La posta elettronica

a cura di Alberto Vasciaveo

E-mail

- Un servizio Internet molto utilizzato è quello della **posta elettronica** o ***e-mail*** (electronic mail) che permette lo scambio di messaggi tra un mittente e un destinatario attraverso computer o dispositivi mobili collegati da una rete

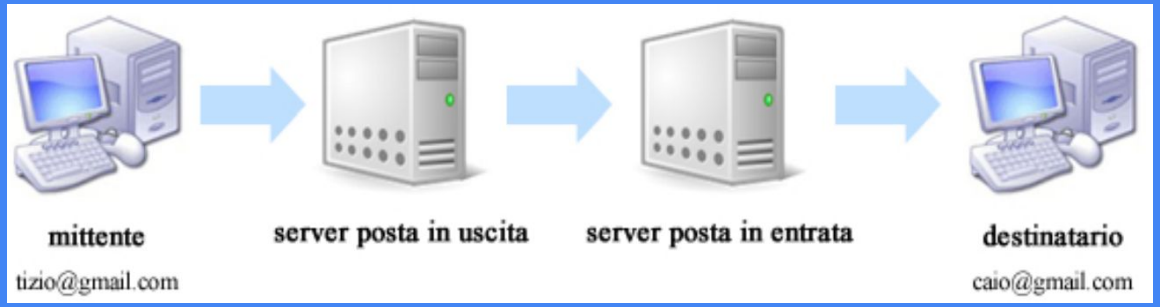
E-mail

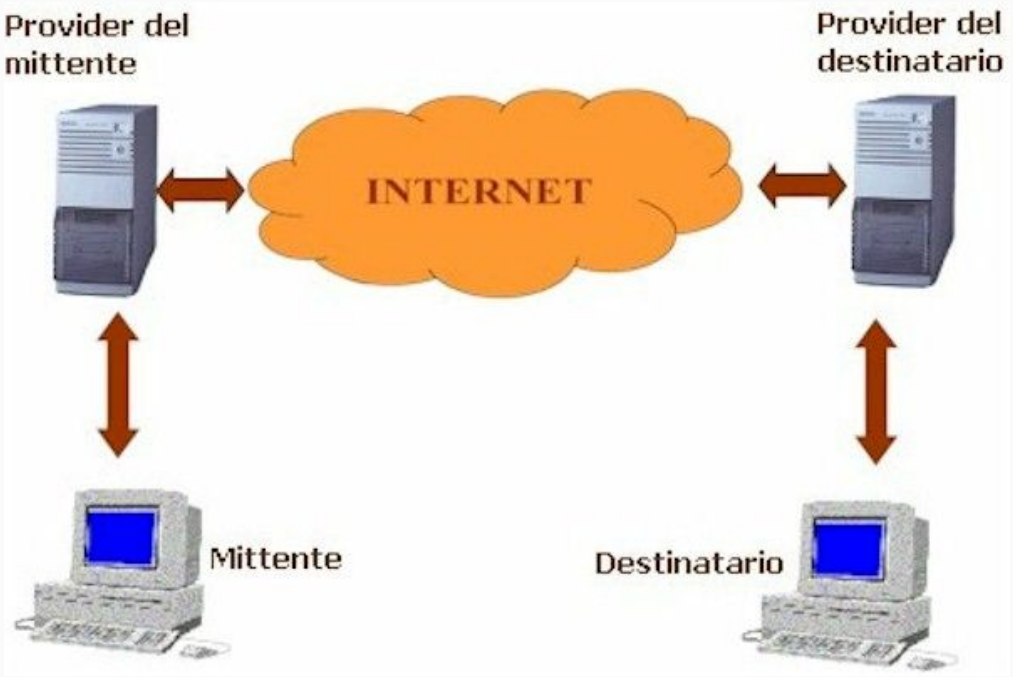
- E’ un servizio internet messo a disposizione da un fornitore di servizi chiamato ***provider***
- Per utilizzare il servizio è necessario attivare un ***account*** (nome identificativo univoco presso il provider + una password per accedere a tale servizio)

