segreteria@unisanpaolo.org www.unisanpaolo.org

Università Anglo Cattolica San Paolo Apostolo

GUIDA RAPIDA ALLA POSTA ELETTRONICA UNISANPAOLO

versione 4.0

Server e Gestione

La posta elettronica è un pilastro delle comunicazioni nel terzo millennio e gli indirizzi di posta concessi a ricercatori, docenti e staff sui server UniSanPaolo sono ricchi di funzionalità e possono essere utilizzati con semplicità oppure in modo avanzato.

Queste esigenze si riflettono in questa guida che va intesa come una guida di riferimento da consultare all'attivazione della propria casella UniSanPaolo e come riferimento per utilizzarne le molteplici funzionalità quando è utile o necessario.

UniSanPaolo ha preferito utilizzare un servizio esterno di posta scegliendo come gestore Aruba. Come per le comunicazioni telefoniche è sistemico e più conveniente affidarsi ad gestore di servizi con il quale implementare i propri esattamente come facciamo quando scegliamo un gestore acquistando la SIM card per i servizi di telefonia cellulare.

La posta elettronica

Le mail sono messaggi di posta elettronica, lettere trasmesse online e recapitate in termini di secondi e in tutto il mondo le mail hanno la stessa validità della posta ordinaria.

Dal punto di vista giuridico alcuni Paesi si ostinano a distinguere tra posta inviata e posta ricevuta attribuendo valore maggiore a quella di cui si può avere la prova dell'avvenuta ricezione: come in Italia la famosa raccomandata con ricevuta di ritorno sigla R.R.R..

Eppure negli anni '90 i fax sono diventati comuni e si è dovuto riconoscere ad un documento digitale validità pari ad una raccomandata cartacea con ricevuta di ritorno.

In Italia si è tentato di modificare il concetto di mail attraverso la pec (Posta Elettronica Certificata) introducendo cioè un tipo specifico di mail (inefficiente e che per questo esiste solo in Italia) che avrebbe dovuto consentire di certificare l'avvenuta ricezione.

La PEC non è mai stata adottata in altri Paesi perché è un sistema complesso che richiede sia per il mittente che per il destinatario una casella specifica attiva e funzionante. Nonostante le normative italiane il sistema pec non ha mai decollato.

Mentre i fax sono ormai inutilizzati la posta elettronica è legalmente valida quanto quella cartacea con la normativa che impone alla Pubblica Amministrazione di utilizzare mail e non più fax e sanzioni importanti per i soggetti privati che vessano gli utenti evitando di fornire indirizzi mail.

Se per la raccomandata cartacea l'avvenuta giacenza presso l'ufficio postale gli conferisce validità come se fosse stata ricevuta per estensione anche la normale mail è valida dopo un eguale periodo di “compiuta giacenza” sul server.

Inviando un messaggio di posta elettronica:

►si può richiedere al destinatario di confermarne l'avvenuta ricezione;
►si riceve immediatamente un messaggio in caso di indirizzo inesistente;
►si può considerare ricevuta dopo il termine di compiuta giacenza;

La diminuzione di spreco di carta, inchiostro e rifiuti con la posta elettronica, che possiamo utilizzare direttamente al terminale senza doverla stampare, è enorme e i benefici ecologici ed economici sono importanti visto che arriva subito, non ha costi e non richiede francobolli o alberi abbattuti.

Attualmente ogni singolo minuto vengono distrutti l'equivalente di dieci campi di calcio della foresta amazzonica generando danni ambientali non recuperabili che devono essere fermati evitando gli sprechi di risorse ed energie.

Se sbagliamo indirizzo inviando la nostra mail ad un indirizzo inesistente il server di posta ci avvisa del problema mentre in tutti gli altri casi la mail è stata correttamente trasmessa e ricevuta. Quindi ogni mail possiede pieno valore giuridico a patto naturalmente che, come per la posta tradizionale, l'indirizzo del destinatario sia corretto.

