



ADICU aps

Associazione a Difesa dei Consumatori
e degli Utenti aps

MANUALE SULLA SICUREZZA DELLA POSTA ELETTRONICA

RICONOSCERE E NEUTRALIZZARE LE MINACCE DIGITALI

INIZIATIVE A VANTAGGIO DEI CONSUMATORI, ART. 4, CO. 1 DEL
DECRETO MINISTERIALE 6 MAGGIO 2022; ART. 4, COMMA 1, DEL
DECRETO MINISTERIALE DEL 31 LUGLIO 2024; DECRETO
DIRETTORIALE 29 NOVEMBRE 2024

DIGITALMENTIS

Iniziativa Competenze Digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024



Visita il nostro sito internet

www.adicu.it

INTRODUZIONE

LA POSTA ELETTRONICA COME ASSET AZIENDALE E VETTORE DI RISCHIO

Inventata nel lontano 1971, la posta elettronica (email) rappresenta uno degli strumenti di comunicazione più longevi e strategici del mondo digitale. Nel contesto aziendale moderno, si è affermata come un canale indispensabile per lo scambio di informazioni, la gestione di progetti e la comunicazione con clienti e partner. Si comporta a tutti gli effetti come una lettera digitale che viaggia istantaneamente attraverso Internet. Tuttavia, la sua ubiquità e la sua importanza la rendono anche una delle principali porte d'accesso per le minacce informatiche, trasformando ogni casella di posta in un potenziale punto di vulnerabilità.

I vantaggi strategici dell'email sono innegabili e includono:

- **Nessun costo aggiuntivo** oltre a quello della connessione a Internet.
- La capacità di inviare **lo stesso messaggio a più destinatari** contemporaneamente.
- Un significativo **risparmio di carta**, a sostegno della sostenibilità ambientale.

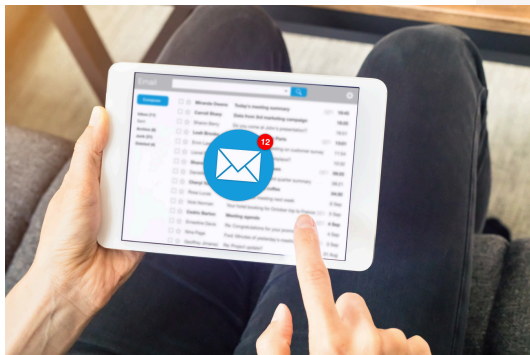
Ogni indirizzo email è unico e strutturato in modo specifico: *nome utente + @ + nome di dominio*. Proprio come non esistono due indirizzi di casa identici, non possono esistere due indirizzi email uguali. Questa struttura garantisce che ogni messaggio arrivi esattamente al destinatario designato.

Per proteggere questo strumento vitale e le preziose informazioni che veicola, è fondamentale partire dalle basi: la creazione e la gestione sicura del proprio account di posta elettronica.



LA PRIMA LINEA DI DIFESA: GESTIONE SICURA DELL'ACCOUNT EMAIL

La creazione e la gestione sicura di un account di posta elettronica rappresentano il primo e più critico passo per proteggere le informazioni sensibili. Le scelte effettuate durante la fase di registrazione, in particolare quelle relative alle credenziali di accesso, hanno un impatto diretto e duraturo sul livello di sicurezza complessivo dell'account e dei dati in esso contenuti.



Creazione di Password Robuste

Una password efficace è la prima barriera contro gli accessi non autorizzati. Per essere considerata "robusta", una password deve seguire regole precise che ne aumentano la complessità e rendono estremamente difficile la sua violazione. Le regole fondamentali sono:

- Utilizzare una combinazione di **lettere maiuscole e minuscole**.
- Includere **numeri e caratteri speciali** (simboli come \$, #, &, =).
- Evitare password ovvie e facilmente intuibili come 'password' o '123456'.
- **Cambiare la password regolarmente** per limitare i danni in caso di compromissione.
- **Non utilizzare mai la stessa password** per più account. Se un servizio viene violato, tutti gli altri account che usano la stessa password diventano immediatamente vulnerabili.