E-mail

- Ogni casella postale è caratterizzata da un indirizzo e-mail del tipo:
  - ***utente@indirizzo.xx***
    - dove utente è il nome dell'utente possessore della casella,
    - @ è il suffisso che contraddistingue l'indirizzo e-mail,
    - indirizzo.xx è generalmente l'indirizzo del provider che mette a disposizione il servizio o del dominio registrato o del dominio web a cui è associata la posta elettronica

E-mail





Tratto da www.centrostudihelios.it

E-mail

- Per utilizzare la posta elettronica abbiamo bisogno di:
  - un account registrato presso un Provider che ci fornisca il servizio di posta elettronica
  - un computer o uno smartphone connesso in internet
    - WEBMAIL: un browser per la navigazione in Internet
    - e-MAIL CLIENT: un software per la gestione della posta elettronica (Outlook, Thunderbird, ecc.) se vogliamo gestire la posta direttamente dal nostro PC

E-mail

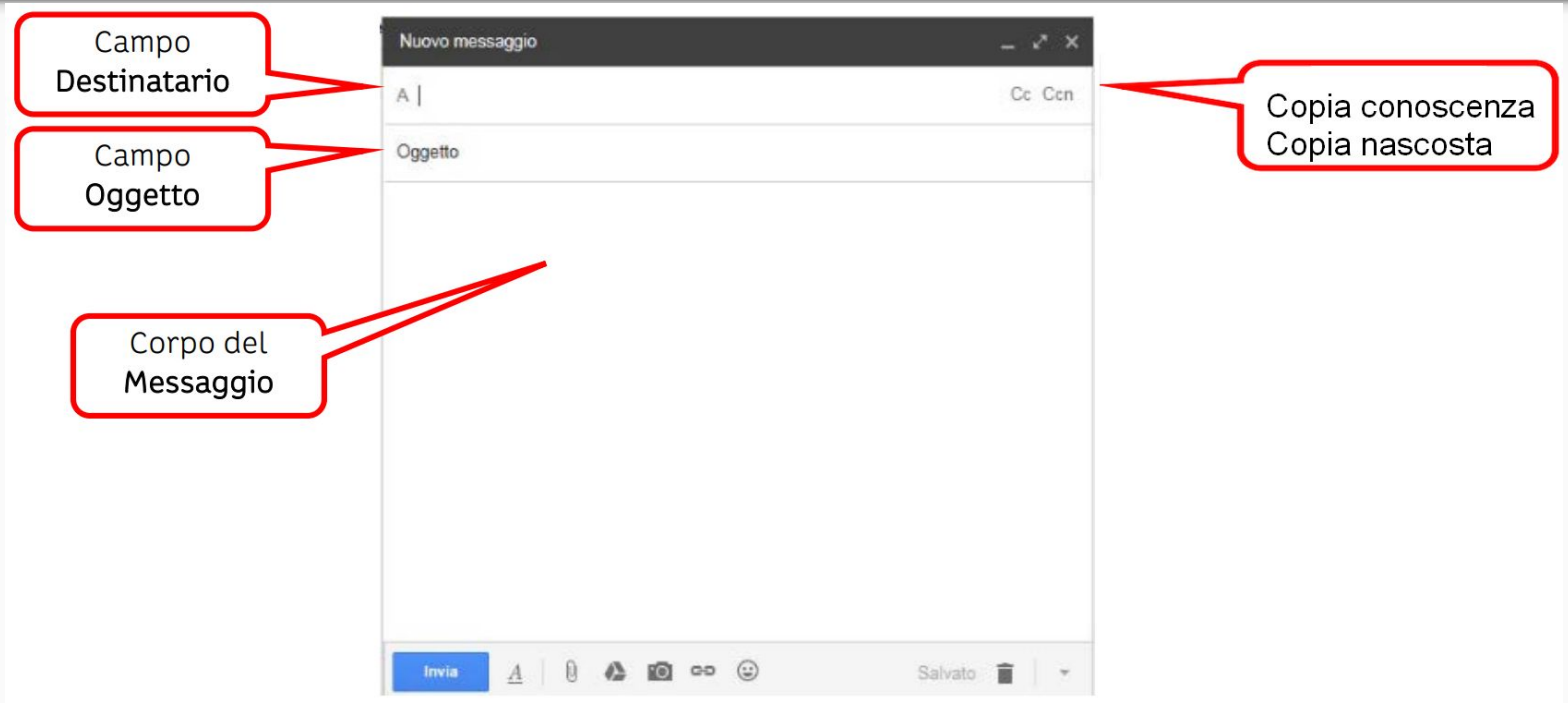
- Presenta molti vantaggi:
  - permette di inviare e ricevere messaggi da qualsiasi computer connesso ad Internet
  - i tempi di ricezione sono quasi istantanei
  - non è necessario che mittente e destinatario siano connessi nello stesso momento, in quanto il messaggio viene recapitato in una “casella” consultabile successivamente
  - si può allegare al messaggio qualsiasi tipo di file (documenti, immagini, audio/video)
  - non ci sono costi aggiuntivi oltre a quello della connessione Internet
  - si può inviare uno stesso messaggio a più destinatari contemporaneamente

