Precauzioni per la privacy "informatica"

Dal sito del SIAF (Sistema Informatico dell'Ateneo Fiorentino) – modificata

Precauzioni nell'utilizzo della posta elettronica

- evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT (a meno che non attesi e provenienti da mittente conosciuto e di fiducia)
- se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail
- nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti
- evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "*worm*"
- configurare il programma di posta elettronica in modo tale che non esegua automaticamente gli allegati.

Gestione delle credenziali

Scelta della password

- la password deve essere composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: & @ ? % £ $);
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- la password deve essere facile da ricordare per l'utente.

Cautele per la segretezza della password

- non comunicare ad altri le proprie credenziali di accesso e le password
- mantenere e custodire le proprie *password* con la dovuta riservatezza**;**
- evitare di scrivere le proprie *password* su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave;
- nel digitare sulla tastiera la password, prestare attenzione ad eventuali sguardi indiscreti
- evitare di "salvare" la password sul computer, come proposto dal sistema operativo
- modificare immediatamente la password nel caso sia stato necessario fornire le credenziali ai tecnici intervenuti per la manutenzione del computer o del software

Modifica della password

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo log-on);
- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- in caso di trattamento di dati sensibili (es. dati personali inerenti lo stato di salute) e giudiziari la password deve essere modificata almeno ogni tre mesi.

Precauzioni nella gestione della postazione di lavoro informatica.

Se devo allontanarmi momentaneamente dal mio computer	Evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro che comporti trattamento di dati personali: bloccare manualmente il computer oppure **attivare il blocco automatico** dopo 5 minuti di inattività. Lo sblocco dello screen saver deve avvenire tramite le credenziali di accesso e non tramite la semplice pressione di un tasto.
Al termine della sessione di lavoro se sono connesso ad un server	Effettuare la procedura di disconnessione ("logoff"/"logout"/"esci") e NON semplicemente bloccare il computer.
Al termine della sessione di lavoro sul mio computer	Effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare lo studio.
Quando eseguo operazioni a video sulla cartella del paziente	Posizionare il video in modo che non possa essere visto da persone che non autorizzo.
Se, allo spegnimento del computer, sta scaricando degli aggiornamenti	Aspettare che li abbia completamente scaricati ed installati, in modo da essere certi dello spegnimento dello stesso.