REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Sommario

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Amministrazione non solo a rischi di natura patrimoniale, ma anche alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto contrattuale, dipendente o meno, sono state redatte in questo regolamento delle indicazioni nell'uso delle apparecchiature informatiche al fine di evitare che comportamenti inidonei possano innescare problemi o minacce alla Sicurezza.

1. INDICAZIONI PER L'UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer utilizzato dall'utente è uno strumento di lavoro che deve essere custodito con cura evitando il più possibile ogni forma di danneggiamento ed utilizzo al di fuori dell'attività lavorativa.
L'accesso ad ogni personal computer è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.
Sono vietati l'uso e/o l'installazione di programmi diversi da quelli distribuiti ed installati ufficialmente dall'UOC Sistemi Informativi dell'Azienda come previsto dalla normativa AGID (ABSC 2.3.1). L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Nel caso fossero necessari ulteriori programmi, gli stessi dovranno essere autorizzati.
Il Personal Computer deve essere spento prima di lasciare gli uffici o nel caso di assenza prolungata; nel caso di breve e temporaneo inutilizzo, ad esempio nella pausa pranzo, la postazione deve essere bloccata tramite la combinazione dei tasti WINDOWS + L o in alternativa deve essere fatta la disconnessione del proprio utente in maniera tale da impedirne l'utilizzo a personale non autorizzato.

Lo spegnimento e successiva riaccensione del P.C. almeno una volta al giorno consente l'applicazione degli aggiornamenti atti a correggere le vulnerabilità del sistema come previsto dalla normativa AGID (ABSC 4.5.1).
La sicurezza e il rispetto della normativa sulla privacy nel trattamento dei dati di cui l'Azienda è titolare sono garantiti solamente se ogni dato viene conservato nelle cartelle condivise residenti su server, messe a disposizione dall'Az. Stessa, oppure viene trattato mediante l'utilizzo dei sistemi software aziendali.

Secondo tale principio, negli hard disk dei dispositivi assegnati **non devono essere depositati dati per i quali l'eventuale perdita di disponibilità, di integrità o di riservatezza causerebbe un danno all'Azienda oltre che agli interessati**.

Si ricorda inoltre che tutti i dischi e altre unità di memorizzazione locali (es. Disco C, chiavette, dischi esterni) non sono soggette a salvataggio da parte dell'UOC Sistemi Informativi.

2. INDICAZIONI PER L'UTILIZZO DI DOTAZIONI INFORMATICHE PORTATILI

L'utente è responsabile delle dotazioni informatiche portatili, quali notebook, tablet, smartphone, ecc… assegnategli e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Alle dotazioni informatiche portatili si applicano le regole di utilizzo previste per i P.C. connessi in rete, eventuali regole particolari di utilizzo saranno concordate direttamente con il responsabile dell'UOC Sistemi Informativi e gli utenti interessati.
Deve essere posta massima attenzione alla custodia delle dotazioni informatiche portatili durante il loro utilizzo ed in particolare all'esterno delle sedi istituzionali dell'Ente.
La sicurezza e il rispetto della normativa sulla privacy nel trattamento dei dati di cui l'Azienda è titolare sono garantiti solamente se ogni dato viene conservato nelle cartelle condivise residenti su server, messe a disposizione dall'Az. Stessa, oppure viene trattato mediante l'utilizzo dei sistemi software aziendali.

Secondo tale principio, negli hard disk dei dispositivi assegnati **non devono essere depositati dati per i quali l'eventuale perdita di disponibilità, di integrità o di riservatezza causerebbe un danno all'Azienda oltre che agli interessati**.

Si ricorda inoltre che tutti i dischi e altre unità di memorizzazione locali (es. Disco C, chiavette, dischi esterni) non sono soggette a salvataggio da parte dell'UOC Sistemi Informativi.

3. UTILIZZO DI FOTOCOPIATRICI E STAMPANTI LOCALI E DI RETE

È cura degli utenti effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti (soprattutto per le stampanti di rete site in luoghi facilmente accessibili al pubblico), al fine di evitare che possano essere visionate da persone non autorizzate.
È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni, è inoltre sconsigliato la stampa di email, ricevute di posta elettronica certificata e altri documenti che sono facilmente reperibili dalle risorse informatiche a disposizione.
Inoltre, è consigliabile sempre effettuare l'anteprima di stampa prima della stampa effettiva, al fine di verificare la correttezza della stampa ed evitare di mandare in stampa documenti non impostati correttamente.
Quando si cambiano le impostazioni di un fotocopiatore e/o stampante, alla fine del proprio lavoro, si deve in seguito ripristinare l'assetto originario.