GMAIL

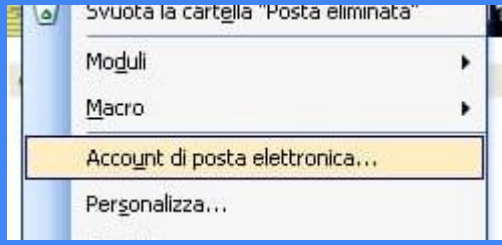
Diamo uno sguardo a come è organizzata l'interfaccia di Gmail

Tratto da https://www.paneeinternet.it/frontend/documenti/Pratica08_%20Usare_la_posta_elettronica.pdf

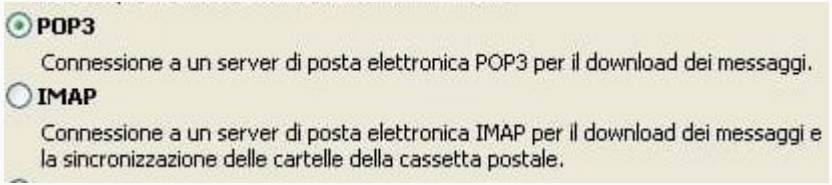
GMAIL


Campo
Destinatario
Campo
Oggetto
Corpo del
Messaggio
Nuovo messaggio
A
Cc Ccn
Oggetto
Invia
Salvato
Copia conoscenza
Copia nascosta

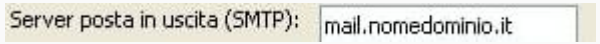
Parametri client di posta



- Per configurare il proprio client di posta è possibile registrare un account, generalmente da una apposita voce del programma utilizzato
- Per le email in entrata (per la lettura della propria casella postale) si può usare i protocolli POP3 o IMAP



