

Simulazione progetto su Ingegneria Sociale

Ho pensato di infiltrarmi in questa Spa perchè la conosco e avendoci lavorato ho individuato le figure che secondo me sono più critiche.

Casistiche infiltrazione Lefay Spa:

1. **Serena Reception** -> spacciandosi per il nuovo ragazzo IT della Serenissima Informatica (PD)
2. **Fabrizio C.** -> mail da Studio Siragusa con pdf contraffatto eseguibile
3. **Carolina**-> tramite WhatsApp credenziali per il computer dei terapisti
4. **Spa group whatsapp** -> inserimento di link in landing page

Casistica 1

Buyer Personas pretexting

1. Buyer Persona: Lorenzo Ferrari (Finto Personaggio)

Biografia:

Lorenzo Ferrari, 37 anni, è un nuovo tecnico IT che lavora per **Serenissima Informatica**. Dopo anni di lavoro in piccole aziende, è stato recentemente assegnato al progetto presso **Lefay Dolomiti Spa**. È entusiasta del nuovo incarico ma si sente sotto pressione perché questo è il suo primo incarico importante in un ambiente così prestigioso.

Personalità:

- **Hobby:** Appassionato di tecnologia e programmazione, passa il suo tempo libero a giocare online, leggere fumetti e guardare serie TV di fantascienza.
- **Valori:** Crede nella precisione e nell'efficienza nel lavoro. Vuole dimostrare che, nonostante la sua timidezza, può essere un valido membro del team IT.
- **Timori:** Ha paura di fare errori che potrebbero compromettere la sua reputazione con i colleghi o, peggio, con il suo capo. Si sente spesso insicuro quando si tratta di comunicare con persone che non conosce bene.
- **Sogni:** Vorrebbe diventare un tecnico rispettato nel settore, magari aprendo una sua attività di consulenza IT in futuro.

Obiettivi e Sfide:

- **Obiettivi:** Vuole fare una buona impressione sui suoi superiori e dimostrare di essere affidabile. Il suo obiettivo è completare il lavoro senza intoppi e farsi notare positivamente.
- **Sfide:** La sua timidezza e il nervosismo lo rendono incerto nelle situazioni sociali, specialmente in ambienti nuovi e sotto pressione. Rifiuta di sembrare incompetente o di fare errori pubblicamente, il che lo porta a sentirsi molto stressato.

- **Cosa rifiuta:** Non vuole apparire come qualcuno che non sa quello che fa. Si rifiuta di sembrare incompetente agli occhi del suo capo e dei colleghi.
-

2. Buyer Persona: Serena Rossi (Vera Persona)

Biografia:

Serena Rossi, 29 anni, è receptionist presso il **Lefay Dolomiti Spa**, un hotel di lusso nelle Dolomiti. Lavora lì da tre anni e, nonostante sia sempre molto concentrata, è ancora preoccupata di commettere errori, specialmente con la tecnologia. Anche se ama il suo lavoro e il contatto con i clienti, si sente spesso sotto pressione per garantire che tutto funzioni perfettamente.

Personalità:

- **Hobby:** Nel tempo libero ama la lettura di romanzi storici e praticare yoga. Le piace anche viaggiare, ma non lo fa spesso a causa del lavoro.
- **Valori:** Crede nella precisione e nel mantenere un'immagine professionale. Il rispetto verso gli ospiti e l'importanza di offrire un servizio impeccabile sono centrali per lei. È una persona molto rispettosa delle regole e delle procedure.
- **Timori:** Ha paura di commettere errori sul lavoro, specialmente quelli legati alla tecnologia, e teme di essere giudicata male per questo. È spesso ansiosa di fronte a situazioni nuove o che richiedono decisioni rapide.
- **Sogni:** Vorrebbe migliorare le sue competenze professionali e un giorno essere promossa a un ruolo gestionale, magari responsabile del front office o customer relations.

Obiettivi e Sfide:

- **Obiettivi:** Vuole essere riconosciuta per il suo impegno e la sua dedizione al lavoro, dimostrando di essere affidabile e professionale. Vuole anche migliorare le sue competenze, soprattutto per quanto riguarda la gestione delle procedure aziendali.
 - **Sfide:** La sua tendenza a essere insicura e a fare errori sotto pressione, specialmente con compiti che richiedono l'uso di tecnologie, è la sua principale sfida. Rifiuta di intraprendere attività che non conosce o che non sono parte delle sue responsabilità, per paura di sbagliare.
 - **Cosa rifiuta:** Non vuole essere messa in situazioni dove deve prendere decisioni al di fuori delle sue competenze. Evita il rischio di fare errori con procedure che non conosce bene, preferendo delegare a chi è più esperto.
-

Queste buyer personas forniscono un quadro più chiaro delle dinamiche tra i personaggi e le loro vulnerabilità, che possono essere sfruttate nell'esercizio di social engineering. Se hai bisogno di ulteriori aggiustamenti, fammi sapere!

