Confagricoltura Padova

Le buone pratiche per la sicurezza informatica

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.);
- 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 stessa password non deve essere riutilizzata per almeno quattro anni;
- la password deve essere facile da ricordare per l'utente;

Cautele per la segretezza della password

- utilizzare sempre esclusivamente le proprie credenziali di autenticazione;
- non condividere la propria password con altre persone;
- non usare la password del proprio account mail come password di registrazione a siti internet e/o servizi che richiedono la fornitura dell'indirizzo mail come account.
- 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
- comunicare tempestivamente al responsabile o all'amministratore di sistema eventuali dubbi sulla segretezza della password
- 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

Difendersi dal phishing

- non digitare le proprie credenziali su siti web raggiunti tramite link presenti su messaggi e-mail o altri documenti
- non aprire messaggi di posta provenienti da utenti sconosciuti o sospetti
- non comunicare la propria password a nessuno, nemmeno all'amministratore di sistema

Modifica della password

- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- modificare la password di accesso alle applicazioni utilizzate per il trattamento di dati personali almeno ogni sei mesi;

- 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;

Il custode delle credenziali
All'interno di ogni ufficio è buona pratica individuare uno o più custodi delle credenziali che hanno il compito di conservare, in luogo sicuro (armadio o cassetto chiuso a chiave, cassaforte, ecc.), le credenziali del personale afferente alla struttura. Le credenziali da conservare possono essere quelle di accesso agli applicativi centralizzati, ma anche quelle per l'accesso al proprio computer o alla propria casella di posta elettronica.

Gestione delle stazioni di lavoro

Custodia della stazione di lavoro
- evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro che comporti trattamento di dati personali;
- proteggere la stazione di lavoro attraverso cui si accede a sessioni di trattamento di informazioni riservate, utilizzando o key locks, password di qualità o screen saver (da attivare su richiesta o dopo un tempo prestabilito di inattività), nel caso in cui ci si assenti temporaneamente dall'ufficio;
- al termine della sessione di lavoro sui server centrali, effettuare la procedura di disconnessione ("logoff"/"logout"/"esci") ;
- al termine della sessione sulla stazione di lavoro, effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare l'ufficio;
- effettuare (almeno una volta alla settimana) il backup dei dati e documenti essenziali presenti sulla propria stazione di lavoro su server esterni, su CD o altro supporto esterno dedicato a questo scopo e opportunamente protetto.

Prevenzione dei virus informatici nelle postazioni
- installare almeno un software antivirus
- configurare la protezione permanente e l'aggiornamento automatico via rete;
- verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine
- utilizzare il software rispettando le istruzioni del fornitore
- verificare, tramite adeguato programma antivirus, i file, il software e i dispositivi di memorizzazione rimovibili (hard disk esterni, chiavette USB, ecc.) provenienti dall'esterno, prima del loro utilizzo
- configurare il sistema operativo affinché sia possibile visualizzare l'estensione dei file: tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure "logo.jpg.exe")
- ripulire immediatamente le stazioni che si rivelino o vengano segnalate come infette;
- segnalare tempestivamente al servizio informatico qualsiasi presenza di virus sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni
- nello scaricare dalla rete Internet programmi (es. software open source; freeware, shareware ecc.) e documenti (testi e tabelle che possono contenere dei "virus macro") necessari allo svolgimento della propria attività lavorativa, utilizzare unicamente i siti delle case produttrici dei medesimi o i link che esse stesse propongono sul loro sito

Prevenzione dei virus informatici 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.

Telefoni

Sono considerati strumenti informatici che possono dare accesso ad informazioni riservate o strategiche. E' bene quindi:

- non lasciare il telefono a disposizione di persone estranee
- valutare l'opportunità di inserire il lucchetto elettronico all'uscita dal lavoro o in caso di assenza prolungata
- non comunicare il codice per la gestione della segreteria telefonica e per lo sblocco del telefono a persone estranee

Stampanti

Se si dispone di stampanti di rete o condivise:

- ritirare immediatamente le stampe contenenti informazioni riservate o strategiche
- non lasciare operazioni di stampa in sospeso sul computer
- assicurarsi che la stampante sia in linea e funzionante prima di inviare in stampa i documenti
- non comunicare a persone estranee la password di accesso alla stampante o altri parametri di configurazione che potrebbero consentire la stampa da remoto

Gestione del materiale

Gestione del materiale di output

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. chiavette USB, cd) contenenti informazioni riservate o strategiche;
- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine.

Gestione del materiale cartaceo

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);
- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento.

Gestione delle apparecchiature dismesse

Le informazioni classificate come "riservate" (dati personali, dati sensibili ecc.) devono essere cancellate in maniera definitiva dai dispositivi di memorizzazione, prima che le apparecchiature vengano dismesse (trasferite per essere riutilizzate da altri utenti, riciclate o smaltite).