- Per l'invio delle email viene utilizzato il protocollo SMTP



POP e IMAP

- **POP e IMAP** sono le modalità in cui puoi configurare l'accesso alla Posta nel programma (client) di posta del computer o nell'app su smartphone e tablet.
- Con **IMAP** (Internet Mail Access Control) i **tuoi messaggi**, sia della cartella **Posta arrivata** che di tutte le altre Cartelle, **rimangono sul server**: sul tuo computer/device mobile ne viene scaricata una copia.
- Puoi quindi **accedere alla tua casella da qualsiasi dispositivo** sia mobile che PC, purché tutti siano in IMAP, anche da **Webmail**.
- Se scegli la modalità **POP** (Post Office Protocol), **i messaggi saranno prelevati** dalla cartella Posta in arrivo del server **e scaricati in locale sul tuo PC**: **sulla Webmail quindi non ci saranno più**, a meno che non scelga nel POP l'opzione che ti permette di conservare una copia dei messaggi sul server.
- Se vuoi **consultare la posta attraverso più modalità** (per esempio un client e la Webmail oppure la webmail e diversi client o cellulari e tablet) **ti consigliamo** di configurare la casella sui client utilizzando sempre **il protocollo IMAP**.
- **Consigliamo IMAP** anche perché POP in alcuni casi potrebbe causare **problemi di sincronizzazione** di mail e Cartelle quando si accede alla casella contemporaneamente in modalità diverse.

SPAM e PHISHING

Spam e phishing

https://encyclopedia.kaspersky.it/knowledge/spam-and-phishing/

Che cos'è lo spam ?

Il termine "spam", al giorno d'oggi, è conosciuto da qualsiasi utente di Internet. Chiunque utilizzi la posta elettronica, in effetti, avrà di sicuro rilevato a più riprese la presenza di fastidiosi messaggi di spam nella propria e-mail box. Fino a qualche tempo fa, tuttavia, la parola "spam" non veniva in alcun modo associata al mondo di Internet.

Che cos'è il "phishing"?

Con il termine phishing si indica una particolare tipologia di frode in Internet; lo scopo dei malintenzionati, nella circostanza, è quello di entrare in possesso dei dati personali e confidenziali degli utenti. Più precisamente, i phisher praticano il furto di login e password, dei numeri relativi a carte di credito e conti bancari, così come di ulteriori dati riservati.

Le tematiche dello spam

Nel corso di questi ultimi anni, la quota dello spam si è stabilizzata su valori medi pari al 70-80% del volume complessivo di messaggi e-mail circolanti nel segmento russo di Internet. Ciò significa che senza un'adeguata protezione anti-spam risulta in pratica impossibile utilizzare in maniera davvero proficua ed attiva la posta elettronica.

Come prevenire l'invasione dello spam

Per l'utente privato, le problematiche connesse al diffondersi dei mailing pubblicitari (spam) iniziano nel preciso momento in cui il suo indirizzo e-mail entra a far parte dei database di cui sono in possesso gli spammer. È possibile far sì che questo non si verifichi?

Le tematiche dello spam

1. Spam “per adulti”
   - pubblicità preposte a reclamizzare prodotti farmaceutici ed affini per aumentare la potenza maschile (viagra, etc.), oppure prodotti o strumenti atti a migliorare le prestazioni fisiche. Messaggi di spam attraverso i quali si invita il destinatario dell’e-mail a visitare determinati siti, oppure visionare/acquistare materiali (video e via dicendo) o ancora siti di incontri con sedicenti spasimanti
2. Farmaci; prodotti e servizi per la salute
   - proposte più svariate e fantasiose per realizzare la perdita del peso corporeo in eccesso, per migliorare l’aspetto e la salute della pelle e dei capelli, per assumere posture corrette, oppure relative all’acquisto di integratori biologici
3. Computer e Internet
   - offerte commerciali relative alla vendita di hardware e software a basso costo, sia le offerte inerenti ai servizi rivolti ai proprietari di siti Internet, quali hosting, registrazione domini, ottimizzazione siti web, e così via
4. Finanze personali
   - offerte relative ad assicurazioni di vario tipo, servizi per la riduzione dei debiti contratti, prestiti a tasso agevolato, etc.
5. Istruzione
   - offerte relative all’acquisto di diplomi / attestati, così come le pubblicità inerenti a seminari, training di vario genere e corsi online
6. notifiche di vincite ad inesistenti lotterie online
   - ai destinatari dei messaggi vengono letteralmente promessi mari e monti, mentre, in realtà, i truffatori cercano solo di ottenere l’accesso al conto bancario dell’utente-vittima, oppure di fare in modo che quest’ultimo provveda a pagare certe inevitabili “spese preliminari”