La mail può essere letta on line oppure con un software dedicato che prende il nome di client. I sistemi web-based utilizzano il programma di navigazione ma i vantaggi di utilizzare un client sono moltissimi potendolo configurare secondo le esigenze personali.

Un client permette di gestire più caselle di posta (account), può essere configurato in modo da personalizzare la posta e selezionare preventivamente quella indesiderata. Lo spam o spamming è la spazzatura, come quella tradizionale anche quella elettronica può essere intasata da pubblicità non richiesta ma quella digitale può filtrarla e salvarci.

Tra i client migliori suggeriamo Thunderbird un client Open Source gratuito e potente ma semplice da configurare e utilizzare, ampiamente personalizzabile e dotato di eccellenti funzionalità in grado di gestire un numero illimitato di account.

Anche se è possibile filtrare lo spam la casella UniSanPaolo va utilizzata solo per fini istituzionali e mai per registrazioni in rete di altro tipo per le quali ognuno può continuare ad utilizzare la propria casella personale tradizionale tipo gmail o simili.

IMAP E POP3

I server UniSanPaolo utilizzano entrambi i protocolli ma la configurazione della vostra casella di posta deve essere fatta esclusivamente con il protocollo IMAP.

IMAP è un sistema efficacissimo per condividere la posta su più dispositivi e filtrare preliminarmente quella pericolosa evitando di scaricarla indiscriminatamente sul nostro

terminale computer o smartphone.

Al contrario il protocollo POP3 è concepito per essere utilizzato su un unico terminale e scarica sempre tutti i messaggi di posta quindi se leggiamo una mail con il telefono non possiamo poi leggerla più sul computer o sul tablet e viceversa.

POP3 scarica sempre tutti i messaggi quindi è meno sicuro di IMAP che ci permette di gestire i messaggi senza scaricarli cancellando preventivamente quelli potenzialmente pericolosi senza infettare il nostro computer.

Una casella IMAP può allo stesso modo essere anche condivisa fra più persone (ad esempio un gruppo di ricerca) rivelandosi di grande utilità.

La password

Fondamentale è modificare immediatamente la password iniziale utilizzandone una adeguata da custodire gelosamente e modificarla periodicamente.

Una password di 12 caratteri richiede meno di un ora per essere decrittata dal supercomputer più potente al mondo denominato Tianhe-2 o anche Via Lattea 2 che sviluppato dall'Università Nazionale per la Tecnologia della Difesa Cinese dispone di oltre 3,12 milioni di core in processori Intel di nuova generazione i11, ma richiede qualche secolo di operazioni per un normale PC.

Tuttavia questi tempi si riferiscono a combinazioni complesse di lettere, numeri e caratteri speciali in quanto utilizzando parole di senso compiuto oppure serie di numeri il tempo di decrittazione diventa sempre per una password di 12 caratteri di soli 38 minuti per un comune computer domestico (frazioni di centesimi di secondo per Tianhe-2.

Quindi non è sufficiente che la password sia lunga ma deveanche essere composta da lettere maiuscole e minuscole inframezzate da simboli, numeri, spazi e punteggiatura compatibilmente con le richieste del server fra i quali alcuni non accettano determinati simboli oppure non distinguono maiuscole e minuscole, ecc.

Mai infine utilizzare date di nascita e nomi di parenti, animali e altre cose simili riconducibili a noi stessi.

Configurazione IMAP

Tutti gli smartphone utilizzano un client di posta che configura automaticamente i parametri necessari con poche indicazioni ma frequentemente il sistema automatico non funziona correttamente ed è indispensabile inserire manualmente i parametri da utilizzare.
UniSanPaolo utilizza come gestore Aruba quindi riporteremo estesamente elementi della guida elaborata da Aruba per la comodità dei nostri utilizzatori.

La casella di posta standard è del tipo: nome.cognome@unisanpaolo.org e al prof. Giuseppe Verdi verrà quindi assegnata la casella giuseppe.verdi@unisanpaolo.org.