4. UTILIZZO DELLE CARTELLE DI RETE

Le cartelle di rete (cartelle dedicate ai servizi presenti sul server) sono aree di condivisione di informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup, da parte dell'UOC Sistemi Informativi.
Nel caso in cui vengano rilevati dei file impropriamente memorizzati nelle cartelle di rete, questi verranno eliminati d'ufficio.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti da evitare un'archiviazione ridondante che comporta inutili costi aggiuntivi.
Appena terminata l'attività è bene scollegarsi dalla cartella di rete.

5. INDICAZIONI PER L' UTILIZZO DEI SUPPORTI RIMOVIBILI

È fatto divieto di memorizzare dati ricadenti nelle particolari categorie ex art. 9 GDPR nei supporti rimovibili (penne USB, HD esterni USB, CD, DVD) che devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, divulgato, alterato e/o distrutto o successivamente alla cancellazione, recuperato.
Nel caso in cui i dati relativi alle particolari categorie di dati ex art. 9 GDPR siano memorizzati nei supporti rimovibili, ai fini di creare dei salvataggi, questi devono essere custoditi in archivi chiusi a chiave. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente la UOC Sistemi Informativi nel caso in cui vengano rilevati virus o altri comportamenti informatici anomali.
Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali come previsto nella normativa AGID (ABSC 8.3.1).

6. ANTIVIRUS

Il sistema informatico dell'Azienda è protetto da software antivirus centralizzato, della modalità Client/Server, aggiornati periodicamente.
Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al servizio di assistenza dell'UOC Sistemi Informativi.
I Virus di tipo "ransomware" continuano a rappresentare la minaccia più temuta. In questo tipo di minaccia i criminali informatici puntano a sfruttare i punti deboli umani, i cattivi comportamenti e la scarsa attenzione che la maggioranza degli utenti ripone nell'utilizzo degli strumenti informatici.
Il ransomware ("ransom" significa riscatto) è una forma di malware che impedisce all'utente di accedere ad aree del proprio computer perché crittografa i files o protegge l'hard disk dagli accessi, visualizzando un messaggio che forza l'utente a pagare per riavere accesso al computer.
Questo tipo di malware si diffonde attraverso file scaricati o vulnerabilità presenti nei P.C. non aggiornati e nei servizi di rete.
È bene quindi verificare che l'antivirus sia installato ed aggiornato come previsto dalla normativa AGID (ABSC 8.1.1). Per fare ciò occorre tramite il puntatore del mouse posizionarlo sull'Area di notifica, situata in basso a destra del Desktop, sopra l'icona del simbolo dell'antivirus, cliccare con il tasto destro del mouse, e scegliere l'opzione '*Apri console*'.
Verrà visualizzata la data e ora dell'ultimo aggiornamento effettuato che nel caso corrispondesse al giorno precedente si deve fare immediatamente l'aggiornamento.
L'azienda per quanto possibile imposterà delle politiche di configurazione in modo da:
a) evitare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. AGID (ABSC 8.7.1)
b) evitare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. AGID (ABSC 8.7.2)
c) evitare l'apertura automatica dei messaggi di posta elettronica. AGID (ABSC 8.7.3)
d) evitare l'anteprima automatica dei contenuti dei file. AGID (ABSC 8.7.4)
Ogni utente deve comunque tenere comportamenti rispettosi di quanto appena descritto in modo da ridurre il rischio di attacco al sistema informatico dell'Ente da parte di virus o altro software dannoso.

