CORTE DI APPELLO DI CAMPOBASSO

Presidenza P.zza V.Emanuele II – 86100 CB tel.0874/400244-245- Fax 0874/97445✉ E-mail ca.campobasso@giustizia.it

Prot. n. 122425

Campobasso, 2/10/2025

Oggetto: Manuale di sicurezza per gli utenti

Al Presidente di Sezione
dr. Roberto Melone
SEDE

A Presidente del Collegio civile
dr.ssa Maria Grazia d'Errico
DSEDE

Ai Consiglieri
SEDE

Al Personale SEDE

Si trasmette, per opportuna conoscenza e norma, il manuale di sicurezza per gli utenti con preghiera di attenersi alle disposizioni impartite.

IL PRESIDENTE DELLA CORTE
Dott. Vincenzo Pupilella

Manuale di sicurezza per gli utenti

Di seguito vengono elencati i principali suggerimenti da fornire ad un utente per aumentare la sicurezza globale del sistema.

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 backup.

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'ADSI.

Non 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.

Utilizzo del PC

L'utente deve attenersi scrupolosamente all'utilizzo del PC solo ed esclusivamente per attività di Ufficio, ed è fatto divieto, salvo operazioni semplici (p.e., sostituzione di mouse, di tastiera) che non possano compromettere la funzionalità del PC, assumere iniziative personali per porre rimedio ad eventuali problemi tecnici, in particolar modo di tipo hardware; in tale caso è consigliabile rivolgersi al proprio ufficio che curerà la pratica di assistenza (Ufficio Informatica, laddove presente, o Ufficio Economato/Beni Patrimoniali e in caso di urgenza ai tecnici dell'assistenza sistemistica o, in assenza di questi, all'ADSI dell'ufficio.

Amministrare correttamente le password

Essendo le password il metodo più semplice e diffuso per accedere agli account sia su stazioni di lavoro sia in Internet, appare evidente che la scelta della password è estremamente importante per la sicurezza dei propri dati e dell'intera rete del Ministero della Giustizia. Vengono quindi elencate in questo paragrafo una serie di norme che dovrebbero essere rispettate a norma dell'articolo *25* del DM 24/5/2001.

Le password debbono essere cambiate con frequenza:

- trimestrale, per gli account relativi a dati sensibili e particolarmente importanti
- semestrale per gli account utenti
- annuale per le password di accensione delle postazioni di lavoro.

Al proposito si noti che l'articolo 25 comma 3 del DM 24/5/2001 richiede che tutte le password siano rinnovate almeno una volta all'anno.
Tutte le password debbono rispettare i seguenti requisiti:

- devono essere composte da almeno otto caratteri
- devono contenere almeno tre tipi diversi di caratteri inclusi tra quelli maiuscoli, minuscoli, cifre e simboli di interpunzione
- non devono essere parole presenti in dizionari delle lingue più diffuse
- non devono essere basate su parole dialettali o gergali
- non devono essere basate su informazioni personali come data di nascita, numeri di telefono, indirizzi
- non devono essere basate su informazioni personali di familiari, amici, colleghi, attori, personaggi famosi, ecc.
- non devono essere termini tecnici o informatici, comandi, siti, società. ecc.
- non devono essere del tipo aaabbb, 123456, fedcba, o simili
- non devono essere password dei tipi elencati in precedenza scritte al contrario
- non devono essere basate su password analoghe alle precedenti con l'aggiunta di cifre prima o dopo.

Tutti gli utenti, infine, debbono attenersi scrupolosamente alle seguenti prescrizioni:

- utilizzare password diverse per servizi e account a livelli di sicurezza diversa (es. posta elettronica gratuita su Internet ed accesso ai DataBase interni)
- non rivelare le password a nessuno, inclusi amici e familiari
- non condividere le password con altri colleghi o assistenti, salvo quanto disposto a proposito dell'utilizzo del programma "Proteus PA"
- non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono
- non scrivere le password su carta o biglietti e non memorizzare le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura
- non scrivere la propria password su questionari o presunti moduli di sicurezza
- non parlare della propria password o rivelare indizi su essa
- non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password
- non riutilizzare in nessun caso le password.

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).
Si fa presente che per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro è necessario far riferimento al responsabile o al titolare del trattamento dei dati.

Sicurezza delle reti

La prima linea di difesa di qualunque sistema informatico è la protezione dell'infrastruttura di rete. A questo riguardo vengono qui considerati i principali pericoli che si corrono ed elencate le contromisure da adottare.