Questo standard adottato da UniSanPaolo non solo consente di ricordare facilmente la propria casella di posta ma anche di comunicare facilmente con altri docenti UniSanPaolo dei quali sarà sufficiente conoscere il nome e il cognome.

Da Regolamento vengono considerati esclusivamente il primo nome e il primo cognome mentre le eventuali vocali o consonanti accentate sono trasformate in caratteri semplici non essendo queste riconosciute dal sistema mondiale di posta elettronica.

IMPOSTAZIONI SERVER DI POSTA IN ARRIVO

Posta in Arrivo (IMAP): imaps.aruba.it
Nome account: indirizzo di posta (nome.cognome@unisanpaolo.org)
Password: la password fornita inizialmente o scelta successivamente
Usa SSL: Attiva
Autenticazione: Password
Porta Server: 993

IMPOSTAZIONI SERVER DI POSTA IN USCITA

Posta in uscita (SMTP): smtps.aruba.it
Nome account: indirizzo di posta (nome.cognome@unisanpaolo.org)
Password: la password fornita inizialmente o scelta successivamente
Usa SSL: Attiva
Autenticazione: Password
Porta Server: 465

Ultimata la configurazione alcuni client di posta come quello degli smartphone Android visualizzano e sincronizzano in automatico le cartelle relative alla casella:
Sent *(per la posta inviata)*
Drafts *(bozze)*
Trash *(il cestino per la posta eliminata)*
Spam *(la casella per i messaggi indesiderati)*

Qualora la sincronizzazione non venga effettuata correttamente dal client e alcune cartelle non risultino visibili, è possibile sottoscrivere le cartelle. Per procedere è sufficiente

cliccare con il tasto destro del mouse sull'Account di interesse visualizzato nel menù a sinistra del Client, selezionare quindi la voce Sottoscrivi.. / Cartelle IMAP (è possibile che la voce indicata cambi in base al client utilizzato) e precedere alla sottoscrizione delle cartelle desiderate.

Condividere lo stesso account IMAP

Utilizzando il protocollo IMAP4, i messaggi di posta rimangono salvati sul server e da ogni terminale con il quale l'utente si collega alla posta, tramite client o WebMail, possono essere visualizzati e gestiti.

Nei casi di condivisione della stessa casella da più terminali personali (smartphone, pc, tablet) o quando più persone condividono lo stesso account se anche un solo terminale o utente utilizza paramenti di configurazione POP3 anzichè IMAP (senza impostare l'opzione di 'Conserva una copia dei messaggi sul Server'), all'avvio questo scaricherà tutti i messaggi di posta in arrivo presenti sul server che non verranno più visualizzati dalle altre connessioni. È quindi fondamentale utilizzare esclusivamente configurazioni IMAP.

Caratteristiche delle mail su server UniSanPaolo

Le nostre caselle standard hanno la capacità complessiva di un Gb e possono gestire singoli messaggi sino a 100 Mb di dimensioni. La cifratura SSL garantisce trasmissioni sicure e i server UniSanPaolo dispongono di servizi antivirus e antispam che vengono configurati dai ns. webmaster oltre ai servizi selettivi antispam che possono venire configurate in locale attraverso il client personale.

Tuttavia la sicurezza non può mai essere assoluta in campo informatico quindi suggeriamo di prestare molta attenzione con i messaggi di posta elettronica in particolare quelli dotati di allegati e di non aprire mail che arrivano da mittenti esterni sconosciuti.

In casi dubbi è doveroso contattare la Segreteria.

