Indicazioni generali per l'utilizzo del servizio di posta elettronica

I servizi di posta elettronica offerti da CABER sono sicuri, professionali e protetti lato server da sistemi automatici Anti-malware e Antispam

Per garantire la propria sicurezza è indispensabile attrezzare la propria postazione con un sistema Antivirus aggiornato e professionale.
Infatti attraverso la posta elettronica possono essere veicolati contenuti e link che potrebbero costituire un serio pericolo per se stessi e la propria azienda.
Diversi tipi di frodi sono oggi veicolate attraverso le mail, incluse attività di **Phishing**, **Virus** e **Malware**.

La protezione più efficace si ottiene utilizzando tutte le tre linee di difesa qui descritte.

Prima linea di difesa
A livello tecnico la prima difesa è lato server, con i sistemi di analisi automatica Anti-malware e Antispam.
I nostri sistemi catturano le email contenenti virus e malware *noti*, così come contenuti di tipo **SPAM**.
Queste mail, non raggiungono mai la casella del destinatario, costituendo così un sicuro presidio nel contrasto a questo fenomeno.

Seconda linea di difesa
È rappresentata dai Firewall sulla propria LAN e dall'**Antivirus** locale.
SE la tua connessione ad Internet non è protetta da un Firewall di ultima generazione o non aggiornato, **SE non utilizzi un sistema antivirus** o l'antivirus non è aggiornato, **il livello di rischio è da considerare elevato**.
Se hai perplessità sui sistemi di protezione adottati, consulta il nostro supporto tecnico.

Terza linea di difesa
L'ultima linea di difesa è costituita dall'essere umano che è in grado di intercettare possibile minacce eventualmente sfuggite ai sistemi automatici.
Se ritieni di non essere sufficientemente preparato per utilizzare il servizio, **puoi richiedere una sessione di formazione** per acquisire le conoscenze necessarie per utilizzare il servizio con tranquillità.

Indicazioni fondamentali per un utilizzo sicuro

Credenziali
Conserva con cura le credenziali per accedere al servizio.
Modifica periodicamente la tua password per assicurarti la necessaria sicurezza.
Per una password sicura evita di utilizzare frasi o parole di senso compiuto, lunghezza di almeno dieci caratteri, mescola numeri, lettere maiuscole, minuscole e caratteri speciali.
Per violare una password di 10 caratteri che rispetti le indicazioni sopra riportate, un sistema automatizzato di "brute force" impiegherebbe 5 anni.
Ma attenzione basta calare il livello di complessità per vedere ridotto questo tempo anche a pochi minuti.
Al contrario basta aumentare la lunghezza a 11 caratteri (con rispetto delle regole di complessità) per portare il tempo necessario a 400 anni! [Fonte Security.org]

Invii multipli
Se devi inviare la stessa mail a diversi destinatari puoi inserire diversi indirizzi nel campo CC / CCN a seconda dei casi.
Tuttavia il sistema non è predisposto per invii massivi, essendo il numero dei destinatari limitato ad un normale utilizzo.

Se hai questa necessità richiedi l'attivazione del servizio di **Mailing List** che consente di inviare con un solo click la mail anche a migliaia di destinatari.

Netiquette
Netiquette è una parola inglese che unisce il vocabolo inglese network (rete) e quello francese etiquette (buona educazione).
È un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti.
Riportiamo qui i consigli di "Netiquette" per un uso intelligente della posta elettronica.
Queste indicazioni sono un sottoinsieme dele regole di **Netiquette pubblicate da Wikipedia**