Come prevenire l’invasione dello spam

1. **Utilizzate almeno due diversi indirizzi di posta elettronica: un account privato, per intrattenere la corrispondenza quotidiana (un indirizzo poco conosciuto, che non sarà mai reso pubblico su fonti accessibili a tutti), ed un account pubblico, destinato ad attività quali forum, chat, iscrizione a mailing list, etc.**
2. **Nel momento in cui effettuate la registrazione online a forum e chat, oppure vi iscrivete a mailing list o promozioni varie, indicate sempre il vostro indirizzo “pubblico”. Potete in effetti considerarlo preventivamente “perduto”, senza alcun patema d’animo**
3. **Non rispondete mai agli spammer. Magari non succede nulla di spiacevole. Può anche verificarsi, tuttavia, che la vostra risposta venga letta da un “robot”, il quale segnalerà poi il vostro indirizzo come attivo; in sostanza, più rispondete a simili e-mail, maggiore è la probabilità di ricevere quantità di spam sempre crescenti**
4. **Utilizzate un filtro antispam, collocato sul server di posta (avendo scelto un provider in grado di offrire il servizio di filtraggio dello spam) oppure direttamente sul vostro computer**

Che cos’è il phishing

- lo scopo dei malintenzionati, nella circostanza, è quello di entrare in possesso dei dati personali e confidenziali degli utenti.
- Più precisamente, attraverso il phishing viene praticato il **furto di login e password**, dei numeri relativi a carte di credito e conti bancari, così come di ulteriori dati riservati.
- Il phishing è costituito da messaggi e-mail fasulli, mascherati sotto forma di notifiche e comunicazioni provenienti (in apparenza!) da istituti bancari, provider, sistemi di pagamento online ed altre organizzazioni.
- In genere, per un motivo o per l’altro, viene richiesto al destinatario del messaggio di posta elettronica di comunicare / aggiornare urgentemente i propri dati personali

Esempi

Da ARUBA-S.P.A <webmaster-pec6553@36104.hostserv.eu>

A Me <info@vasciaveo.it>

Oggetto **RIFIUTO DI RINNOVO#655377**

Etichette Da tenere come esempio

Ti informiamo che il dominio -aruba.it
a cui risulta collegato questo account di posta, scadrà Il giorno 1
Desideramo ricordare che, qualora il dominio non venga rinnov
associati, comprese le caselle di posta verranno
disattivate e non potranno ou essere utilizzate per l invio e la ric

COME RINNOVARE?
Il cliente Aruba che dispone della login e della
password di accesso al dominio, potrà rinnovare semplemente

RINNOVA IL DOMINIO

https://t.co/70lnM4uAwR

Da Victoria (Federal Express) <dosbor@static.101.159.21.65.clients.your-server.de>

A Me <alvas@tiscali.it>

Oggetto **Ticket No.79186**

FedEx #79186

We have sent you a message.

An email containing confidential personal information was sent to you.

Have trouble reading this email?
Click here to open this email in your browser.

View messages

Please click unsubscribe if you don't want to receive these messages from Federal Express

http://orgaafoods.com/variano.php?utm_source=sacrilege

Da Assistenza clienti <proxad55@romani-fifa.com>

A Me <info@vasciaveo.it>

Oggetto **Notifica nuovo messaggio**

Aruba SPA

Gentile cliente
ti informiamo che il dominio a cui è collegato questo

account di posta elettronica scadrà il 19/12/2022

COME RINNOVARE IL DOMINIO?