7. GESTIONE DELLE PASSWORD

Le credenziali di autenticazione per l'accesso al computer, alla mail ed ai software applicativi vengono assegnate dal personale dell'UO Sistemi Informativi previa richiesta informatizzata, da parte del direttore del reparto di appartenenza, tramite l'applicativo GRU o CREDNET. Alternativa alla richiesta informatizzata, solo per i reparti non ancora abilitati, è l'invio del modulo di richiesta appositamente predisposto, debitamente compilato dal Direttore/Responsabile della UOC/UOS di appartenenza ed autorizzato dalla DMPO o dalla Direzione di riferimento.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (userid) associato ad una parola chiave (password) riservata che dovrà essere modificata al primo accesso e custodita dall'utente con la massima diligenza e non divulgata. **È proibito entrare nei P.C. e nei programmi con credenziali non proprie.**
La password è la prima protezione ai dati, non deve essere ceduta ad altri, non deve essere scritta in un foglietto lasciato sullo schermo o sulla scrivania. Ciascun utente è responsabile delle proprie credenziali per cui, se dovessero essere usate da altri in modo improprio, la colpa ricadrebbe sull'utente stesso.
È buona regola impostare la password:

- con una sequenza minima di 14 caratteri alfanumerici
- utilizzando caratteri maiuscoli, minuscoli, numeri,
- utilizzando caratteri speciali, come @ # $ % ^ &
- alternando maiuscole a minuscole.

Nel creare una password sicura è altresì buona norma non usare parole comuni per la password come ad esempio: la data di compleanno, il proprio nome utente (User-ID), così che non sia riconducibile all'incaricato.
Al fine di aumentare il grado di sicurezza è consigliabile creare password diverse per tipologie diverse di utilizzo. Questo al fine di evitare che, se la propria password venisse scoperta da un malintenzionato, questo possa accedere a tutti i servizi.
Il sistema di autenticazione del dominio/posta interno provvede 15 giorni prima della scadenza (ogni 90 giorni), a richiedere la variazione della password agli utenti, si invitano pertanto gli utenti ad effettuare il cambio password prima della sua scadenza. Per le altre autenticazioni, ove non sono previsti sistemi automatizzati di rinnovo delle password, si invitano gli utenti, prima della scadenza, a variare la propria password periodicamente attraverso i sistemi delle singole applicazioni.

8. UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.

Per ragioni di sicurezza è stato implementato un servizio di filtro dei siti internet, che permette di inibire o limitare l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali, sono pertanto **da evitare tutte le azioni atte ad eludere tali politiche di filtro**.
Si informa che l'UOC Sistemi Informativi dispone di strumenti di controllo che evidenziano le attività di elusione delle politiche di filtro.
È necessario evitare di collegare il telefonino al computer anche solo per la ricarica in quanto tale azione potrebbe essere considerata dai sistemi di controllo una elusione al filtro.
Qualora tali sistemi di filtro impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, l'utente interessato dovrà richiedere lo sblocco alla UOC Sistemi Informativi.
È facoltà dell'UOC Sistemi Informativi inibire temporaneamente, anche senza preavviso, la navigazione in internet alle postazioni dove si prefiguri un utilizzo improprio o che metta a repentaglio la sicurezza del Sistema informatico dell'Ente.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, compresa la partecipazione a forum non professionali.

9. ACCESSO ALLA RETE AZIENDALE DA ESTERNO TRAMITE CONNESSIONE VPN

Se necessario, e previa autorizzazione dei Sistemi Informativi, è possibile richiedere l'accesso alla rete aziendale da esterno (rete privata internet) mediante l'utilizzo di connessioni VPN dedicate. L'azienda fornirà la possibilità di connettersi in VPN utilizzando un sistema sicuro protetto da doppia autenticazione che richiede l'utilizzo di un dispositivo mobile (cellulare) dell'utente.

10. UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta istituzionale, assegnata dall'Amministrazione all'utente, è uno strumento di lavoro consentito per finalità connesse allo svolgimento della propria attività lavorativa. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
La casella di posta deve essere mantenuta in ordine, controllando periodicamente il rispetto della dimensione assegnata, mantenendo pulita la cartella "Cestino" / "Posta Eliminata".
Per la trasmissione di files è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati; per gli scambi di files tra colleghi si incoraggia l'utilizzo delle cartelle condivise esistenti.

Al fine di incrementare il livello di sicurezza aziendale e della posta elettronica è necessario attivare l'autenticazione a due fattori sulla casella di posta personale (su piattaforma Google Workplace); L'autenticazione a due fattori è uno strumento di sicurezza con il quale viene richiesto all'utente di fornire un fattore di autenticazione aggiuntivo alla normale password dell'account, al fine di verificare la propria identità. Questa impostazione rende più sicuro l'accesso a qualsiasi tipo di risorsa con cui l'operatore interagisce.