---

1. Non usare l'e-mail per alcun proposito illegale o non etico.
2. Non diffondere SPAM.
3. Includere sempre l'argomento del messaggio in modo chiaro e specifico; non inviare mai e-mail prive del campo "oggetto".
4. Rispondere alle e-mail mantenendo sempre lo stesso argomento per conservare una struttura storica ordinata dei messaggi inviati e ricevuti
5. Rispettare la privacy dei mittenti/destinatari, cancellando dal testo l'eventuale indirizzo di posta elettronica del mittente (se si inoltra una e-mail quando il destinatario non dovesse conoscere il mittente originale) e utilizzando la casella Bcc o Ccn (e non quella A o Cc) se si deve inviare la stessa e-mail a destinatari che non si conoscono tra loro.
6. Non fare uso indiscriminato di parole scritte in maiuscolo (esse, infatti, corrispondono al tono di voce alto, gridato.)
7. La dimensione del messaggio da inviare non deve essere troppo grande (al posto di allegati di grandi dimensioni si possono utilizzare servizi quali NextCloud / SharedFolder offerto da CABER).
Bisogna tenere presente che la dimensione massima ammessa per gli allegati può essere diversa in base al provider di posta del mittente e del destinatario.
8. Gli allegati devono essere di formati diffusi e aperti (come .pdf o .jpeg) in modo da essere facilmente apribili con i dispositivi e i sistemi operativi più diffusi, già disponibili per la stampa.
9. Non richiedere indiscriminatamente, per qualsiasi messaggio, la ricevuta di ritorno da parte del destinatario.
10. Non allegare file con nomi eccessivamente lunghi o che contengono caratteri particolari come quelli di punteggiatura o lettere con segni diacritici, in quanto potrebbero creare problemi con alcune piattaforme.
11. Non impostare indiscriminatamente, per qualsiasi messaggio, il flag di importante e/o urgente.
12. Scrivere in modo semplice e diretto, con periodi brevi e andando a capo spesso perché gli spazi bianchi delle interlinee aiutano la lettura.
13. Fare una lista per punti se ci sono molte cose da dire: il testo così si leggerà facilmente anche su uno smartphone.
14. Non dimenticare la cortesia con una formula di saluto.
15. Firmare sempre con il proprio nome alla fine del messaggio.

Condizioni generali di utilizzo dei servizi di CABER
I servizi WEB offerti da CABER SRL, e tra questi i servizi di Posta Elettronica, sono regolati dalle **Condizioni Generali di utilizzo**.
La mancata accettazione o la violazione delle Condizioni Generali può costituire motivo di Risoluzione del Contratto con conseguente disattivazione dei servizi in essere.

Come configurare il programma locale di Posta Elettronica

Per l'utilizzo della posta elettronica solitamente si utilizzano programmi quali MS Outlook, Mail, Em Client e altri.
Ogni client di posta ha la sua propria interfaccia e modalità di configurazione, ma tutti hanno necessità di configurare alcuni parametri fondamentali, qui di seguiti elencati.
Nell'aggiunta di una nuova casella al tuo programma di Posta Elettronica, può essere richiesta la scelta tra diverse piattaforme come iCloud, Microsoft Exchange, Google ecc.
Scegliere in questo caso **"Altro" o "Account Mail"** per consentire la corretta configurazione.
Il nostro servizio, infatti non utilizza piattaforme che, in alcuni casi, hanno evidenziato problematiche nella sicurezza e nella protezione dei dati personali.

Autenticazione richiesta
L'autenticazione è sempre richiesta per accedere al servizio.
È necessario quindi indicare nella configurazione il nome utente, corrispondente all'indirizzo di posta elettronica, e la password scelta.
Per configurare il tuo programma di Posta Elettronica utilizza i seguenti parametri:

Server di posta in arrivo
Utilizza il nome server indicato all'attivazione della casella.

Crittografia obbligatoria
La crittografia permette una comunicazione sicura.
In base alle tue necessità, scegli il protocollo da utilizzare **(IMAP o POP3)** utilizzando la crittografia **SSL** o **TLS**.

POP3 Porta 995
È la porta specifica per POP3 con crittografia SSL

IMAP Porta 143
È la porta specifica per IMAP con crittografia SSL

IMAP Porta 993
È la porta specifica per IMAP con crittografia TLS

Server di posta in uscita

Utilizza il nome server indicato all'attivazione della casella.

