UNIVERSITÀ DEGLI STUDI DI MILANO

Istruzioni per proteggersi dal phishing ed evitare la sottrazione di dati riservati e personali ai sensi dell'Articolo 32, comma 4[1], del Regolamento Europeo per la Protezione dei Dati (GDPR)

L'Università degli Studi di Milano, in qualità di Titolare del trattamento dei dati personali, dispone che chiunque abbia accesso a dati, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, riferite a persone, al fine di evitare **frodi**, **attacchi informatici** e furto di **credenziali**, si attenga, nell'attività quotidiana, alle seguenti **istruzioni.**

Tali **istruzioni** sono da considerarsi, a tutti gli effetti, quali direttive provenienti dal proprio datore di lavoro e, in quanto tali, il loro mancato rispetto potrebbe generare delle responsabilità a carico del dipendente.

Istruzioni

tenuto conto che il servizio di posta elettronica di Ateneo, pur essendo protetto da strumenti che applicano politiche di antivirus ed antispam, può non bloccare fisiologicamente una quota di mail potenzialmente malevole, si rende necessario prescrivere a tutti i dipendenti di

1. Non utilizzare la e-mail di Ateneo per usi personali

Non utilizzare la e-mail di Ateneo per usi privati, quali scambi di e-mail con amici, partecipazione a gruppi di discussione, acquisti online (Amazon, eBay, shopping online in generale), partecipazione a mailing list informali e non istituzionali di discussione, iscrizione a siti non istituzionali quali, ad esempio, Facebook, Google, Dropbox, LinkedIn e altre piattaforme di social network. Ciò comporta la circolazione e l'esposizione pericolosa dell'indirizzo istituzionale in ambiti dove operano malintenzionati alla ricerca di potenziali vittime. Un simile comportamento può anche sollevare, in molti casi, un problema di immagine e di reputazione per l'Ateneo.

2. Non rispondere mai a e-mail che richiedano dati

Non bisogna **mai** rispondere a messaggi di posta elettronica che richiedano l'autenticazione con le credenziali di Ateneo o domandino esplicitamente dati, credenziali, numeri di carta di credito, informazioni correlate al dipendente o al suo account. **Nessun Amministratore dei Servizi di Ateneo e nessun Ente pubblico o società privata** (ad es. aziende informatiche, banche, Agenzia delle Entrate, Poste Italiane, Equitalia o la Procura della Repubblica) **richiede oggi, tramite e-mail, tali dati**. Sono tutte richieste **truffaldine**, che mirano ad ottenere dette informazioni.

[1] Regolamento Generale per la Protezione dei Dati (EU 2016/679): Art. 32, comma 4: Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

3. Mantenere un atteggiamento prudente nella lettura delle mail e soprattutto nell'apertura degli allegati.

Non aprire mai **allegati** non attesi o il cui invio non sia stato concordato con il mittente. Spesso gli allegati servono per veicolare virus informatici o programmi che permettono a malintenzionati di entrare nel sistema informatico.
In ogni caso, prima di aprire qualsiasi allegato è sempre necessario effettuare una scansione preventiva del file allegato utilizzando l'antivirus di Ateneo (https://work.unimi.it/servizi/servizi_tec/6562.htm) e gli eventuali ulteriori strumenti messi a disposizione dell'Ateneo.
Non abilitare mai le macro di Office, anche se il documento ci invita a farlo. Far attenzione anche ai file PDF perchè questo tipo di file può eseguire addirittura ulteriori componenti (ad es. flash o javascript) lanciare applicazioni esterne. Molti attaccanti usano nomi di file con un doppia estensione, tipo pippo.jpg.exe: Windows mostrerà il file come pippo.jpg nascondendo il fatto che in realtà è un eseguibile; per ovviare a questo, disabilitare nelle opzioni di Esplora Risorse la voce "nascondi estensioni per tipi di file noti"

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

Spesso le e-mail ricevute contengono banali **errori** di ortografia, sintassi, traduzioni dall'inglese approssimative che immediatamente devono insospettire il destinatario. Si tratta infatti di e-mail standard che vengono inviate contemporaneamente a milioni di potenziali vittime.

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

Un modo efficace che i criminali usano per convincere il soggetto a rispondere, a cliccare su un link o ad aprire l'allegato, è quello di **mettere urgenza** minacciando un imminente pericolo (ad esempio la perdita di danaro o la chiusura di determinati servizi), per impedirgli di pensare. Quindi, **non rispondere** a e-mail che minacciano sanzioni, che annunciano premi, che chiedono di fare qualcosa in fretta, che contengono richieste di aiuto umanitario, che propongono relazioni sentimentali o fugaci incontri.