Configurazione del client Thunderbird

Per procedere all'autoconfigurazione di caselle di posta legate al dominio del tipo **nomecasella@unisanpaolo.org** con il client Mozilla Thunderbird è necessario **aprire il client di posta** e seguire la procedura indicata:

1. Aprire il menù -**Strumenti**- in alto
2. Selezionare -**Impostazioni account**-
3. Aprire il menù -**Azioni account**- in basso a sinistra della finestra visualizzata
4. Click su -**Aggiungi account di posta**-
5. **Inserire i dati** richiesti dal form (Nome: indicare il nome esplicativo per l'indirizzo ad esempio il nome con il titolo o la qualifica [sono ammessi spazi e punti]; email: il nome della casella completo nome.cognome@unisanpaolo.org; la password relativa avendo cura di spuntare la casella: ricorda password per evitare ci venga richiesta ad ogni accesso)
6. Click sul pulsante -**Continua**-
7. **Thunderbird riconosce automaticamente** i parametri corretti
8. Click sul pulsante -**Fatto**- per confermare

Terminare l'operazione tramite il pulsante -**OK**- in basso a destra e v**erificare che il protocollo di sicurezza SSL sia abilitato sia per il Server di Posta in Entrata che in Uscita.** In caso contrario provvedere alla configurazione manuale dello stesso dalle -Impostazioni avanzate- del client di posta, scegliendo l'opzione -Utilizzare il tipo di connessione crittografata (SSL)-, sia per il Server di Posta in Entrata, che per quello di Posta in Uscita.

Sicurezza della posta

È molto importante saper gestire mail indesiderate o potenzialmente rischiose che cercano di indurre il destinatario a rispondere, indicando i propri dati personali, come ad esempio password o numeri delle carte di credito, utilizzando falsi mittenti che sembrano provenire da aziende o persone legate alla vittima.

Al fine di proteggere il proprio account è importante sapere che UniSanPaolo:

Non richiede l'inserimento di ID e password in risposta al messaggi di posta elettronica;
Non richiede l'inserimento di dati personali in risposta al messaggi di posta elettronica;
Non richiede l'inserimento di codici o PIN di carte di credito;
Non allega bollettini postali richiedendone il pagamento.

La tecnica più comune di phishing (termine che identifica le truffe attraverso la posta elettronica) è quella di inserire all'interno del messaggio, link a siti web esterni che sembrano riferirsi a siti web attendibili e spesso legati alla vittima. Consigliamo di non cliccare mai i medesimi pulsanti ma di controllare sempre l'intestazione della mail per verificare la reale provenienza del messaggio.

L'header (intestazione)

Per stabilire se un messaggio è contraffatto è fondamentale identificare il reale mittente. Il modo migliore di verificare la reale identità è quello di leggere le informazioni di autenticazione per rintracciare il reale mittente (indirizzo IP) del messaggio di posta, analizzando quanto contenuto nell'header dell'email ricevuta.

L'header è l'intestazione del messaggio e contiene informazioni relative alla "vita" dell'email, dal momento in cui viene inviata all'accettazione da parte del server destinatario, oltre alle informazioni che riguardano l'autore. Per ottenere l'Header è necessario generalmente scegliere Visualizza >> Sorgente messaggio (Thutderbird) o fare doppio click sul messaggio (Webmail Aruba).

Queste intestazioni sono etichette e codici creati dal Client del mittente e da ogni mailserver nel quale transita il messaggio: ad ogni passaggio vengono aggiunte informazioni e per questo l'header deve essere letto dal basso verso l'alto.

Per visualizzare gli header è necessario accedere alle proprietà dell'email ricevuta, operazione eseguibile da un qualunque Client di posta o dal pannello WebMail Aruba.

Esempio di header:

Return-Path	<nomecasella@nomedominio.ext>
Delivered-To	casella_destinatario@nomedominio.ext
Received	(qmail 11111 invoked by uid 11); 14 Jun 2016 10:02:22 -0000
Received	from unknown (HELO mx.xx.aruba.it) (11.11.11.111) by mx.aruba.it with SMTP; 14 Jun 2016 10:02:22 -0000
Received	from smtp.aruba.it ([22.22.22.22]) by mx.aruba.it with bizsmtp id 6a2L1t00X21B1vA01a2Lpy; Tue, 14 Jun 2016 12:02:22 +0200
Received	from nomedominio.ext ([33.33.33.33]) by smtp.aruba.it with bizsmtp id 6a2L1t00S1xJdJu01a2LV7; Tue, 14 Jun 2016 12:02:20 +0200
Date	Tue, 14 Jun 2016 12:02:20 +0200
Message-Id	<O8RAJW$84901134BDC7C45F58E8272C7AAAED58@nomedominio.ext>
Subject	Header
MIME-Version	1.0
X-Sensitivity	3
Content-Type	multipart/alternative; boundary="_=__=_XaM3_.1465898540.2A.469743.42.2397.52.42.007.568922602"
Reply-To	nomecasella@nomedominio.ext
From	"Mario Rossi" <casella_mittente@nomedominio.ext>
To	casella_destinatario@nomedominio.ext
X-XaM3-API-Version	V3(R2)
X-SenderIP	95.110.221.50
X-Spam-Rating	mx.aruba.it 1.6.2 0/1000/N

Molte di queste informazioni possono essere modificate e quindi falsificate ad eccezione delle linee Received, che sempre, almeno in parte, possono essere ritenute affidabili.

Ad esempio Received: from indirizzo (IndirizzoIP) By nome_server_mail …. è il campo indirizzo con il nome con cui si identifica il mittente al destinatario e può essere falsificato ma IndirizzoIP è effettivamente quello del reale mittente.

I campi che solitamente compongono l'header di una mail sono i seguenti:

• Return-Path: l'indirizzo mail a cui torneranno eventuali errori di recapito del messaggio
• Delivered-To: l'indirizzo e-mail del destinatario
• Received: le informazioni generate dai server in cui è transitata, come data/ora e IP
• Date: data di trasmissione della mail
• Message-Id: stringa alfanumerica seguita da @nomedominio_mittente.ext che identifica in modo la mail ed è generato dal client da del mittente
• Subject: oggetto dell'email
• MIME-Version: versione del protocollo MIME utilizzato dal mittente cioè il Multipurpose Internet Mail Extensions lo standard per il formato dei messaggi originariamente definito dall'SMTP del mittente ossia il protocollo di trasmissione delle email.
• X-stringa: campi non standard inseriti discrezionalmente e quindi inverificabili
• Reply-To: può indicare un indirizzo email diverso dal mittente per eventuali risposte
• From: indirizzo del mittente
• To: indirizzo del destinatario

Nell'header dell'esempio riportato il primo received partendo dal basso, è quello che comunemente identifica la postazione mittente; in particolare, la parte del From indica il server mittente, mentre To (o For) indica il destinatario dell'email. Gli ultimi Received, cioè quelli più in alto, mostrano il passaggio dell' email dai server che ne hanno gestito l'invio ai server che ne hanno gestito la ricezione. ***È possibile aggiungere righe Received falsificate ma solo alla fine dell'header cioè più in alto e questo le rende comunque riconoscibili.***

Gli orari indicati nell'header fanno sempre riferimento al GMT (Tempo medio di Greenwich). In Italia l'orario è GTM+1 (aggiungere un ora) o GTM+2 (aggiungerne due nel periodo dell'ora legale). L'ora locale sulla base del fuso con Greenwich è inserita dal server in automatico quindi un'attenta analisi degli orari in rapporto alla posizione dichiarata dei server può rivelare incongruenze e truffe: ad esempio se i server di transito sono dichiarati appartenenti alla stessa nazione ma gli orari GMT variano si tratta di una evidente contraffazione.

L'email spoofing

Tecnica utilizzata dagli spammer (soggetti che hanno lo scopo di inviare messaggi indesiderati in modo fraudolento contenenti ad esempio pubblicità non richiesta o virus) per falsificare l'identità dell'effettivo mittente di un messaggio. Tale metodo prevede l'invio di email con un mittente falsificato ma simile o corrispondente ad indirizzi esistenti conosciuti dal destinatario. Lo scopo è indurre chi la riceve a pensare provenga da un mittente conosciuto e affidabile persuadendo ad aprire allegati e a cliccare sui link proposti.