Implementazione dell'Autenticazione a Due Fattori (2FA)

L'Autenticazione a Due Fattori (2FA) aggiunge un **ulteriore livello di sicurezza** al processo di login. Il suo funzionamento è semplice ma estremamente efficace: oltre alla password (il primo fattore), il sistema richiede una seconda verifica per confermare l'identità dell'utente. Questa seconda verifica consiste tipicamente nell'inserire un codice univoco ricevuto tramite **SMS** sul proprio telefono o generato da un'**App** di autenticazione. Attivare la 2FA complica drasticamente la vita a un malintenzionato, perché anche se riuscisse a rubare la password, non potrebbe accedere all'account senza possedere anche il secondo fattore di verifica.

Anche con un account ben protetto, le minacce possono arrivare direttamente nella nostra casella di posta. È quindi fondamentale imparare a riconoscere i messaggi fraudolenti prima che possano causare danni.

RICONOSCERE LA MINACCIA: L'ANATOMIA DI UN ATTACCO PHISHING

Il **phishing** è una delle minacce informatiche più diffuse, ingannevoli e pericolose veicolate tramite email. Si tratta di una frode studiata per rubare dati personali e sensibili, come password, informazioni bancarie o numeri di carte di credito. Riconoscere tempestivamente questi tentativi di inganno è una competenza strategica fondamentale per prevenire il furto di dati, sia personali che aziendali.

Il termine "**phishing**" deriva dalla parola inglese "**fishing**" (**pescare**). La metafora è calzante: i truffatori "**gettano l'amo**" inviando email fraudolente a un vasto numero di persone, sperando che qualche vittima "**abbocchi**" e fornisca le informazioni richieste.

Questi attacchi non si basano solo su debolezze tecniche, ma sfruttano soprattutto la psicologia umana. Le tattiche più comuni mirano a manipolare le emozioni del destinatario per indurlo ad agire d'impulso, senza riflettere.



Le leve psicologiche fondamentali includono:

- **Creazione di un senso di urgenza:** L'email avvisa di un problema imminente che richiede un'azione immediata (es. *"il tuo account verrà sospeso entro 24 ore"*), spingendo l'utente ad agire senza pensare.
- **Creazione di un senso di soddisfazione:** Il messaggio comunica una notizia positiva e inaspettata (es. *"hai diritto a un rimborso fiscale"*), inducendo l'utente a cliccare spinto dall'entusiasmo.
- **Creazione di un senso di preoccupazione:** Si sfrutta l'ansia per un problema fittizio (es. *"il tuo ordine è stato annullato"*), spingendo la vittima a cercare una soluzione rapida cliccando sul link malevolo.

Quando si riceve un'email sospetta o inaspettata, è imperativo **evitare di cliccare su link o scaricare allegati** prima di aver verificato con certezza l'attendibilità del mittente. Analizzare esempi concreti di queste tattiche è il modo migliore per imparare a difendersi.

ANALISI DI SCENARI DI PHISHING COMUNI

Analizzare scenari di phishing reali è essenziale per sviluppare la capacità pratica di identificare le email fraudolente nella propria casella di posta. Di seguito sono riportati alcuni degli esempi più comuni, con le relative strategie di difesa.

Esempio 1: Phishing Bancario

Lo Scenario: Si riceve un'email che sembra provenire dalla propria banca. L'oggetto recita: *"Azione urgente richiesta: verifica il tuo account bancario!"* e il messaggio avvisa: *"Caro cliente, abbiamo rilevato un'attività sospetta sul tuo conto. Per proteggere la tua sicurezza, accedi immediatamente tramite il link qui sotto e aggiorna le tue credenziali. Se non completi questa verifica entro 24 ore, il tuo account verrà sospeso."*

La Leva Psicologica: L'email sfrutta un senso di **urgenza**, creando allarme e fretta per spingere l'utente a cliccare senza riflettere.