6. Non cliccare su link contenuti nel corpo delle e-mail

Non cliccare su **collegamenti** contenuti nel testo di e-mail inattese. Il link può condurre a siti web capaci di carpire informazioni o di infettare il computer del dipendente. E' necessario perciò passare il mouse sui collegamenti e verificare l'URL (spesso non coincide con quella scritta nella mail);

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

7. Non vergognarsi per la truffa subita e segnalare subito l'incidente all'Ateneo

In caso di comportamento sbagliato, non vergognarsi per l'accaduto mantenendo il silenzio, ma informare subito l'Ufficio Sicurezza ICT e il responsabile della propria struttura della avvenuta fuoriuscita di dati all'esterno.

Se si sospetta di aver comunicato le credenziali a un sito truffaldino, cambiare immediatamente la password utilizzando un dispositivo diverso e scegliendone una sufficientemente robusta. Avvisare tempestivamente il referente tecnico della propria struttura, l'Ufficio Sicurezza ICT di Ateneo (sicurezza@unimi.it) e il Responsabile della protezione dei dati (dpo@unimi.it) Usare sempre password univoche, di lunghezza adeguata, composte da caratteri minuscoli, maiuscoli, numerici e speciali; non inserire nelle password elementi banali o riferimenti personali (es. nomi, date), perché rendono la password semplice da indovinare.

8. Adoperare particolare cautele anche nel caso di mail provenienti (apparentemente) da mittenti noti (compreso l'Ateneo)

A volte le e-mail truffaldine sembrano provenire da mittenti noti, da account della nostra Università, da un sedicente "ufficio di sicurezza" dell'Ateneo, da una non meglio specificata "assistenza tecnica", dal "gestore dell'account", da un fantomatico "webmaster" o dal "gestore del server" di posta elettronica.
È un modo **subdolo** per ingannare il destinatario, essendo molto facile, oggi, sostituirsi nella identità telematica di un soggetto.
Diffidare in modo particolare da **comunicazioni** che sembrano provenire **dall'Ateneo stesso** e che segnalano problemi con il vostro account o le vostre credenziali. Nel dubbio si può contattare telefonicamente la struttura o l'utente da cui sembra provenire il messaggio e chiedere chiarimenti. **Non inserire mai credenziali di autenticazione su siti raggiunti cliccando nel corpo di un'e-mail**.

9. Diffidare anche di e-mail personalizzate

La e-mail ingannevole può essere anche **personalizzata** con informazioni relative al nostro ufficio o alla nostra persona: sono tutte informazioni che si possono reperire agevolmente sui social network o da elenchi pubblici (ad es. sul portale di Ateneo sono pubblicati alcuni dati relativi al luogo di lavoro, ruolo in Ateneo, numero di telefono).
Ciò significa che, anche se la e-mail dovesse sembrare **realmente** diretta a noi, ci si rivolga usando il nostro nome di battesimo o si riferisca a compiti, documenti, fatture, servizi o uffici di nostra competenza, occorre mantenere alta l'attenzione.

10. Cosa fare nei casi dubbi

In caso di e-mail che desta sospetto, il miglior modo di agire è quello di **non fare nulla**, non rispondere, non aprire allegati, non cliccare su link, non inoltrare la e-mail a colleghi.
Verificare se nella sezione dedicata agli avvisi di Sicurezza Informatica, sia stato emesso dall'Ufficio Sicurezza ICT un bollettino riguardante una campagna malevola o di phishing basata su messaggi che hanno caratteristiche simili a quello ricevuto: https://work.unimi.it/servizi/security_gdpr/118606.htm.
Se il messaggio non rientra tra quelli classificati, e persista il dubbio, è opportuno consultare il referente tecnico di struttura.
Se dalle verifiche effettuate, la mail risultasse essere un tentativo di phishing o contenere un allegato malevolo, è necessario avvisare tempestivamente l'Ufficio Sicurezza ICT inviando il corpo della mail malevola come allegato a **sicurezza@unimi.it** e a **spam@unimi.it**. Nei casi in cui, invece, la mail risulti essere semplicemente una mail di spam (posta indesiderata), inoltrare la stessa come allegato esclusivamente all'indirizzo **spam@unimi.it**.

Riferimenti e approfondimenti

Per gli approfondimenti e aggiornamenti di quanto descritto nel presente documento, e per le modalità di implementazione delle misure di sicurezza richieste, fare riferimento ai documenti dell'Ufficio di Sicurezza ICT di Ateneo pubblicati sul portale di Ateneo a partire dalla URL: https://work.unimi.it/servizi/security_gdpr/118546.htm