Clicca qui

Cordiali saluti

https://s.free.fr/5GYZ3RCF

Tutto sulla Posta Elettronica

L'unico sito italiano dedicato a tutto quello che riguarda la posta elettronica. Dai trucchi ai suggerimenti, dal malware al phishing a tutte le minacce che quotidianamente ti intasano la casella di posta.

www.tuttosullapostaelettronica.it

18 elementi da controllare per scoprire un'email falsa

1 CARATTERI DEL TESTO
Uso di caratteri non standard, greci o latini, che assomigliano ai caratteri che vogliono sostituire. Ad esempio Accounт al posto di Account

2 LINGUA INGLESE
L'uso della lingua inglese per servizi che invece dovrebbero essere in italiano. Apple, Netflix o altre grosse aziende ti scrivono in italiano, non in inglese!

3 IL SERVIZIO CHE USI
La supposizione che tu abbia un account per un servizio quando invece non lo hai. Se non hai un account su PostePay, l'email che ti arriva è sicuramente un phishing.

4 LINK CON UN MODULO
Nessuno ti chiederà mai di cliccare su un link per verificare i tuoi dati. Al limite ti chiederanno di fare il login, senza link nell'email, e di verificare.

5 LA GRAMMATICA
Nessuna azienda di un certo rilievo ti scriverà mai un'email in un italiano così scorretto che se ne accorgerebbe anche un bambino di terza elementare.

6 HTTP E NON HTTPS
Tutte le aziende famose, dalle Poste a Netflix, da Apple a una qualsiasi banca, usano https e non http, soprattutto quando devi inserire dei dati.

7 LINK CAMUFFATO
Succede quando il link indica un indirizzo ma poi passandoci sopra con il mouse o cliccandoci sopra appare un indirizzo completamente differente. Segno inequivocabile di qualcosa di losco.

8 MITTENTE SOSPETTO
Se ricevi un'email da Apple, ti aspetti che chi scrive lo faccia dal dominio apple.com o apple.it, non da un dominio che è completamente differente.

9 NOTTI INFUOCATE
Se ti scrive Irina e ti promette notti di sesso infuocato è sicuramente un'email tranello che nasconde qualcosa di poco chiaro dietro. Non cascarci!

10 SCONTI RIDICOLI
Se ti propongono un paio di RayBan, per citare il caso classico, a 19.95 euro quando in negozio costano più di 200 euro, il tranello è dietro l'angolo. Sicuramente tutto falso!

11 COMPILAZIONE PDF
Pensi di firmare un'aggiornamento dei tuoi dati aziendali e invece firmi un contratto dove devi pagare una certa somma mensile a fronte di un servizio che non esiste!

12 UNITÀ DEMO
Tipico di Facebook dove, in cambio di un tuo like, ti promettono in regalo qualcosa di normalmente costoso solo perché usato come dimostrazione in negozio. Falso!

13 FATTURA VIA EMAIL
Se qualcuno ti invia una fattura via email, di solito la fattura è allegata alla stessa email. Se invece nell'email è presente un pulsante o un link allora è sicuramente un'email falsa

14 LINK PER SCARICARE
Se chiunque ti chiede di cliccare un link in un'email per scaricare qualcosa che poteva facilmente essere allegato alla stessa email, fai bene attenzione a cosa scarichi.

15 IMMAGINE E NON TESTO
Le email sono composte da testo. Se ricevi un'email che ti invita a cliccare e che non ha testo ma solo un'immagine che sembra testo, quasi sicuramente è malware o phishing.

16 SITO NON FUNZIONANTE
Tutti i siti di phishing replicano più o meno bene il sito a cui si riferiscono, ma tutti hanno menu e link non funzionanti per evitare che tu li clicchi ed esci dal sito falso.

17 SITO DIFFERENTE
Molti phisers creano una copia del sito che somiglia all'originale solo vagamente. Se sei incerto controlla sempre cercando su Google quale è il sito originale.

18 URL DIFFERENTE
Il sito delle Poste è poste.it. Se ti colleghi a un sito che dovrebbe essere quello delle Poste ma ha un url che non è poste.it è sicuramente un sito falso.

