Manuale di sicurezza per gli utenti

Non spostare le apparecchiature assegnate. L'utente non è autorizzato in alcun modo ad effettuare spostamenti o cambi delle postazioni ad esso assegnate, di cui è il diretto responsabile. Nel caso di mal funzionamento di un'apparecchiatura (i.e. stampanti, monitor) l'utente è tenuto a segnalare, con le modalità previste, il guasto alla ditta di assistenza tecnica che provvederà ad effettuare l'intervento di riparazione. Nel caso di necessari spostamenti dovuti a particolari esigenze è tenuto ad informare il consegnatario Economo dell'Ufficio di appartenenza, il quale dovrà informare tempestivamente il Servizio di Assistenza Tecnica Unificata per apportare le modifiche alle banche dati dell'inventario.

Chiudere a chiave cassetti ed uffici. Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti ogni volta che potete.

Spegnere il computer se ci si assenta per un periodo di tempo lungo. Lasciare un computer acceso non crea problemi al suo funzionamento ed al contrario velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

Non lasciare lavori incompiuti sullo schermo. Chiudete sempre le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro per più di pochi minuti: potreste rimanere lontani più del previsto, e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

Salvaschermo. Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

Proteggere attentamente i dati. Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

Conservare supporti di memoria e stampe in luoghi sicuri. Alla conservazione dei supporti di memoria (CD, dischetti) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

Maneggiare e custodire con cura le stampe di materiale riservato. Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.

Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali. Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una macchina distruggi-documenti (shredder). In ogni caso non gettate mai documenti cartacei senza averli prima fatti a pezzi.

Non riutilizzare i dischetti per affidare a terzi i vostri dati. Quando un file viene cancellato da un disco magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

Prestare particolare attenzione all'utilizzo dei computer portatili. I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sul BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed effettuate periodicamente il back-up.

Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso. Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password. La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

Non permettere l'uso del proprio computer o del proprio account da personale esterno, a meno di non essere sicuri della loro identità. Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

Non utilizzare apparecchiature non autorizzate o per cui non si è autorizzati. L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutta la rete di cui fate parte. E' quindi vietato l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio all'amministratore di sistema.

Installare programmi non autorizzati. Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

Diffidare dei dati o dei programmi la cui provenienza non è certa. Per proteggersi di virus ed altri agenti attivi di attacco, diffidate di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante. Infatti molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

Applicare con cura le linee guida per la prevenzione da infezioni da virus. La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure anti-virus potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro.

Usare, se possibile, il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari. Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.

Non violare le leggi in materia di sicurezza informatica. Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se siete interessati a studiare la sicurezza della vostra postazione di lavoro o della rete di cui fate parte, chiedete preventivamente l'autorizzazione al Responsabile della sicurezza del singolo Ufficio. Non utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro perché può essere il sintomo di un attacco in corso.

Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo. Ad esempio segnalate al Responsabile della sicurezza dell'Ufficio se un altro utente insiste per avere accesso ai vostri dati o per conoscere la vostra password o per poter lavorare sulla vostra postazione di lavoro. Analogamente non fidatevi e segnalate telefonate o messaggi che sembrano provenire da un sistema e vi chiedono di fare operazioni strane sul vostro computer (ad esempio, cambiare subito la password con una datavi al telefono o nel corpo del messaggio).