Modem

Come già detto, la disponibilità di modem sulle postazioni di lavoro costituisce una potenziale minaccia perché il loro uso per instaurare un collegamento con una rete esterna potrebbe esporre la rete ad attacchi che aggirano i firewall ed eludono i sistemi di monitoraggio e di controllo.

Sebbene il regolamento informatico del Ministero già vieti l'uso dei modem, è opportuno rimarcare questo punto perché un modem è facilmente installabile e configurabile (ove si disponga degli opportuni privilegi) ed è spesso incluso nei computer portatili.
E' vietato aggiungere dispositivi modem sulle porte seriali e USB.
Il Responsabile della sicurezza deve essere immediatamente informato in caso di rilevazione di telefonate a numeri noti di Internet Service Provider esterni.
L'uso del modem in contrasto con questa norma deve essere espressamente richiesto con adeguata motivazione ed autorizzato per iscritto dal Responsabile della sicurezza. In questo caso l'utente deve seguire le norme suggerite nel manuale di sicurezza per gli utenti (disconnessione dalla rete locale durante il periodo di attivazione del modem, installazione locale di un antivirus aggiornato), nonché installare un Personal Firewall con configurazione molto restrittiva definita dal Responsabile della sicurezza. In ogni caso l'utente diventa responsabile di eventuali danni che possano derivare al sistema da un uso non appropriato del modem.

Virus e contromisure

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato;
- evitare di utilizzare giochi o software di condivisione file o di farlo soltanto su computer dove questo è permesso perché i programmi per i video giochi possono essere usati come veicoli per software dannoso, e farlo su postazioni isolate serve a contenere i danni
- assicurarsi di non far partire accidentalmente il computer da dischetto e, se possibile, impostare il BIOS in modo da avere come "primary boot device" il disco rigido di avvio e proteggere l'accesso al BIOS tramite password. Infatti se il dischetto fosse infetto, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file. Impostando la partenza dal disco rigido si evitano anche errori o dimenticanze accidentali;
- proteggere i dischetti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- installare (o farsi istallare dagli i di sistema) l'ultima versione dell'antivirus e tenere aggiornati i file con gli identificativi dei virus. La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus;
- salvare o sottoporre a backup i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:

- diffondere messaggi di provenienza dubbia o partecipare a "catene di S. Antonio" e simili. In particolare, quando si ricevono informazioni (via posta elettronica o per altra via) circa nuovi virus, con la preghiera di dare massima diffusione al messaggio, prima di effettuare qualunque azione controllare che non si tratti di una "bufala" (in gergo, hoax) con l'e di sistema o su un sito web specializzato, ciò per evitare di diffondere informazioni sbagliate, che possono generare paure ingiustificate e generare traffico inutile (veri scopi di chi diffonde queste "bufale"). E' anche opportuno informare l'e di sistema che si è ricevuto un messaggio di questo genere, affinché possa essere messo in guardia, fornire informazioni più corrette agli utenti ed eventualmente attivare una ricerca e/o blocco del mittente nel caso che il fenomeno diventasse pesante.
- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione anti-virus
- visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi
- modificare le configurazioni del software antivirus.

Posta elettronica

Gli utenti devono:

- usare solo il software di posta approvato dal Ministero della Giustizia;
- effettuare la scansione con programmi di controllo antivirus approvati dal Ministero dei messaggi in ingresso per evitare virus o contenuti maligni;
- impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
- trasmettere dati confidenziali solo se adeguatamente cifrati (standard S/MIME);
- trasmettere di preferenza messaggi con firma digitale (standard S/MIME con firma di tipo deatched), per garantire al destinatario l'origine del messaggio; si noti che questa tecnica, pur basandosi sui medesimi principi della firma digitale usata per la sottoscrizione di documenti elettronici con valore legale, è fondamentalmente diversa e viene usata nello standard S/MIME per garantire l'autenticità dei messaggi di

posta elettronica ed evitare quindi la generazione di messaggi falsi ("fake mail") che potrebbero indurre in errore utenti inesperti.

Gli utenti non devono:

- utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza ed in ogni caso non utilizzarla eccessivamente per scopi personali
- partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, non utilizzare la posta elettronica per spamming
- inviare mai informazioni confidenziali tramite posta elettronica non cifrata
- aprire posta elettronica di provenienza dubbia.