Ma in realtà queste email sono spedite tramite server utilizzati dagli spammer in maniera fraudolenta, generalmente dall'estero che non possono essere bloccate automaticamente. In questi casi si può riconoscere la truffa quando: appaiono notifiche o messaggi di errore/mancata consegna per cose ma fatte oppure viene segnalata la ricezione di strane email che non sono mai state spedite.

Nel caso in cui lo spammer riesca ad ottenere la password della casella, le email di Spam vengono inviate dalla casella originale che è stata violata e non da un indirizzo fittizio. In questo caso di parla di violazione casella e non più di Email Spoofing.

E' possibile che il proprio Account sia stato violato quando:
• non si riesce ad accedere oppure a cambiare la password;
• nella Posta inviata sono presenti email non spedite;
• si riscontrano modifiche nelle impostazioni personali.

Consigli per proteggersi dalla violazione Account

Utilizzare un sistema Linux.
Cambiare spesso la propria password senza riutilizzare mai le vecchie.
Effettuare accurate scansioni antivirus del proprio PC (se non Linux).
Utilizzare password sicure da almeno 12 caratteri a caso fra lettere, numeri e simboli.
Non condividere la password sui siti web.
Non usare password soggettive con nome, cognome, anno di nascita o simili.
Analizzare gli header in caso di dubbio o mittenti sconosciuti.
Controllare periodicamente i dati personali del proprio Account.
Conservare le password in modo sicuro e non su file presenti sul pc (SpyWare).
Non cliccare mai sui link contenuti nelle email se non si è certi della provenienza.
Farsi aiutare nei casi dubbi.

Webmail

Ogni gestore di posta elettronica mette a disposizione un sistema on line di controllo della posta, il gestore scelto da UniSanPaolo non fa eccezione e il proprio account di posta può essere gestito on line dall'indirizzo http://**webmail.aruba.it**.
I questa pagina inseriremo il nome completo della casella

(giuseppe.verdi@unisanpaolo.org), la password e selezioneremo la versione completa per accedere a tutte le funzioni.

https://guide.hosting.aruba.it/email-aruba/utilizzo-email-aruba/webmail-aruba-completa-accesso-e-funzioni.aspx

Modificare la Password

Aprire il menù Opzioni in basso a sinistra e selezionare password

Quindi inserire la password attuale, quella nuova, confermarla e fare click su Salva in alto verificando il messaggio di operazione completata.

La funzione di ricerca

La funzione Cerca è utilissima e permette di trovare rapidamente cioè che cerchiamo fra i Messaggi di Posta presenti in casella.

La funzione viene eseguita su ogni elemento dei messaggi (intestazioni, mittente, destinatario, oggetto ecc…), basta immettere la parola chiave da cercare nel campo apposito, e l'operazione restituisce tutti i messaggi contenenti la parola esatta.

La Ricerca avanzata consente invece di restringere i criteri di ricerca introducendo parametri specifici ed è utile quando abbiamo molti messaggi, ad esempio se vogliamo trovare un particolare messaggio di un nostro corrispondente con il quale scambiamo molte missive non utilizzeremo il suo nome (che restituirà tutte le mail scambiate con lui) ma un particolare specifico della mail cercata (una data approssimativa, l'oggetto specifico o qualche contenuto unico).

Aggiungere una Firma ai messaggi di posta

A tutti i messaggi di posta in uscita si possono aggiungere Firme Personalizzate composte da: nome e cognome, indirizzo email, numero di telefono e qualunque altra informazione utile per contattarvi.

La Firma viene aggiunta alla email dopo l'invio e viene visualizzata dal destinatario in fondo al messaggio.

Selezionare il menù Opzioni >> Firma >> Modifica quindi:

Identificare la Firma con un titolo mnemonico (firma lavoro) inserire le righe di testo della firma e confermare con Salva.

Le firme possono essere anche più di una ma una firma unica che viene aggiunta automaticamente a tutte le email inviate e più semplice ed efficace.

