In alcuni casi, si è riscontrato un marcato senso di appartenenza alla realtà Caritas di riferimento dei dipendenti degli enti terzi (es. Cooperative, Fondazioni) e dei professionisti chiamati a svolgere attività per conto della prima. Per questa ragione alcuni di questi dipendenti o professionisti invece di utilizzare per l'espletamento delle attività Caritas indirizzi mail aziendali dei propri datori di lavoro (es. Cooperativa, Fondazione) o professionali sono stati muniti di un indirizzo mail aziendale da parte della realtà Caritas interessata, sia essa di livello regionale, diocesano o parrocchiale.
Tenuto conto della volontà del Titolare del trattamento dei dati processati da Caritas di mantenere, per il momento, questa impostazione, diretta a preservare lo spirito di appartenenza e di comunità tra i soggetti chiamati ad operare per Caritas, si è reso necessario predisporre le seguenti istruzioni dirette a fornire ai soggetti che siano stati muniti di un account di posta elettronica con dominio Caritas, sia esso declinato a livello regionale, diocesano o parrocchiale (es. @caritastoscana.it, caritasdiocesanapistoia.it), le modalità per una corretta e sicura gestione dello stesso.
Si fa presente che nel caso in cui gli operatori siano stati muniti ed utilizzino mail aziendali dei propri datori di lavoro (es. Cooperative, Fondazioni) o mail professionali (nel caso di professionisti) sarà onere di quest'ultimi provvedere a fare in modo che l'utente utilizzi detti strumenti in modo corretto e sicuro al fine di evitare che possano essere causa di compromissione di dati o dei sistemi utilizzati. In ogni caso, è fatto divieto di utilizzare mail personali.

Avv. Martina Lumini

ISTRUZIONI SULL'UTILIZZO DELLE MAIL CON DOMINIO CARITAS

MODALIÀ DI GESTIONE DELL'INDIRIZZO E-MAIL.

i. Gli account mail di posta con dominio appartenente a Caritas (es. @caritas..) sono individuali e nominativi. È possibile creare gruppi che trasmettano email a più account individuali all'uopo autorizzati (es. centrodascolto@caritasdiocesanapistoia.it). In quest'ultimo caso, nell'ipotesi di cessazione del rapporto con Caritas (es. scadenza dell'accordo con Cooperative, Fondazioni o latri enti, cessazione dell'attività di volontario o scadenza del rapporto di lavoro) l'amministratore di sistema territoriale disabilita l'inoltro ("forward") all'account nominativo di riferimento entro e non oltre 30 giorni dalla cessazione del rapporto stesso.

ii. Impostare una password di accesso alla mail aziendale robusta, da modificare annualmente, che presenti:
   - Almeno 10 (dieci) caratteri;
   - Almeno una maiuscola, non posizionata nella prima lettera;
   - Almeno un numero e un carattere speciale, non posizionati negli ultimi due caratteri della password.
   - Non contenente riferimenti personali facili da indovinare.

iii. È vietato salvare la password sul browser.

iv. Effettuare sempre il logout prima di chiudere la finestra della casella di posta.

v. Effettuare, con cadenza annuale, la pulizia della casella di posta elettronica, eliminando le mail che non si ha necessità di conservare.

UTILIZZO DELLA MAIL

La mail aziendale dovrà essere utilizzata soltanto per le attività espletate per conto di Caritas, sia essa considerata a livello regionale, diocesano o parrocchiale, pertanto, è vietato utilizzate la mail aziendale di Caritas per comunicazioni che riguardano attività non espletate per conto della stessa.
È vietato utilizzare la mail aziendale con dominio Caritas per uso personale.

DISATTIVAZIONE DELL'ACCOUNT MAIL

Nel caso di cessazione del rapporto con Caritas (es. scadenza dell'accordo con Cooperative, Fondazioni o latri enti, cessazione dell'attività di volontario o scadenza del rapporto di lavoro), l'amministratore di sistema territoriale disattiva l'account nominativo entro e non oltre 30 giorni dalla cessazione del rapporto. Contestualmente, è attivato un messaggio di risposta automatica con invito a contattare altri indirizzi e-mail.