Posta Elettronica Certificata

PEC

- La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare ***e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno***, come stabilito dalla normativa (DPR 11 Febbraio 2005 n.68).
- Rispetto alla Posta Elettronica ordinaria, il servizio PEC presenta delle caratteristiche aggiuntive che forniscono agli utenti la certezza a valore legale dell'invio e della consegna (o mancata consegna) delle e-mail al destinatario:
  - ha lo stesso valore legale della raccomandata con ricevuta di ritorno con attestazione dell'orario esatto di spedizione;
  - grazie ai protocolli di sicurezza utilizzati, è in grado di garantire la certezza del contenuto non rendendo possibile nessun tipo di modifica nè al messaggio nè agli eventuali allegati.

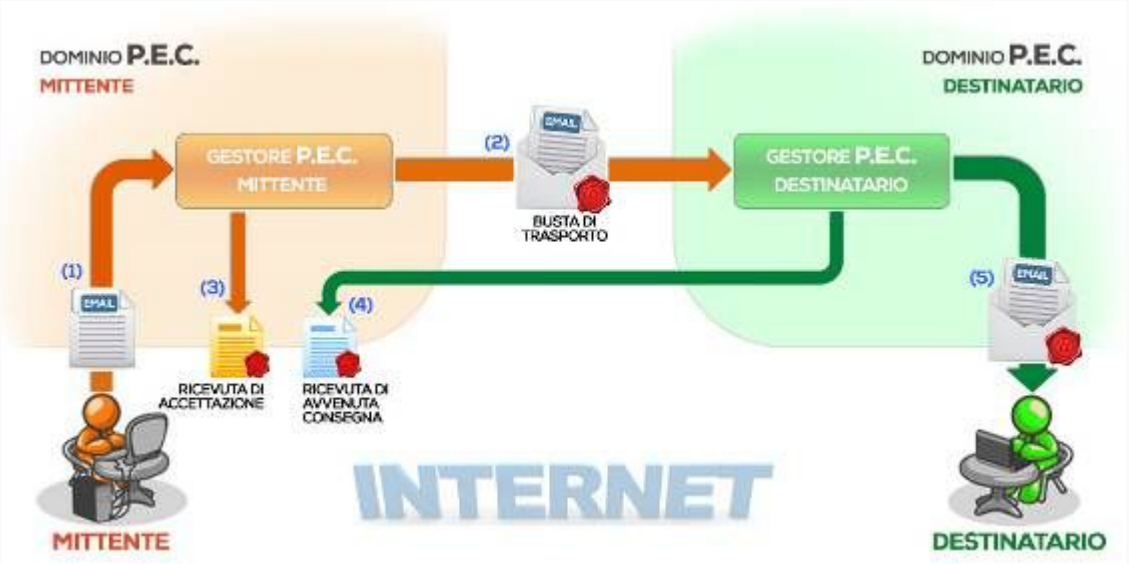
PEC

La Posta Elettronica Certificata garantisce, in caso di contenzioso, l'opponibilità a terzi del messaggio

- Il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell’avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la ricevuta di avvenuta consegna

I gestori certificano quindi con le proprie "ricevute" che il messaggio:

PEC



PEC

- In ogni avviso inviato dai gestori è inserito anche un riferimento temporale che certifica data ed ora di ognuna delle operazioni descritte.
- I gestori inviano avvisi anche in caso di errore in una qualsiasi delle fasi del processo (accettazione, invio, consegna) in modo che non possano esserci dubbi sullo stato della spedizione di un messaggio.
- Nel caso in cui il mittente dovesse **smarrire le ricevute**, la traccia informatica delle operazioni svolte, **conservata dal gestore per 30 mesi**, consentirà la riproduzione delle ricevute stesse con lo stesso valore giuridico.

PEC

FINE

Grazie per l’attenzione