La principale porta d'ingresso dei crimini informatici è l'e-mail di conseguenza meglio evitare di eseguire download di file o documenti da siti Web o Ftp non conosciuti o provenienti da indirizzi mail di dubbia provenienza, né cliccare su link sospetti presenti nel corpo di messaggi di posta provenienti da mittenti sconosciuti.
L'apertura dell'allegato della mail che sembra del tutto innocuo, può comportare ad esempio l'installazione di un malware/virus attraverso il download da un server controllato dai criminali informatici, in caso di dubbi contattare il Servizio Sistemi Informativi.
Evitare di utilizzare la mail privata dalle postazioni di lavoro perché priva degli strumenti di controllo virus impostati dal Servizio Sistemi Informativi nelle mail aziendali.

Per riconoscere una mail sospetta si consiglia di controllare il mittente della e-mail, se è sconosciuto o vi sembra un nominativo strano, state attenti. Questo però non è sufficiente, in quanto potrebbe arrivarvi un messaggio da una persona o da un ufficio con cui siete in contatto, per tale motivo è consigliato controllare anche le seguenti caratteristiche:

- Il nome di chi vi invia il messaggio è conosciuto ma il reale indirizzo email non ha un formato standard
- Manca l'oggetto od esso vi pare strano, se possibile chiedete a chi vi spedisce una e-mail di inserire un oggetto significativo e non di singole parole.
- La data e l'ora della mail sono anomale.
- E-mail provenienti da aziende o persone importanti, uffici, ecc., scritte male e/o con errori di battitura.
- Pubblicità o richieste personali indesiderate.
- Richieste di denaro o con troppe promesse.
- E-mail che provengono da posti lontani in cui non conosci nessun amico o parente.

Si consiglia Inoltre di

- Leggere attentamente ogni e-mail prima di aprire allegati anche se provengono da familiari
- NON aprire mai un allegato di posta elettronica proveniente da un mittente sconosciuto.
- Porre attenzione nell' aprire un allegato di posta elettronica di un mittente noto, a meno che non sapete cosa contenga
- se continuate ad avere dei dubbi, chiamate direttamente il mittente e chiedetegli se vi ha inoltrato volutamente la mail

- evitate di rispondere alle catene di Sant'Antonio
- Non rispondere MAI allo spam, né per protestare, né per "disiscrivervi"
- Se è proprio necessario mettere il vostro indirizzo in una pagina Web, mettetelo sotto forma di immagine grafica
- Non date il vostro indirizzo ai siti che ve lo chiedono, a meno che abbiano una reputazione Conosciuta e garantita.

Le caselle di posta elettronica generiche o non nominative e le modalità di configurazione (e conseguentemente di accesso) possono essere di due tipi:

- **Casella di posta elettronica istituzionale** - potrà essere condivisa tra più lavoratori (a discrezione del Responsabile/Dirigente di Area) e sarà riconducibile ad un determinato settore o servizio. A queste caselle verrà dato accesso in delega con l'utilizzo della propria casella personale e senza la fornitura delle credenziali (utente e password della email di gruppo).
- **Gruppo di distribuzione**: non richiede licenza aggiuntiva e quindi non ha costo. Le mail inviate a questo indirizzo vengono inoltrate a tutti i membri del gruppo, i quali, come requisiti, devono essere in possesso di mail Aziendale. Tutti i membri del gruppo di distribuzione possono essere abilitati anche all'inoltro di email a nome del gruppo stesso.

In caso di cessazione del rapporto di lavoro o collaborazione o di mandato dei Direttori, la casella di posta elettronica individuale dell'interessato verrà sospesa per 30 giorni dalla data di cessazione del rapporto in essere. **Trascorsi i 30 giorni la casella verrà eliminata**.
Sarà cura dell'intestatario della casella di posta, prima della cessazione del rapporto in essere con l'Azienda e previa richiesta di abilitazione ai Sistemi Informativi, scaricare una copia dei messaggi e dei contatti presenti su GSuite.
La procedura da seguire è la seguente:
Entrare nella propria casella di posta
Dal pannello in alto a destra cliccare su Account e selezionare "Gestisci il tuo account Google"
Dalla videata che si apre selezionare *Dati e privacy*
Scarica o Elimina i tuoi dati
Selezionare il servizio Posta e selezionare i dati per i quali si intende effettuare il backup
Selezionare eventualmente altri servizi per i quali si intende effettuare il backup
Procedere al passaggio successivo
Impostare i parametri desiderati, tipicamente "Invia tramite e-mail il link per il download"
Premere crea archivio
Successivamente si riceverà via mail il link tramite il quale scaricare i file prodotti.