Strategia di Difesa: È fondamentale ricordare che **nessuna banca chiederà mai di cliccare su un link** in un'email per inserire credenziali. Inoltre, indirizzi email del mittente strani, molto lunghi o senza senso sono un chiaro segnale di allarme.

Esempio 2: Phishing da Ente Governativo

Lo Scenario: Si riceve un'email che sembra provenire da un ente governativo come INPS o Agenzia delle Entrate. L'oggetto è allettante: "*Avviso importante: il tuo rimborso fiscale è pronto!*", e il messaggio promette: "*Congratulazioni, hai diritto a un rimborso fiscale di €500. Per riceverlo, clicca sul link e compila il modulo con i tuoi dati bancari.*"

La Leva Psicologica: L'attacco fa leva su un senso di **soddisfazione**. La promessa di un guadagno inaspettato induce l'utente ad abbassare la guardia e a fornire dati sensibili.

Strategia di Difesa: Nessun ente governativo comunicherà mai l'importo di un rimborso via email né chiederà di inserire dati bancari cliccando su un link. È cruciale ricordare che **nessun ente indicherà un valore di rimborso** in una comunicazione di questo tipo. La procedura corretta è **uscire dalla mail e accedere autonomamente al sito o all'app ufficiale dell'ente**: eventuali comunicazioni importanti saranno disponibili nell'area riservata.

Esempio 3: Phishing E-commerce (Amazon)

Lo Scenario: Arriva un'email con il logo di un noto sito di e-commerce. L'oggetto genera allarme: "*Il tuo ordine è stato annullato: verifica il motivo!*" e il messaggio sollecita un'azione: "*Caro cliente, il tuo ordine recente è stato annullato a causa di un errore nel pagamento. Per risolvere il problema e completare l'acquisto, clicca qui per fornire i tuoi dati di pagamento.*"

La Leva Psicologica: L'email genera **preoccupazione** riguardo a un presunto problema con un acquisto, spingendo l'utente a cliccare impulsivamente per risolverlo.

Strategia di Difesa: È necessario seguire un processo di verifica a tre passaggi.

Primo: se non si è iscritti al servizio, eliminare subito l'email.

Secondo: se si è iscritti ma non si sono effettuati ordini di recente, eliminare l'email.

Terzo: se si ha un ordine in corso, **non cliccare mai sul link**. Uscire dall'email e verificare lo stato dell'ordine direttamente sul sito o sull'app ufficiale del venditore.

Esempio 4: Phishing da Supporto Tecnico

Lo Scenario: Un'email avvisa di un presunto problema di sicurezza con un account online (es. email, social media). L'oggetto è perentorio: *"Azione richiesta: reset della password per motivi di sicurezza!"* e il messaggio istruisce: *"Gentile utente, abbiamo rilevato un problema di sicurezza con il tuo account e per proteggerti, abbiamo bisogno di aggiornare la tua password. Clicca sul link per creare una nuova password."*

La Leva Psicologica: Viene sfruttata la **preoccupazione**. La paura che il proprio account sia stato compromesso spinge a seguire le istruzioni senza verificarne la legittimità.

Strategia di Difesa: Prima di tutto, chiedersi: *"Utilizzo davvero questo servizio?"*. Se la risposta è sì, non cliccare sul link. È possibile verificare online se il fornitore del servizio ha effettivamente subito un attacco informatico o segnalato problemi di sicurezza. La procedura sicura è accedere al servizio dal suo sito ufficiale e cambiare la password da lì, se necessario.



PROTOCOLLI DI SICUREZZA AGGIUNTIVI E BUONE PRATICHE

La sicurezza informatica è un processo continuo che richiede un'attenzione costante non solo alla gestione delle credenziali e al riconoscimento del phishing, ma anche all'ambiente digitale in cui si opera. Adottare protocolli di sicurezza aggiuntivi è fondamentale per creare una difesa a più livelli.

