie di backup; saranno stati persi solo gli aggiornamenti effettuati dopo l'ultima operazione di salvataggio.

Oltre ai dati è importante salvare anche il software, tutte le volte che viene modificato.

Periodicamente è utile anche effettuare il cosiddetto "backup di sistema", consistente nella copia dell'intero hard disk.

Non esistono regole rigide sulla frequenza dei salvataggi; il buon senso dice che è bene farlo ogni volta che le variazioni dei dati sono significative. In una grande azienda il salvataggio deve essere almeno quotidiano, ma spesso viene anche fatto più volte al giorno; in una piccola impresa è certamente più frequente un backup giornaliero o settimanale.

Il backup può essere completo o incrementale. Quello completo, come dice il nome, salva tutti i dati, anche quelli non modificati; quello incrementale invece salva solo quelli modificati dopo la data dell'ultimo salvataggio.

E' evidente che il secondo ha un peso e una durata inferiori rispetto al primo, ma mentre il ripristino con un backup completo implica di caricare semplicemente il salvataggio stesso, il ripristino da backup incrementale richiede il caricamento di un backup completo e l'aggiornamento con tutti i successivi backup incrementali fino al momento del danno.

Le regole di sicurezza che abbiamo enunciato nei punti precedenti non riguardano solo le aziende, ma anche i privati che ormai detengono tutti, in una forma o in un'altra, dei dati per loro importanti.

Inoltre, le apparecchiature portatili sono per loro natura meno protette di quelle che si trovano in locali non accessibili a tutti.

Per chi utilizza portatili o tablet è importante effettuare periodici backup dei dati, in modo che, in caso di smarrimento o di furto dell'apparecchiatura, almeno non vadano persi anche tutti gli archivi.

6.1.4 Comprendere l'importanza di aggiornare regolarmente i diversi tipi di software, quali anti-virus, applicazioni, sistema operativo.

L'hardware di un computer o di un dispositivo portatile è progettato e realizzato per avere l'assoluta garanzia di non dare risultati errati. Per ottenere tale risultato, all'interno sono inseriti dispositivi di controllo, che garantiscono la correttezza del funzionamento; a fronte di un guasto il computer si blocca, ma non dà risultati errati.

Se una elaborazione dovesse dare dei risultati sbagliati, questi sono dovuti al software, che, invece, non è esente da errori, soprattutto quando è particolarmente complesso.

Per questo il software è sottoposto ad un continuo aggiornamento, i cui risultati portano ad avere versioni successive dello stesso programma.

Le nuove versioni contengono le correzioni degli errori riscontrati sino a quel momento e, talvolta, l'aggiunta di nuove funzioni in risposta a nuove esigenze. Nasce quindi la necessità di tenere aggiornato in continuazione il software, sia quello applicativo che quello di sistema.

Un discorso a parte va fatto per i programmi antivirus, di cui parleremo tra poco. Gli aggiornamenti, in questo caso, devono saper riconoscere i nuovi virus, che vengono realizzati in continuazione, per cui un programma per la protezione contro i virus risulta inefficace se non viene aggiornato tempestivamente.

6.2 Malware

6.2.1 Definire il termine "malware". Identificare diversi tipi di malware, quali virus, worm, trojan, spyware.

Ormai anche i non addetti ai lavori hanno sentito parlare dei cosiddetti "virus informatici", anche perché con una certa frequenza si trovano articoli allarmistici, anche sui quotidiani.

In realtà il termine è improprio, sarebbe più corretto parlare di malware, in quanto i virus sono solo uno dei possibili tipi di questo software. Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e questo è in parte dovuto al fatto che i programmi antivirus proteggono anche da altre categorie di software maligno, oltre ai virus propriamente detti.

Il malware è un software realizzato e diffuso con lo scopo di recare danni più o meno permanenti ad un computer o anche ad un dispositivo elettronico o di acquisire dati riservati, quali identificativi utente e password, da utilizzare in modo fraudolento. Il termine deriva dalle parole inglesi malicious e software e ha dunque il significato letterale di "programma maligno".

Alcuni di questi programmi sono abbastanza innocui: si limitano a far comparire scritte o immagini sullo schermo, ma altri possono giungere a danneggiare in modo irreparabile i dati e i programmi contenuti nelle memorie di massa del computer.

Si distinguono parecchie categorie di malware, anche se spesso questi programmi sono composti di più parti con caratteristiche diverse, per cui rientrano in più di una tipologia.