11. ISTRUZIONI PER PROTEGGERSI DAL PHISHING ED EVITARE LA SOTTRAZIONE DI DATI RISERVATI E PERSONALI AI SENSI DELL'ARTICOLO 32, COMMA 4, DEL REG (UE) 2016/679 (GDPR)

Il presente modulo intende fornire delle Istruzioni operative agli Incaricati, anche ai sensi dell'art. 32, comma 4 GDPR, in relazione al trattamento dei dati del Titolare effettuato per il tramite del servizio di posta elettronica, in considerazione del fatto che tale servizio, pur essendo protetto da strumenti che applicano politiche di antivirus ed antispam, potrebbe non bloccare email potenzialmente malevole.
Tali Istruzioni devono essere considerate quali direttive provenienti dal datore di lavoro il cui mancato rispetto potrebbe generare delle responsabilità a carico del dipendente.

11.1. Non utilizzare il proprio account e-mail fornito dal Titolare per usi personali

Il dipendente è tenuto a non utilizzare il proprio account e-mail fornito dall'Azienda per propri fini ed usi privati, quali, a titolo esemplificativo, scambi di e-mail con persone inerenti la propria sfera privata; partecipazione a gruppi di discussione; acquisti online su piattaforme di e-commerce (Amazon, eBay, Poste Italiane e simili); ricezione di e-mail promozionali e pubblicitarie; iscrizione a siti non istituzionali o piattaforme di social network.
Ciò, infatti, comporta la circolazione e l'esposizione pericolosa dell'indirizzo istituzionale in ambiti dove operano malintenzionati. Un simile comportamento, inoltre, potrebbe anche ledere l'immagine e la reputazione aziendale.

11.2. Non inviare risposte ad e-mail che richiedano dati

Il dipendente non deve rispondere a messaggi di posta elettronica che richiedano l'autenticazione con le proprie credenziali di accesso all'account aziendale, ovvero che richiedano dati personali, credenziali di accesso, numeri di carta di credito, altre informazioni correlate al dipendente.
Si avvisa, infatti, il dipendente che allo stato attuale nessuna Amministratore di Servizi o Ente Pubblico o società privata (a titolo esemplificativo banche, Agenzia delle Entrate, Poste Italiane e simili) richiede tramite e-mail tali dati.
Pertanto, le eventuali richieste pervenute a mezzo mail sono da intendersi come richieste truffaldine e si richiede quindi la massima accortezza.

11.3. Non aprire allegati anche se provengono da mittenti noti

Il dipendente non deve aprire allegati non attesi o il cui invio non sia stato concordato con il mittente in quanto gli allegati sono mezzi attraverso cui vengono veicolati virus informatici o programmi che permettono a terzi di entrare nel sistema.
Prima di aprire qualsiasi allegato il dipendente è tenuto ad effettuare una scansione preventiva utilizzando l'antivirus.

11.4. Verificare sempre con attenzione il mittente delle e-mail ricevute

Il dipendente deve controllare sempre il nome ma anche il reale indirizzo e-mail del mittente dei messaggi ricevuti. E' consuetudine infatti che le mail di phishing arrivino personalizzate e camuffate come messaggi di persone realmente conosciute.

11.5. Verificare sempre ortografia e sintassi nel testo delle e-mail ricevute

Il dipendente deve prestare attenzione al testo delle e-mail al fine di verificare la presenza di errori di ortografia, sintassi, traduzioni dall'inglese che risultano approssimative.

Nel caso in cui nel testo di una e-mail ricevuta si rilevino tali imprecisioni il dipendente deve prestare la massima attenzione in quanto potrebbe trattarsi di e-mail standard che vengono inviate contemporaneamente a milioni di potenziali vittime.

11.6. Diffidare di e-mail che mettono urgenza, che minacciano sanzioni, che promettono premi e vincite o che contengono richieste di aiuto

Il dipendente deve prestare attenzione e diffidare di e-mail il cui contenuto richiede l'apertura di un link o di un allegato minacciando un imminente pericolo (es.: la perdita di denaro o la chiusura di servizi).
Il dipendente, pertanto, non deve rispondere ad e-mail che minacciano sanzioni, che annunciano premi, che chiedono di fare qualcosa con urgenza, che contengono richieste di aiuto umanitario e simili.