SMTP – Crittografia obbligatoria
Nelle impostazioni avanzate della posta in uscita, è necessario abilitare la "Crittografia", in modalità Automatica, TLS o SSL.

Porta 587
È la porta specifica per la crittografia TLS.

Porta 465
È la porta specifica per la crittografia SSL

Password dimenticata: cosa fare

È possibile recuperare la password persa direttamente dalla WEB Mail, cliccando sul link Recupero Password.

L'indirizzo della WEB Mail dipende dal server utilizzato. Verificate la vostra documentazione in merito.

Indicare quindi l'indirizzo e-mail di cui si desidera recuperare la password

Per poter utilizzare questa funzionalità è necessario che nella mail box sia stata precedentemente impostato un **indirizzo e-mail di recupero**.

A questo indirizzo infatti verrà inviata una mail con un codice che potrà essere utilizzato per impostare una nuova password.

Se non è stato impostato l'indirizzo di recupero, si avrà un messaggio di errore con indicato "funzione non disponibile".

In questo caso contatta il servizio di assistenza tecnica per richiedere il RESET della password scrivendo a support@caber.srl o telefonando allo **0522 391337.**

Un tecnico del gruppo di supporto ti assisterà

In futuro ricorda di modificare periodicamente la password, in modo da mantenere privata e sicura la tua mailbox.

Per scegliere la nuova password segui queste semplici regole:

- lunghezza minima dieci caratteri
- utilizza almeno un numero, almeno una lettera maiuscola, almeno una lettera minuscola e almeno un carattere speciale
- nessun senso compiuto.

Allegati

Con il messaggio di posta elettronica potete inviare e ricevere allegati, ovvero documenti, contenuti multimediali in file di diversi formato e dimensione.
Si consideri che la dimensione eccessiva di un'e-mail potrebbe impedirne il trasporto o la consegna.

La dimensione massima delle e-mail generalmente non può essere superiore a 25MB.
Superando questo limite è possibile ricevere un messaggio di errore dal server di destinazione, con segnalazione di mancato recapito.

552 5.3.4 Error: message file too big

Per ovviare al problema è possibile eseguire diversi invii con allegati più piccoli.
Da tenere in considerazione che molti server possono rispondere con un messaggio di errore anche a diverse ore di distanze dall'invio.

Suggerimenti per l'invio di allegati

Formato
Il formato migliore per gli allegati è PDF che consente di inviare documenti e immagini in modo sicuro e senza che altri sistemi intervengano marcando il vostro messaggio come SPAM.
Infatti formati comuni come DOC e XLS, utilizzati abitualmente da applicativi tipo Office, possono contenere "codice eseguibile" e quindi sono considerati potenzialmente pericolosi.
Se possibile salvate i documenti in formato PDF e spediteli in questo formato.
Se ricevete un allegato da un'origine non sicura conviene sempre sottoporlo a scansione antivirus prima di aprirlo, anche se si tratta di un PDF.
Sistemi Operativi, alcune aziende/organizzazioni possono imporre particolari restrizioni su alcuni allegati, fino ad impedirne la visualizzazione.

Estensione allegati
I file allegati hanno un nome e una estensione (generalmente di tre caratteri preceduti da un punto).
Questo è un elenco delle estensioni file che più comunemente possono rappresentare un pericolo diretto ed immediato:
.ade, .adp, .apk, .appx, .appxbundle, .bat, .cab, .chm, .cmd, .com, .cpl, .diagcab, .diagcfg, .diagpack, .dll, .dmg, .ex, .ex_, .exe, .hta, .img, .ins, .iso, .isp, .jar, .jnlp, .js, .jse, .lib, .lnk, .mde, .msc, .msi, .msix, .msixbundle, .msp, .mst, .nsh, .pif, .ps1, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vhd, .vxd, .wsc, .wsf, .wsh, .xll.
Non inviate quindi allegati con questo formato.