I tipi più comuni sono i virus, i worm, i Trojan horse, gli spyware.

I virus sono serie di istruzioni, normalmente di piccole dimensioni, che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da attivarsi ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti. Quando un virus contagia un programma ospite, inserisce all'inizio del programma un'istruzione che rinvia alle operazioni del virus, alla fine delle quali è posta una istruzione che rinvia all'inizio del programma infettato. In questo modo, l'utente vede la normale esecuzione del programma richiesto e non si accorge delle operazioni eseguite dal virus. Una sottocategoria è costituita dai macro virus, che possono inserirsi, ad esempio, nei programmi della suite di Office, nella forma di macro, cioè sequenze di istruzioni che possono essere previste, ovviamente per altri scopi, nei programmi Word, Excel, Access e Power Point. In questi casi la difesa è semplice, in quanto all'apertura del programma l'utente viene avvisato della presenza di macro e gli viene chiesta l'autorizzazione per eseguirle. Se non si è certi che il documento debba contenere macro per elaborazioni previste, è sufficiente non autorizzare la loro esecuzione.

L'attivazione del virus, come abbiamo detto, avviene quando viene eseguito il programma infetto, ma le conseguenze possono essere immediate, all'esecuzione di un particolare comando, o a data stabilita. I danni provocati possono essere danneggiamento o cancellazione di programmi o di archivi, esecuzione di operazioni non previste, segnalazione di guasti inesistenti, rallentamento delle prestazioni.

I worm (vermi) infettano direttamente il sistema operativo, modificandolo, e si attivano automaticamente e, per diffondersi, sfruttano normalmente la posta elettronica. L'azione più comune dei worm è quella di cambiare l'indirizzo del mittente, creando dei falsi messaggi. Il programma antivirus è in grado di riconoscerli e di respingere il messaggio infetto, ma l'informazione non può essere inoltrata al mittente, in quanto il suo indirizzo è stato modificato dal worm. Il principale effetto di questo contagio è quello di una diminuzione delle prestazioni del sistema a causa di operazioni inutili o anche dannose.

I trojan horse (cavalli di Troia) devono il loro nome al fatto che il software maligno si nasconde in un programma che svolge funzioni interessanti per l'utente, che viene allettato in questo modo ad installare ed eseguire il programma, e quindi le istruzioni dannose.

Lo spyware (software spia) è un programma che permette di accedere a dati riservati e di trasmetterli a chi ha attivato il contagio. Le informazioni così raccolte possono essere più o meno pericolose: in alcuni casi riguardano i siti e le pagine Internet visitati dall'utente, e risultano utili per operazioni di marketing, altre volte vengono trasmessi i codici utente e le password o le chiavi crittografiche dell'utente, dando quindi la possibilità di accesso ad informazioni riservate. I programmi di tipo spyware non si replicano automaticamente, ma solo se vengono installati ed eseguiti i programmi che hanno contagiato.

6.2.2 Sapere come un malware può infettare un computer o un dispositivo.

I due più frequenti sistemi di contagio da malware sono le memorie di massa mobili, quali CD, DVD, penne USB e hard disk esterni e la posta elettronica. In entrambi i casi il contagio avviene con la lettura di file infetti.

Oltre all'utilizzo di un programma antivirus aggiornato, per difendersi può essere utile adottare alcuni accorgimenti.

Non scaricare file di cui non sai la funzione e la provenienza, in particolare diffida dai siti web non conosciuti; nel caso avvenga il download automatico di un file non richiesto, elimina subito il file.

Verifica il nome degli allegati dei messaggi di posta elettronica, ed elimina quelli con doppia estensione (tipo prova.txt.doc).

Verifica i file con estensione .exe e .com, perché sono autoeseguibili e quindi si attivano senza un tuo comando.

Fai attenzione agli allegati inattesi, che ad esempio non sono citati nel messaggio di posta elettronica, potrebbero essere file infetti, inseriti all'insaputa del mittente.

Con una certa frequenza arrivano messaggi apparentemente da siti ai quali accedi per informazioni e servizi riservati; questi messaggi normalmente dichiarano che sono scadute le tue credenziali, identificativo utente e password, e ti chiedono di collegarti ad un indirizzo inserito nel messaggio; fai attenzione, si tratta di tecniche per catturare i tuoi dati di accesso.