La firma può anche contenere indicazioni estese e non il semplice nome e selezionando testo HTML si possono inserire formattazioni e immagini.

Gestire il Calendario

Lo strumento Calendario consente di organizzare appuntamenti o riunioni giornaliere impostandone il promemoria e creare inviti da inviare ai partecipanti.

La gestione è facile e intuitiva. Con i pulsanti in alto al pannello, è possibile selezionare una delle tre modalità di visualizzazione del Calendario: giornaliera, settimanale e mensile

Per creare un evento si posizionare il puntatore del mouse direttamente sulla data di interesse inserire i dati richiesti:

1. Nome dell'evento;
2. Luogo in cui si svolgerà l'evento;
3. Data e Ora di Inizio e Fine dell'evento;
4. Includere il Promemoria specificando la data di inizio (scelta opzionale);
5. Impostare la ripetizione della notifica per il Promemoria, se l'evento è destinato a ripetersi o meno (scelta opzionale);
6. Indicare gli indirizzi di posta dei partecipanti a cui inviare l'invito
7. Click su Salva per memorizzare l'evento.

Gli eventi possono essere modificati o rimossi.

Impostare Regole e Filtri

Questa (Opzioni >> Regole messaggi) è una funzione utilissima che permette di impostare con semplicità regole per i messaggi in arrivo filtrando ad esempio tutta la posta ricevuta

da un mittente indesiderato che verrà automaticamente cestinata.

È anche possibile attivare e disattivare temporaneamente le regole evitando di doverle reimpostare.

Blocco di email indesiderate

Se si ricevono email sospette e/o indesiderate quali spam, newsletter, email che richiedono informazioni personali ecc.., il pannello WebMail Aruba consente di bloccare questi indirizzi impostando un filtro selezionando Opzioni >> Mittenti bloccati e inserire l'indirizzo nella black list. A differenza dei filtri questa operazione blocca a priori la posta dalla lista dei mittenti inseriti senza doverla andare a cancellare.

Spazio disponibile

La WebMail Aruba permette di monitorare costantemente lo spazio utilizzato e quello ancora disponibile della casella. Per verificare lo spazio disponibile visionare le informazioni raggiungibili dalla sezione Desktop. Lo spazio disponibile per ogni casella UniSanPaolo è di un Gb mentre la massima capacità di ricezione e trasmissione è di 100 Mb per singolo messaggio. UniSanPaolo ricorda che queste caselle vanno utilizzate per scopi ufficiali essenzialmente e per lo scambio di file di grandi dimensioni è più pratico l'utilizzo di Telegram che permette di scambiare sino a 1,5 Gb.

Contatti e Gruppi

La Webmail dispone di una propria rubrica nella quale inserire i contatti con le informazioni relative che vengono salvate nel cloud del server e rimangono disponibili al proprietario ovunque e da qualsiasi terminale.

La gestione, accessibile dal menù Contatti permette anche di creare rubriche specifiche per gestire i propri contatti, oppure creare Gruppi di Persone inviando messaggi in

modalità broadcast (vale a dire: inviare un messaggio contemporaneamente a più contatti, cioè a tutto il gruppo creato).

Altre opzioni consentono di creare, importare ed esportare rubriche CSV, LDIF e anche Vcard.

Esportare e Importare Messaggi e Cartelle

Queste possibilità consentono di liberare spazio ed effettuare backup locali di singoli messaggi (formato .eml) e di intere cartelle (formato .mbox)

Ulteriori possibilità

Riguardano la creazione di cartelle specifiche, l'inoltro della posta in modo automatico ad altre caselle, l'inserimento di messaggi di risposta automatica al ricevimento delle mail, l'inserimento temporaneo di un “messaggio vacanze” per avvertire i mittenti della nostra assenza ed impossibilità temporanea di rispondere, la gestione di template personalizzati e molto altre da scoprire nelle Opzioni e nei menù specifici.