Se ricevete un allegato con una di queste estensioni non apritelo mai.
Bisogna tuttavia sapere che anche allegati di tipo **.zip** e **.pdf** abitualmente utilizzati per condividere documenti e altri contenuti, posso rappresentare un serio pericolo.

I file **.pdf**, anche se universalmente utilizzati, possono includere codice eseguibile (quindi malware).
Verificate quindi sempre che l'origine della mail sia conosciuta e affidabile.

Formato sconosciuto
Se avete ricevuto un allegato di formato sconosciuto non tentate di aprirlo e considerate la possibilità di consultare un esperto prima di farlo.

Doppia estensione
Allegati che presentano doppia estensione (ad esempio documento.doc.exe) sono da considerare assolutamente pericolosi. Rivolgetevi ad un esperto prima di aprirlo o tentare di aprirlo.

Dimensione

Mantenete gli allegati ad una dimensione minima: ciò velocizzerà il trasporto e non creerà problemi al vostro destinatario.
Evitate di comprimere gli allegati. Oggi comprimere gli allegati non è più una pratica consigliata e potrebbe far marcare la vostra e-mail come possibile SPAM.

Come inviare una mail per l'analisi
Se avete deciso di consultare un esperto o il nostro servizio di Assistenza Tecnica per sottoporre ad analisi una e-mail che vi sembra sospetta, inviatela come allegato.
Ciò si può ottenere dal vostro client di posta, creando una nuova mail e trascinando dentro a questa la mail da analizzare.
Così saranno meglio conservate le *intestazioni tecniche* delle mail, con migliori possibilità di analisi,

APPROFONDIMENTI

SMTP di cosa si tratta

SMTP è l'acronimo di "Simple Mail Transfer Protocol" (Protocollo Semplice per il Trasferimento della Posta).
Si tratta del protocollo utilizzato dai server di posta per la spedizione delle e-mail, una specie di postino virtuale che provvede a consegnare le tue e-mail al destinatario, attraverso Internet.

Come Funziona l'invio di mail

Preparazione del Messaggio
Quando scrivi una mail e la invii, il tuo programma di posta elettronica inizia a preparare il messaggio. Questo include l'indirizzo del destinatario, l'oggetto e il contenuto.

Contatto con il Server SMTP
Dopo aver cliccato su "Invia", il tuo programma di posta elettronica entra in contatto con il tuo server di posta in uscita (server SMTP).

Autenticazione
Il server SMTP richiede una identificazione per accertarsi che tu sia autorizzato a inviare mail. Questa autenticazione avviene con una negoziazione automatica, una volta impostati correttamente i parametri di connessione.

Trasmissione al Server Destinatario
Stabilito il contatto con il tuo server, il messaggio viene trasmesso al server SMTP del destinatario che sarà responsabile di consegnare l'e-mail alla casella di posta corretta.

Consegna al Destinatario
Il server SMTP del destinatario consegna l'e-mail alla casella di posta del destinatario
Il destinatario può quindi aprire l'e-mail e leggerne il contenuto.

Notifiche di Stato
Durante tutto il processo, i server SMTP comunicano tra loro per assicurarsi che l'e-mail venga consegnata correttamente.
Se ci sono problemi, riceverai notifiche di stato, come ad esempio quando l'e-mail non può essere consegnata, con specificata la causa del mancato recapito.

Tempo necessario al recapito
Solitamente l'email è disponibile sulla casella del destinatario in pochi secondi.
In casi particolari la consegna potrebbe richiedere tempi più lunghi.
Ad esempio, se il server SMTP del destinatario è Offline o è in errore, il server che spedisce tenterà la spedizione per un tempo massimo di 24 ore.
Scaduto questo termine, se la spedizione non ha potuto essere completata, verrà inviata una notifica di "Mancato recapito" con la specifica delle motivazioni tecniche che hanno impedito la consegna.
In altri casi, quando ad esempio l'email non può essere recapitata per errori nell'indirizzo del destinatario o altro, la notifica di mancato recapito è quasi immediata.

