**PROGETTO S5L5, CREARE UNA EMAIL DI PHISHING**

**Da:** Alleanza Assicurazioni [<supportoalleanzaassicurazioni@libero.com>](mailto:<supportoalleanzaassicurazioni@libero.com>)

**A:** Adriano Bianchi [<Adriano.bianchi@gmail.com>](mailto:<Adriano.bianchi@gmail.com>)

**Oggetto:** Azione urgente richiesta: Assegnazione Premio Assicurativo Polizza Vita – Alleanza Assicurazioni

**Caro Cliente,**

Siamo lieti di informarti che lei è rientrato, data la sua precisione nei pagamenti e data la sua assenza da infortuni, nella nostra annuale lista di clienti premiati.

Tuttavia, per completare il processo, sono necessarie alcune informazioni aggiuntive per confermare i tuoi dati e poter procedere con l’accredito sul tuo conto bancario.

**Dettagli Premio:**  
Importo: €1.250,00  
Tipo di rimborso: Polizza Vita - Premio

Per finalizzare il rimborso premio, ti invitiamo a cliccare sul link sottostante e compilare il modulo con i tuoi dati bancari e personali, come richiesto dalla nostra politica di sicurezza.

**Ti ricordiamo che senza queste informazioni, non potremo procedere con l’accredito.**

[Conferma i tuoi dati ora](http://www.alleanzaassicurazioni-rimborso.com" \t "_new)

**Informazioni richieste:**

* Nome completo
* Codice Fiscale
* Indirizzo di residenza
* Dettagli conto bancario (IBAN, codice SWIFT, nome della banca)
* Numero di carta di credito (per verificare la tua identità)

Per una maggiore sicurezza, ti invitiamo a utilizzare il tuo codice di autenticazione per il login. Se non hai mai ricevuto il tuo codice di sicurezza, puoi richiederlo direttamente tramite il nostro servizio clienti.

**Attenzione:**  
Il termine per completare la procedura è di 24 ore, in quanto non possiamo garantire la validità dell'importo dopo tale scadenza. Ti invitiamo a non ignorare questa comunicazione per evitare il blocco del pagamento.

Se hai bisogno di assistenza, non esitare a contattarci al nostro servizio clienti all'indirizzo email **assistenzaalleanzaassicurazioni@libero.com**.

Oppure puoi contattare il team dedicato all’assegnazione del premio ai seguenti numeri:

Franca Sereni: **3512526365**

Remo Tarquini: **3512526364**

Ernesto Ugo: **3512526368**

Gianna Pelli: **3512526356**

Antonio Iddù: **3512526354**

Tina Difuori: **351252353**

Ottavio Orsini: **351252359**

Cordiali saluti,  
**Team di Alleanza Assicurazioni**  
**Supporto Clienti**

**Nota:**  
Questa email è stata inviata automaticamente dal nostro sistema. Non rispondere direttamente a questa email.

 

**SPIEGAZIONE SCENARIO**

Lo scenario di questa email è una successione di un attacco hacker al gruppo Alleanza Assicurazioni dove sono stati prelevati i nominativi e le email dei clienti della suddetta societa assicurativa nella sezione dedicata proprio alle polizze “Vita”.

L’obiettivo è di inviare contemporaneamente a 100 clienti della società la precedente email che li reinderizza ad una pagina simile a quella di Alleanza dove si troverà una pagina di accesso e successivamente una pagina dedicata all’inserimento dei dati personali, sopratutto quelli bancari.

L’email è molto credibile alla vittima in quanto la vittima stessa è proprietaria di una polizza assicurativa sulla vita, poi ci sono anche dei loghi del gruppo alla fine che potrebbero far sembrare l’email ancora piu autentica.

Inoltre sono stati inseriti dei contatti telefonici da chiamare dove risponderà un gruppo di hacker preparato a qualsiasi domanda da parte del cliente (es. Spiegazione ed erogazione del premio).

Ovviamente come sono presenti dei dettagli che possono far sembrare l’email autentica ci sono anche dei difetti che ne compromettono l’autenticità.

Partendo dall’inizio:

- **L’autenticità del contatto email del mittente**

L’email spedita dal mittente è totalmente inventata o meglio presenta la scritta “ALLEANZA ASSICURAZIONI” ma basta fare una ricerca tra i contatti della società e si può verificare che la suddetta non esiste.

- **Sito web anomalo**

Un altro dettaglio fondamentale è il sito web a cui si è indirizzati dove una volta entrati basta leggere l’URL per capire che non si tratta di una pagina ufficiale.

- **Richiesta di informazioni personali**

Ovviamente ai tempi di oggi nessuna società chiede info personali tramite email, sms o qualsiasi altro mezzo di comunicazioni anzi nelle varie pagine ufficiali o periodicamente tramite email o sms esprimono CATEGORICAMENTE di non inserire queste informazioni in quanto non sono loro a richiederle ma un cyber criminale.

**- Richiesta urgente**

Un altro allarme è la richiesta urgente di inserimento dati, in questo caso 24 ore.

Questa richiesta è una lama a doppio taglio per la vittima in quanto fa scattare un “pulsante” del tipo: “ho solo 24 ore per compilare e ricevere il premio di 1250 euro”.

Bisogna pensare lucidamente e ragionare sul fatto che nessuna compagnia, considerando anche i precedenti allarmi, dà un tempo così breve per compilare un forum specie se si tratta di un accredito bancario.

**Contatti telefonici**

Ovviamente i contatti telefonici non sono un campanello di allarme ma si potrebbero comunqe contattare e fare più domande possibili, specialmente domande complesse ed elaborate così da mettere in difficoltà la persona che si trova dall’altra parte.

**Errori grammaticali**

In alcuni casi nelle email possono esserci degli errori grammaticali (verbi, composizione delle frasi, accenti, virgole ecc.) o come in questo caso dove oltre a qualche mancanza grammaticale nella email il mittente dal del “tu” invece che del “lei”.

**CHICCA FINALE**

I nostri hacker sono dei simpaticoni.

Leggere l’iniziale di ogni nome e poi di ogni cognome.