1. **Utilizzare una Connessione Sicura.** È essenziale evitare di accedere al proprio account di posta elettronica da **reti Wi-Fi pubbliche non protette**, come quelle di aeroporti, hotel o caffè. Queste reti sono spesso vulnerabili agli attacchi informatici e un malintenzionato potrebbe intercettare il traffico di dati, inclusi nomi utente e password.
2. **Mantenere il Software Aggiornato.** Mantenere sempre aggiornato il software di posta elettronica (client) e il sistema operativo del PC o dello smartphone è una pratica di sicurezza critica. Gli aggiornamenti rilasciati dagli sviluppatori spesso includono **correzioni per le vulnerabilità di sicurezza** note. Ignorare questi aggiornamenti lascia il sistema esposto a falle che potrebbero essere sfruttate dagli hacker per ottenere l'accesso ai dati.

Adottare questo approccio olistico non è solo una questione tecnica, ma il primo passo verso la costruzione di una vera e propria cultura della sicurezza, come vedremo in conclusione.



DIGITALMENTIS



Progetto “Digitalmentis 2” è rivolto alle Regioni per lo sviluppo delle competenze digitali dei consumatori adulti e vulnerabili di cui all’Avviso pubblico del Ministero delle Imprese e del Made in Italy (MIMIT), ai sensi dell’art. 148, Legge 388/2000 - Iniziative a vantaggio dei consumatori, art. 4, co. 1 del decreto ministeriale 6 maggio 2022; art. 4, comma 1, del decreto ministeriale del 31 luglio 2024; decreto direttoriale 29 novembre 2024.

Con la nuova Agenda Digitale si apre una nuova stagione che proietta la Regione Lazio direttamente nel futuro.

Tra gli **obiettivi principali** dell’Agenda Digitale da raggiungere entro il **2026** troviamo: colmare il gap digitale, rendendo digitalmente abile almeno il 70% della popolazione; raddoppiare la popolazione in possesso di competenze digitali avanzate; incrementare del 50% la quota delle micro, piccole e medie imprese che utilizzano specialisti ICT; raggiungere almeno il 65% di popolazione che utilizza servizi pubblici digitali; elevare all’80% la percentuale di popolazione che utilizza Internet.



ADICU aps

Ente Terzo Settore

ADICU – Associazione per la difesa dei consumatori e degli utenti – nasce da una precedente realtà associativa, costituita sin dal 2009 e vanta un bagaglio di esperienza nel settore consumeristico.

Lo scopo di ADICU aps è di rappresentare, supportare, assistere e tutelare a 360° i consumatori e gli utenti.

Sin dall'epoca, l'attuale Adicu, attraverso una rete diversificata di iniziative, si è sempre contraddistinta perseguendo **obiettivi di solidarietà** e **promozione sociale**, attività di sostegno, **formazione** e **informazione** promuovendo campagne sia a livello nazionale che locale.

L'attività svolta dall'associazione riguarda i seguenti settori: assicurazioni, sicurezza stradale, risparmio energetico, trasporti, credito e risparmio, poste, telecomunicazioni e nuove tecnologie (tv digitale, banda larga, internet), contratti, vendite fuori e dentro i locali commerciali, turismo, commercio, alimentazione, fisco e tributi,

Adicu, altresì, si rivolge e pone al centro del proprio agire **il consumatore** ed opera, favorendo la **conciliazione** tra consumatori ed aziende e **le buone pratiche** quali strumenti di difesa, mettendo a disposizione il proprio bagaglio di conoscenze e figure professionali preparate nell'approntare una risposta rapida ed efficiente alle problematiche.

Oggi **Adicu** è Associazione autonoma con propri associati e con una composita organizzazione articolata in vari sportelli su tutto il territorio nazionale; è iscritta nel **Registro Nazionale delle APS** presso il Ministero del Lavoro e delle Politiche Sociali ed è un **Associazione riconosciuta** in base alla Legge, 7 dicembre 2000, n. 383.

Per informazioni e contatti

ADICU aps

Via Val Varaita 8 - Roma - Tel.: 06.88642693 - Cell.: 393.9130788
email: segreteria@adicu.it - pec.: adicu@pec.it - sito internet: www.adicu.it
Orari di ricevimento: Martedì e Mercoledì dalle ore 15.30 alle ore 19.30