In sintesi
Il protocollo SMTP è il sistema dietro le quinte che rende possibile l'invio delle e-mail.
Funziona come un postino virtuale, assicurandosi che i tuoi messaggi raggiungano il destinatario corretto in modo affidabile.

SPAM

Lo spam (o spamming) consiste nell'invio di messaggi indesiderati o non richiesti, generalmente di carattere commerciale. Lo spam è noto anche come posta spazzatura o posta indesiderata.
Può avvenire attraverso qualunque sistema di comunicazione, ma solitamente è riferito alla posta elettronica.

I nostri servizi intercettano lo SPAM attraverso regole automatiche di analisi
Quando i messaggi sono sicuramente classificati come spam, questi vengono cestinati e non raggiungono mai il destinatario.
Ma alcuni messaggi potrebbero essere messaggi legittimi che, per diverse motivazioni, hanno al loro interno dei contenuti che potrebbero farli identificare come spam.
Nel caso di dubbio, per evitare di perdere messaggi legittimi, questi vengono consegnati in forma di allegato ma contrassegnati come SPAM.
In questo caso la mail riporta un avvertimento che invita il destinatario a trattare con cautela questi messaggi che potrebbero anche contenere malware (codice malevolo).

Nel 95% dei casi le mail contrassegnate come SPAM sono illegittime.
Considerate con attenzione questa indicazione prima di considerare legittima una mail etichettata come [SPAM].
È possibile, tuttavia, esaminare l'allegato se si ha un ragionevole dubbio che possa trattarsi di una mail legittima. Molti elementi possono aiutarci ad identificare una mail fraudolenta.

Come verificare una mail contrassegnata come SPAM

Verificate con attenzione l'indirizzo del mittente
Talvolta gli spammer sono riconoscibili da un indirizzo che non è da noi conosciuto.

Verificate la firma
Solitamente le aziende utilizzano una "firma" standard, riconoscibile dalla presenza del logo o da altre caratteristiche.

Verificate gli allegati
La presenza di allegati in formato compresso con password è un sicuro indizio di una mail che potrebbe essere pericolosa.
NON aprite gli allegati se vi sembrano anche minimamente sospetti.

Verificate la presenza di Link nella mail o negli allegati
Se sono presenti Link, **prima di seguirli** verificatene il contenuto (basta andare sopra con il mouse e attendere pochi secondi per vedere apparire l'indirizzo completo).

Se la mail non vi convince
Se avete dubbi sulla legittimità della mail ricevuta **NON** seguite le istruzioni in essa contenute, **NON** aprite gli allegati e **NON** seguite eventuali link.

Se non avete sicurezza sul da farsi consultate il gruppo di Supporto tecnico dopo aver inviato una copia del messaggio per l'analisi.

SPAM – Falsi positivi

Può accadere di ricevere mail etichettate come [SPAM], anche se provengono da un mittente conosciuto e legittimo.

Questa condizione si può riscontrare quando si verificano uno o più eventi di questo tipo:

- **Il server di posta del mittente è mal configurato.**
  Ad esempio non ha configurato le opzioni che garantiscono un più alto grado di attendibilità come **SPF (Sender Policy Framework)** e **DKIM (DomainKeys Identified Mail)**
- **Il Client di posta utilizzato dal mittente è mal configurato.**
  Ad esempio non utilizza correttamente le impostazioni previste o utilizza un server differente per spedire.
- **Il Server di posta del mittente è catalogato in Black List** (Liste nere) internazionali tipo SpamCop, Network Abuse Clearinghouse e altre.
- **Il contenuto delle e-mail fa uso di espressioni tipiche dello SPAM.**
- **Uno o più allegati appartiene alla lista degli allegati proibiti** in quanto possono contenere codice eseguibile malevolo.

Prestiamo un'assistenza puntuale e sicura a tutti gli utenti che utilizzano i nostri servizi. Tuttavia ovviamente, non possiamo assistere coloro che utilizzano altri servizi, non da noi erogati.