INVIO DI DATI PERSONALI CON MAIL AZIENDALE

Nel caso in cui per esigenze organizzative e di erogazione dei servizi sia necessario uno scambio di dati personali via mail tra gli operatori chiamati a svolgere attività per conto di Caritas sarà necessario l'uso di cartelle criptate.

RACCOMANDAZIONI CONTRO LE TRUFFE A MEZZO MAIL

Si allega alle presenti alcune utili istruzioni dirette creare consapevolezza e capacità di evitare e gestire le eventuali truffe informatiche messe in atto attraverso gli indirizzi di posta elettronica (c.d. "Phishing") sulla base anche della scheda informativa pubblicata dal Garante per la protezione dei dati personali nel novembre 2020 (cfr. All. A).

Nel caso in cui qualsiasi operatore si dovesse trovare in una situazione di incertezza d'innanzi a messaggi sospetti, egli dovrà prontamente effettuare una segnalazione al proprio referente IT, se presente, al proprio referente di struttura, al titolare del trattamento all'indirizzo mail: amministrazione@caritastoscana.it e al responsabile per la protezione dati all'indirizzo mail: 3marti@live.it.

ALLEGATO A

EVITARE I PESCATORI DI DATI

CHE COS'È IL PHISHING?

Il "Phishing è una tecnica illecita per appropriarsi di informazioni riservate relative ad una persona o ad un'azienda (es. username e password, codici di accesso al cellulare) con l'intento di compiere operazioni fraudolente. La truffa avviene solitamente via e-mail ma non si esclude che possano essere utilizzati- anche sms, chat e social media. I messaggi di phishing possono:

- Invitare l'utente a fornire direttamente i propri dati personali;
- Invitare l'utente a cliccare un link che rimanda ad una pagina web dove è presente un f*orm* da compilare;
- Possono contenere allegati con virus malevoli.

Le conseguenze possono essere:

i. l'utilizzo dei dati personali carpiti (es. credenziali di accesso) per compiere attività illecite;
ii. il trafugamento di dati;
iii. danni più o meno gravi al sistema informatico in uso.

CHE COSA FARE PER TUTELARSI?

1. **IL BUON SENSO PRIMA DI TUTTO:** se si ricevono messaggi sospetti è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati che potrebbero contenere virus o programmi trojan in grado di prendere il controllo di pc e smartphone. Una piccola accortezza consigliata dal garante per la protezione dei dati è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare; in molti casi si potrà leggere, in basso a sinistra nel browser il vero nome del sito su cui si verrà indirizzati.

2. **OCCHIO AL CONTENUTO E AGLI INDIRIZZI DEI MESSAGGI:** i messaggi di phishing sono progettati per ingannare gli utenti, pertanto, spesso utilizzano imitazioni realistiche di loghi o delle pagine web ufficiali di aziende, enti etc.
   Il testo o l'oggetto di questi messaggi, inoltre, possono presentare grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. Occhio anche al mittente di questi messaggi e al suo indirizzo di posta elettronica che potrebbero essere solo apparentemente uguali a quelli reali. Es. Ipotizziamo che l'indirizzo mail reale di un dato ente con cui si collabora sia info@usltoscanacentro.it; essa potrebbe essere trasformata dal truffatore in info@toscan**o**centro.it (sostituendo la a con una o) oppure in inf**0**@toscanacentro.it (sostituendo una o con uno zero). Infine, diffidare dei messaggi con toni intimidatori (es. minaccia di sanzioni o altro) o che presentano richieste urgenti poiché potrebbero essere subdole strategie per spingere l'utente a fornire dati personali.

3. **ESSERE SEMPRE PROTETTI:** è utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Spesso i programmi e i gestori di posta elettronica hanno sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing ma è sempre buona abitudine controllare che siano attivi e verificarne le impostazioni. Attenzione a non memorizzare dati personali e codici di accesso sul browser utilizzati per la navigazione. È buona prassi, infine, creare password di accesso c.d. robuste con le caratteristiche riportate nelle istruzioni operative a cui la presente nota è allegata.

4. **NON PENSARE "A ME NON CAPITERÀ MAI!":** imparare a mettere in dubbio anche le e-mail più familiari soprattutto se ricevute da superiori o enti per cui si lavora e se contenenti richieste urgenti o intimidatorie. Fare una telefonata al diretto interessato può evitare molti rischi.