Se ricevi messaggi con notizie allarmanti da aziende informatiche molto note, che ti invitano a diffondere il messaggio ai tuoi interlocutori, quasi sempre si tratta di messaggi falsi, che hanno l'obiettivo di sovraccaricare la rete, degradandone le prestazioni.

6.2.3 Usare un software antivirus per eseguire una scansione in un computer.

L'unica protezione veramente efficace è l'uso di un buon antivirus, il suo aggiornamento continuo e la verifica dei file prima della loro esecuzione. Questa avvertenza è valida anche nel caso di scambio di CD-ROM, DVD, pendrive, dischi rimovibili con altri utenti.

Infine è importante tener presente che i file come i documenti di Word ed Excel possono contenere programmi maligni che si attivano all'apertura dei documenti stessi. Anche in questo caso l'unico modo per accertarsi che i file non siano infetti è quello di dotare il proprio sistema di un software antivirus.

L'antivirus è un programma in grado di riconoscere il malware e di eliminarlo o isolarlo, mettendolo in quarantena, quando l'eliminazione non risulta possibile. Per maggior sicurezza è opportuno che il programma antivirus sia tenuto sempre attivo, in modo che svolga un controllo continuo sulle attività svolte, e che venga aggiornato in continuazione, perché sia in grado di riconoscere anche il malware di nuova produzione. E' infatti importante che si riesca a isolare il malware prima che possa produrre danni.

Non sempre questo è possibile, soprattutto a fronte di nuovi malware, e si scopre di essere stati infettati proprio perché se ne riscontrano gli effetti. E', quindi, opportuno effettuare periodicamente una "scansione del sistema"; in questo modo l'antivirus rileva la presenza di software infetti e cerca di cancellare il codice virale che vi è stato aggiunto (disinfezione); se l'operazione non riesce, il programma consiglia all'utente di rimuovere integralmente i file infetti (o di metterli in "quarantena") per evitare il propagarsi dell'infezione.

Inoltre è utile disporre di un piano di backup, da utilizzare frequentemente, per essere sicuri di non perdere archivi e programmi nel caso di infezione.

Per effettuare la scansione del sistema, apri il menu “Start” con il tasto WINDOWS e con FRECCIA GIU’ seleziona “Tutti i programmi”. Con FRECCIA DESTRA apri il sottomenu “Programmi” e con FRECCIA GIU’ seleziona il programma antivirus che hai installato. Può darsi che la funzione per avviare il programma sia in un ulteriore sottomenu, in tal caso spostati con FRECCIA DESTRA. Quando hai selezionato l’antivirus premi INVIO. Si apre una finestra che normalmente riporta due date fondamentali, quella dell’ultima scansione e quella dell’ultimo aggiornamento. Prima di avviare la scansione, normalmente è possibile selezionare due opzioni; con l’opzione interattiva ad ogni codice infetto trovato il programma ti chiede come procedere, con l’opzione automatica i risultati vengono riportati in un rapporto finale, che indica quanti interventi sono stati effettuati direttamente dal programma e ti chiede di decidere come procedere su ogni singolo problema non risolto. Segui le indicazioni della finestra per avviare la scansione. Il programma mostra il procedere dell’operazione. Per ogni file messo in isolamento, ti viene chiesto di decidere se riattivarlo o eliminarlo definitivamente.

I programmi antivirus sono molto efficaci, ma non possono garantire una protezione totale. Non è però utile effettuare la verifica con più programmi antivirus, in quanto, solitamente un antivirus vede l’altro come malware e segnala la presenza di un’infezione che in realtà non esiste.

6.3 Tutela della salute e “informatica verde”

6.3.1 Sapere quali sono i principali modi per assicurare il benessere di un utente durante l’uso di un computer o di un dispositivo, quali effettuare pause regolari, assicurare una corretta illuminazione e postura.

I computer sono diventati uno strumento insostituibile nelle attività quotidiane, in ufficio e a casa. E’ quindi elevato il numero di ore che ognuno di noi passa davanti ad una tastiera ed uno schermo; da qui è derivata la necessità di verificare e tutelare con apposite leggi la salute dell’utente degli strumenti informatici.

Per tale scopo si è sviluppata l’ergonomia, cioè la disciplina che studia l’interazione tra la tecnologia e l’individuo, per migliorarne le condizioni di lavoro.

Per gli utenti di strumenti informatici i fattori da considerare sono il livello di benessere, la facilità di utilizzo e la sicurezza.

Il livello di benessere riguarda, in particolare, le caratteristiche del posto di lavoro e la sua corretta illuminazione.