Se occasionalmente verificate un evento di Falso Positivo, questo significa che il sistema Antispam funziona nel migliore dei modi.
Quando il sistema classifica in modo certo una mail come illegittima o pericolosa, questa non viene neppure catalogata come [SPAM] ma viene direttamente respinta al mittente con uno specifico messaggio.

Il 99,5% dello SPAM non è quindi neppure visibile all'utente.
Ciò che viene classificato come [SPAM] è quel residuo 0,5% per il quale permane un dubbio interpretativo. Per questo motivo viene inoltrato al destinatario per evitare che e-mail legittime possano andare perdute.
Il tag [SPAM] quindi non significa necessariamente che la mail sia illegittima o pericolosa.
È responsabilità del destinatario decidere se la mail ricevuta è legittima.

Nel dubbio
Se siete in dubbio, prima di aprire qualsiasi e-mail e i suoi allegati, consultate il nostro servizio di supporto, sempre disponibile anche via **WhatsApp 339 6272451**

e-mail non classificate
Da ultimo si consideri anche che e-mail non classificate come [SPAM] potrebbero comunque essere illegittime o pericolose. Infatti, il servizio Antispam intercetta tutte le e-mail che hanno contenuti o condizioni note come pericolose; non può intercettare nuove minacce che sfruttano vulnerabilità non ancora identificate.

Per aumentare il grado di sicurezza del servizio sono disponibili specifici corsi di formazione erogati anche da remoto.
La sessione formativa dura all'incirca un'ora e fornisce tutti gli elementi utili a identificare chiaramente le casistiche più frequenti.

Per le aziende formazione e aggiornamento sono obbligatori e dovrebbero essere ripetuti con cadenza almeno annuale per essere sempre informati sulle nuove minacce e assolvere gli obblighi di protezione previsti dalle disposizioni Europee per chi utilizza servizi WEB.

Phishing

Secondo la definizione fornita da Wikipedia

> il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Il Phishing può essere attuato anche via e-mail, inviando una e-mail che si presenta come proveniente da una banca, da un'organizzazione o anche da un servizio di posta elettronica, che richiede di seguire un link per evitare, ad esempio, la sospensione del servizio. I nostri sistemi automatici antispam identificano le mail sicuramente fraudolente e le distruggono. L'antispam è un sistema di intelligenza artificiale che assegna un "punteggio" alla possibilità che una mail sia o non sia SPAM.
Quando l'identificazione non è certa il sistema impacchetta la mail in un allegato e invia la mail al destinatario al fine di evitare che mail legittime possano andare perdute.

In questo caso la mail conterrà, oltre all'allegato, un testo simile a questo:
Messaggio Automatico
I servizi antispam hanno identificato il messaggio allegato come possibile SPAM.
Utilizzare particolare attenzione qualora il messaggio provenisse da origine non conosciuta.
Il messaggio infatti potrebbe essere non sicuro e contenere malware.
Qualora l'allegato non fosse visibile potrebbe essere necessario spostare la mail in una cartella differente del client di posta.

Nel 95% dei casi le mail contrassegnate come SPAM sono illegittime
È possibile, tuttavia, esaminare l'allegato per verificare se si tratta di una mail legittima o meno.
Molti elementi possono aiutarci ad identificare una mail fraudolenta.

Mittente
Verificate con attenzione l'indirizzo di provenienza che, ad un esame attento, potrebbe risultare del tutto inappropriato.

Link
I link sono uno degli elementi più pericolosi, in quanto sfuggono all'analisi antivirus (non contengono virus) ma possono indurci a navigare un indirizzo che potrà scaricare e attivare virus o indurci a introdurre Password o altri contenuti sensibili.
Esaminiate quindi attentamente i link presente nel messaggio senza fare click.
Per questo esame basta posizionarsi con il puntatore del mouse sul link per vedere apparire decodificato l'indirizzo di destinazione.

Testo del messaggio
Verificate il testo con attenzione. Spesso Hacker e spammer commettono grossolani errori lessicali che ci fanno prontamente identificare la mail come fraudolenta.