11.7. Non cliccare su link contenuti sul corpo delle e-mail

Il dipendente non deve cliccare su collegamenti contenuti nel testo di e-mail inattese in quanto tale link può condurre a siti web capaci di carpire informazioni o infettare il computer.
Il dipendente deve inoltre prestare particolare attenzione ai collegamenti a siti web che richiedono informazioni personali, anche se l'e-mail sembra provenire da una fonte legittima, perché i siti web di phishing sono spesso repliche esatte di siti web legittimi.

11.8. Segnalare immediatamente l'incidente

In caso di apertura di e-mail / link / allegati sospetti il dipendente deve informare subito, in maniera circostanziata, l'UOC Sistemi Informativi della avvenuta fuoriuscita di dati all'esterno.
Se il dipendente sospetta di aver comunicato le credenziali ad un sito truffaldino è necessario che egli cambi immediatamente la password utilizzando un dispositivo diverso, avvisando immediatamente l'UOC Sistemi Informativi.
Il dipendente deve usare sempre password univoche, di lunghezza adeguata, composte da caratteri minuscoli, maiuscoli, numerici e speciali; evitando di inserire nelle password riferimenti personali.

11.9. Comportamento da adottare nei casi dubbi

Nel caso in cui il dipendente riceva e-mail di contenuto sospetto, il miglior modo di agire è quello di non rispondere, non aprire allegati, non cliccare su link, non inoltrare la e-mail a colleghi ed avvertire l'UOC Sistemi Informativi.
Se dalle verifiche effettuate, la mail risultasse essere un tentativo di phishing o contenere un allegato malevolo, è necessario avvisare tempestivamente l'UOC Sistemi Informativi.

11.10. Diffidare anche di mittenti noti

Potrebbe verificarsi la circostanza che le e-mail truffaldine provengano da mittenti noti, da account dell'Azienda, da "uffici" della stessa, da una "assistenza tecnica", dal "gestore dell'account", da "gestore del server" di posta elettronica e simili.

Diffidare da comunicazioni che sembrano provenire dall'Azienda stessa e che segnalano problemi con il vostro account o le vostre credenziali.
Nel dubbio il dipendente deve contattare direttamente la struttura da cui sembra provenire il messaggio e chiedere chiarimenti.
Non inserire mai credenziali di autenticazione su siti raggiunti cliccando nel corpo di una e-mail.

11.11. Diffidare di e-mail personalizzate

Si avvisa il dipendente che l'e-mail ingannevole potrebbe anche essere personalizzata con informazioni relative all'ufficio o alla persona stessa del dipendente. Tali informazioni si possono reperire agevolmente sui social network o da elenchi pubblici, pertanto, anche se la e-mail dovesse sembrare realmente diretta al dipendente, è necessario mantenere alta l'attenzione e avvisare l'UOC Sistemi Informativi.

11. IMPLEMENTAZIONI DEL SISTEMA INFORMATICO

L'UOC Sistemi Informativi per sua natura si mantiene aggiornata attraverso la sperimentazione di software e hardware e sovraintende al buon funzionamento e alla sicurezza del Sistema Informatico, al complesso dei beni e alle procedure informatiche.
La sicurezza e la gestibilità del Sistema Informatico sono legate alla sua omogeneità e coerenza.
L'UOC Sistemi Informativi è autorizzata ad intraprendere tutte le azioni di razionalizzazione, semplificazione e gestione del Sistema Informatico ai fini della sicurezza, disponibilità e gestibilità.
Ogni variazione del Sistema Informatico comporta valutazioni tecniche di fattibilità, opportunità, integrabilità e di sicurezza da parte dell'UOC Sistemi Informativi; pertanto mentre le acquisizioni di nuovi beni o procedure informatiche, possono di volta in volta trovare copertura in conti di costo di specifici settori/servizi, è l'UOC Sistemi Informativi che le approva, e le organizza sulla scorta dei criteri già menzionati. Le necessità di variazione del Sistema Informatico devono sempre essere portate all'attenzione dell'UOC Sistemi Informativi, per tempo e comunque prima di intraprendere qualsiasi altra attività.
Le richieste di variazioni dei singoli utenti relative a configurazioni dei P.C. o permessi sui sistemi centralizzati di sicurezza, devono essere debitamente motivate e autorizzate dalla Direzione di riferimento.