Un posto di lavoro ergonomico deve garantire all’utente una postura corretta.

L’altezza del piano di lavoro deve permettere di appoggiare gli avambracci nell’utilizzo della tastiera e del mouse e di avere spalle rilassate durante la digitazione. La tastiera deve essere spostabile e il mouse deve essere vicino il più possibile al corpo ed è bene utilizzare un tappetino.

Il sedile deve essere con cinque rotelle, per favorirne la mobilità e la stabilità, dotato di braccioli, regolabile in altezza e con schienale regolabile. Deve consentire una postura con angoli dei gomiti, fianchi e gambe superiori a 90 gradi; piedi ben poggiati a terra o, se necessario, su poggipiedi ampio.

Il video deve essere posizionato davanti all’utente, per evitare torsioni di schiena e collo, con bordo superiore all’altezza degli occhi, ad una distanza che consenta la corretta lettura dello schermo, dovrebbe essere regolabile in inclinazione e direzione, grazie ad una base orientabile; è opportuno che l’utente ne regoli le dimensioni dei caratteri, la luminosità e il contrasto, secondo le sue esigenze.

Per quanto riguarda l’illuminazione, è necessario che la fonte di luce non sia alle spalle o di fronte al video, se è necessario occorre ridurre l’intensità delle lampade o schermare le finestre, e ridurre i riflessi, individuati più facilmente con una verifica a video spento.

Un posto di lavoro non ergonomico può causare una serie di problemi fisici, quali dolori alla schiena o muscolari, affaticamento della vista, stanchezza ed emicrania.

Nel caso di attività prolungata, che può causare stress, è necessario fare pause di lavoro, tendenzialmente un quarto d’ora ogni due ore.

Sono poi consigliabili esercizi per il rilassamento muscolare e per la vista, che viene affaticata se per troppo tempo viene guardato un oggetto a distanza fissa.

Ulteriori precauzioni riguardano la sicurezza del posto di lavoro. Occorre che l'impianto elettrico sia a norma e in buone condizioni, si deve evitare di sovraccaricare i collegamenti con spine multiple, ricorrendo in caso di necessità a ciabatte dotate di interruttore, si devono disporre le apparecchiature in luoghi lontani da fonti di calore e umidità. In questo modo si possono evitare spegnimenti del computer originati da problemi elettrici o anche principi di incendio.

6.3.2 Conoscere le opzioni di risparmio energetico che si applicano ai computer e ai dispositivi elettronici: spegnimento, impostazione dello spegnimento automatico, dell'illuminazione dello schermo, della modalità di sospensione.

Uno dei grandi problemi della società moderna è il consumo energetico. Alla soluzione di questo problema anche tu puoi dare un piccolo contributo con alcuni accorgimenti nell'utilizzo del computer e dei dispositivi elettronici. Innanzitutto usa apparecchi a basso consumo energetico e spegni il computer quando pensi di non utilizzarlo per un po' di tempo.

Attiva le funzioni di sospensione automatica del computer e dell'autospegnimento del video, durante le pause, e di passaggio automatico allo stato di attesa della stampante, quando non è operativa.

Un livello di risparmio energetico è normalmente preimpostato sul tuo computer. Per poter vedere tale impostazione ed eventualmente modificarla, premi il tasto WINDOWS per aprire il menu Start, premi poi FRECCIA DESTRA per passare alla parte destra della finestra e con FRECCIA GIU' o "P" seleziona "Pannello di controllo" e premi INVIO. Nella finestra che si apre, con le frecce seleziona "Opzioni risparmio energia" e premi INVIO. Nella nuova finestra premi TAB sino a raggiungere il riquadro di destra. Con FRECCIA GIU' o FRECCIA SU puoi selezionare una delle due voci alternative, "Bilanciato (scelta consigliata)" e "Prestazioni elevate"; Il pulsante "Mostra combinazioni aggiuntive" consente di vedere anche l'opzione "Risparmio energetico". Per attivare una scelta, selezionala e premi il tasto SPAZIO.

Puoi inoltre modificare i tempi impostati per l'attivazione della funzione. Dopo aver impostato la scelta, con FRECCIA DESTRA vai al pulsante "Modifica impostazioni combinazione" e premi INVIO. Nella nuova finestra vai con TAB alla casella "Disattivazione schermo" e se vuoi cambia i tempi di disattivazione con FRECCIA GIU' o SU. Con TAB vai a "Sospensione computer" e se vuoi cambia i tempi con FRECCIA GIU' e SU. Infine con TAB vai al pulsante "Salva cambiamento" e premi INVIO.