Allegati
Gli allegati all'interno del messaggio ricevuto potrebbero essere ancora una volta fonte di pericolo.
In particolare un allegato compresso (in formato ZIP, TAR ecc.) deve essere considerato generalmente pericoloso, soprattutto se nella stessa e-mail viene fornita la password per aprirlo.
Infatti nessuno invererebbe un contenuto riservato protetto da password indicando al contempo nello stesso messaggio la password stessa.
Se dopo aver esaminato la mail sospetta **non siete sicuri al 100%** della sua legittimità non seguite nessuna indicazione contenuta nella mail e non aprite nessun allegato.

eMailBk.it

Servizio di Backup per la posta elettronica

Questo servizio è particolarmente dedicato alle aziende che vogliono mantenere una rigorosa gestione evitando di perdere e-mail che, per errore o per altre cause, possono essere state cancellate. Il servizio offre una soluzione sicura, efficiente e automatizzata per garantire protezione e integrità delle comunicazioni aziendali. Con la replica in tempo reale delle e-mail il tuo business non perderà mai più una conversazione critica.

Caratteristiche Principali

Backup in Tempo Reale

Ogni e-mail, inviata o ricevuta, è automaticamente replicata su una infrastruttura dedicata, senza interruzioni del servizio.
Replica immediata e trasparente, priva di impatto sulle prestazioni del sistema.

Sicurezza e Crittografia

Comunicazioni crittografate end-to-end, garantiscono la protezione delle comunicazioni durante la trasmissione e l'archiviazione.
Protezione del servizio con codici univoci, assicurando anonimato e riservatezza.

Accesso Riservato all'IT Manager

Solo il responsabile IT o una figura autorizzata dall'azienda potrà accedere al sistema.

Infrastruttura Solida

Basato su standard industriali consolidati, e su un dominio di secondo livello dedicato (emailbk.it), il servizio offre stabilità e affidabilità, con un'infrastruttura riservata per ciascuna realtà.
Disponibilità e stabilità garantita del servizio H24.

Conformità alle normative europee e aziendali

Il sistema è progettato per essere conforme alle normative europee sulla protezione dei dati (GDPR), con strumenti per il controllo e la gestione sicura del servizio la cui gestione è affidata esclusivamente all'IT manager aziendale o al personale autorizzato.
Al di là delle impostazioni iniziali, il sistema è integralmente gestito in via esclusiva dal personale autorizzato dall'azienda cliente che ne garantisce così la conformità del trattamento di eventuali contenuti

Vantaggi per l'Azienda

Continuità Operativa

Non perdere mai più una e-mail importante.
Il nostro sistema garantisce che tutte le tue comunicazioni siano salvaguardate e recuperabili in ogni momento.

Risparmio di Tempo

Il sistema funziona in background senza richiedere interventi manuali.
L'IT manager può accedere ai backup rapidamente in caso di necessità.

Sicurezza di Livello Aziendale

Con comunicazioni criptate e accesso riservato, i dati della tua azienda saranno sempre protetti da accessi non autorizzati.

Recupero Rapido

In caso di cancellazioni accidentali o problemi tecnici, le e-mail possono essere ripristinate rapidamente grazie alla replica in tempo reale.

Come funziona

Configurazione Semplice
Il servizio è configurato in collaborazione con il tuo team IT, integrandosi senza interruzioni con il server di posta esistente.
Replica in Tempo Reale
Ogni e-mail viene replicata istantaneamente su un server dedicato con accesso crittografato.

Chi può beneficiarne

Aziende di ogni dimensione, anche con alti volumi di Comunicazioni mail
Le aziende che dipendono da e-mail per la gestione delle operazioni quotidiane.
Settori Regolamentati
Organizzazioni che devono mantenere una rigorosa conformità normativa in termini di conservazione delle comunicazioni.
Realtà in Crescita
Imprese in crescita che necessitano di garantire la sicurezza e la continuità e la reperibilità delle proprie comunicazioni interne ed esterne.