Torna alla finestra precedente, che puoi chiudere con ALT + F4.

Tieni presente che con l'opzione "Bilanciato (scelta consigliata)" il sistema bilancia automaticamente le prestazioni ed il consumo di energia, con la scelta "Risparmio di energia" l'obiettivo è il risparmio di energia riducendo le prestazioni, quando ciò è possibile, mentre con "Prestazioni elevate" si privilegia la prestazione rispetto al risparmio energetico.

Il problema del risparmio energetico è sentito in particolare sui computer e dispositivi portatili, alimentati dalla batteria, che potrebbero esaurire la loro carica in momenti poco opportuni.

6.3.3 Sapere che i computer, i dispositivi elettronici, le batterie, la carta, le cartucce e i toner delle stampanti dovrebbero essere riciclati.

Un altro problema molto sentito, nella società attuale, è lo smaltimento dei rifiuti ed in particolare di quelli tossici.

Per i materiali di scarto, quali carta stampata, batterie esaurite, computer e dispositivi elettronici non più utilizzati, la soluzione è il loro corretto smaltimento, in modo che possano essere riciclati. L'operazione è favorita dal fatto che nella costruzione delle apparecchiature moderne è aumentato l'uso di materiali facilmente riciclabili.

Per la carta da stampa si può utilizzare la carta riciclata, stampare anche sul retro del foglio, e usare la documentazione elettronica invece dei manuali cartacei.

Per materiali di consumo quali cartucce d'inchiostro e toner, si può procedere alla loro ricarica, invece della sostituzione.

6.3.4 Identificare alcune delle opzioni disponibili per migliorare l'accessibilità, quali software di riconoscimento vocale, screen reader, zoom, tastiera su schermo, contrasto elevato.

I computer si sono anche rivelati fondamentali nel migliorare l'accessibilità alle informazioni e alle comunicazioni per molte persone con disabilità, grazie ad alcuni software specializzati o anche a funzioni di software standard.

I programmi screen reader possono identificare e interpretare il testo visualizzato su uno schermo video, e comunicarlo a un utente non vedente mediante sintesi vocale o display braille.

La funzione di ingrandimento dello schermo, zoom, può aumentare le dimensioni dei caratteri e delle immagini, facilitandone la visione a utenti ipovedenti;

I programmi di riconoscimento vocale consentono di interpretare il linguaggio orale, dando la possibilità a chi non può usare la tastiera di dettare testi o di impartire comandi al computer.

La funzione di tastiera sullo schermo permette di introdurre i caratteri mediante una tastiera simulata sullo schermo di tipo touchscreen.

Abbiamo detto che alcune di queste funzioni fanno parte dei programmi standard. Ad esempio i programmi della suite Office dispongono della funzione di zoom, ed anche sul desktop e nelle cartelle gestite da Windows è possibile l'ingrandimento delle icone.

Inoltre in Windows, nella schermata iniziale, nella quale è possibile selezionare l'utente del sistema, è presente, in basso a sinistra, il pulsante "Accessibilità". Tale funzione è anche disponibile nel "Pannello di controllo" sotto la voce "Centro accessibilità".

Se usi il pulsante della schermata iniziale, quando sei posizionato in tale videata, raggiungi con TAB il pulsante "Accessibilità" e premi INVIO.

La finestra mostra una serie di funzioni di aiuto, che presentano una casella di spunta, seleziona la funzione con FRECCIA SU e GIU' e per attivarla premi il tasto SPAZIO. In modo analogo procedi se vuoi disattivare la funzione attivata.

Vediamo qui di seguito le funzioni disponibili:

- Ascolta lettura del testo sullo schermo (Assistente vocale).

- Ingrandisci gli elementi sullo schermo (Lente di ingrandimento).

- Aumenta contrasto dei colori (Contrasto elevato).

- Digitare senza tastiera (Tastiera su schermo).

- Premi tasti di scelta rapida un tasto alla volta (Tasti permanenti).

- Se i tasti vengono premuti ripetitivamente, ignora le pressioni ripetute dei tasti (Filtro tasti).

Con queste informazioni è terminata la lezione 6° che è anche l'ultima di questo modulo.

Spero di averti fatto appassionare al computer e alle sue grandi possibilità.