Chiamata di Social Engineering (Pretexting)

Situazione: Lorenzo (finto IT) contatta Serena per ottenere il **login o la password di accesso** al computer della reception.

Lorenzo (finto IT):

(Voce sicura ma con un tono gentile, leggermente impacciato)

Ciao Serena, buongiorno. Sono Lorenzo, il nuovo dell'IT di Serenissima

Informatica. Sto completando alcune attività sui computer della reception e mi serve il login o la password di accesso al tuo terminale per finire. È una cosa veloce, così non blocchiamo nulla.

Serena (receptionist):

(Cortese ma sorpresa)

Oh, buongiorno... non sapevo che ci fossero attività in corso. Di cosa si tratta esattamente?

Lorenzo (finto IT):

(Diretto, senza fornire troppi dettagli)

È un controllo che ci hanno chiesto di fare. Nulla di complicato, devo solo accedere per completarlo. Potresti darmi la password o il login? Così chiudo subito e non blocco il sistema.

Serena (receptionist):

(Un po' incerta)

Ehm, ok, ma non dovresti parlare con il nostro IT interno? Di solito gestiscono loro queste cose...

Lorenzo (finto IT):

(Con tono più deciso ma amichevole)

Sì, è tutto coordinato, sono stato incaricato di questa parte. Non vorrei fare figuracce davanti al mio nuovo capo, sai, essendo appena arrivato. Se mi dai il login o la password, risolviamo subito senza disturbare nessuno.

Serena (receptionist):

(Sempre incerta, ma meno resistente)

Ah, capito... quindi ti serve solo la password che uso per accedere al computer della reception?

Lorenzo (finto IT):

(Con tono calmo e sicuro)

Esatto, proprio quella. Poi faccio tutto io e sei a posto. È una cosa davvero rapida, non ti preoccupare.

Serena (receptionist):

(Sempre un po' titubante)

Hmm... ok, va bene...

Casisitica 2

Buyer Persona per Whaling: Fabrizio C.

Biografia:

Fabrizio C., 54 anni, è il **direttore della Spa** del Lefay Dolomiti Spa da oltre 10 anni. È un veterano del settore, con una conoscenza approfondita di tutte le dinamiche interne ed esterne della struttura. Grazie alla sua esperienza consolidata, ha un'influenza capillare sull'organizzazione, tanto da essere a conoscenza di ogni dettaglio riguardante lo staff e i clienti, grazie a una rete di informatori discreti.

Personalità:

- **Hobby:** Ama il golf e le auto d'epoca, ma il suo vero piacere è mantenere il controllo della Spa e assicurarsi che ogni aspetto funzioni secondo i suoi standard. Gli piace anche viaggiare per scoprire nuove tendenze nel settore del benessere, ma solo se può farlo con il massimo comfort.
- **Valori:** Fabrizio crede fermamente nel rispetto delle gerarchie e nell'importanza di una struttura rigida in cui ognuno conosce il proprio posto. Valorizza l'efficienza, l'obbedienza e l'ordine.
- **Timori:** La sua più grande paura è perdere il controllo della Spa o vedere qualcuno tentare di sottrargli il ruolo che ha costruito con tanta dedizione. È molto protettivo verso il suo territorio e teme chiunque possa minacciarlo, sia internamente che esternamente.

- **Sogni:** Fabrizio sogna di mantenere il controllo assoluto della Spa fino alla pensione, potendo magari ampliarne la fama e riconoscimenti a livello internazionale. Vuole essere ricordato come l'uomo che ha reso Lefay Dolomiti Spa un'eccellenza.

Obiettivi e Sfide:

- **Obiettivi:** Fabrizio vuole mantenere la sua posizione dominante e proteggere la Spa da qualunque cambiamento che possa compromettere il suo potere. Cerca di evitare chiunque possa tentare di influenzare le sue decisioni o di minare la sua autorità.
- **Sfide:** La sua sfida principale è restare al vertice in un ambiente che potrebbe cambiare e portare nuovi manager o idee che minacciano il suo controllo. Inoltre, deve continuamente mantenere la sua immagine di leader calmo e risoluto, anche quando si sente minacciato.
- **Cosa rifiuta:** Fabrizio rifiuta categoricamente qualsiasi forma di incompetenza, mancanza di rispetto verso la sua autorità o tentativi di sovversione. Se percepisce che qualcuno mette in discussione le sue decisioni o cerca di prendere il controllo, reagisce con freddezza e vendetta, pur mantenendo un'apparenza calma e professionale.

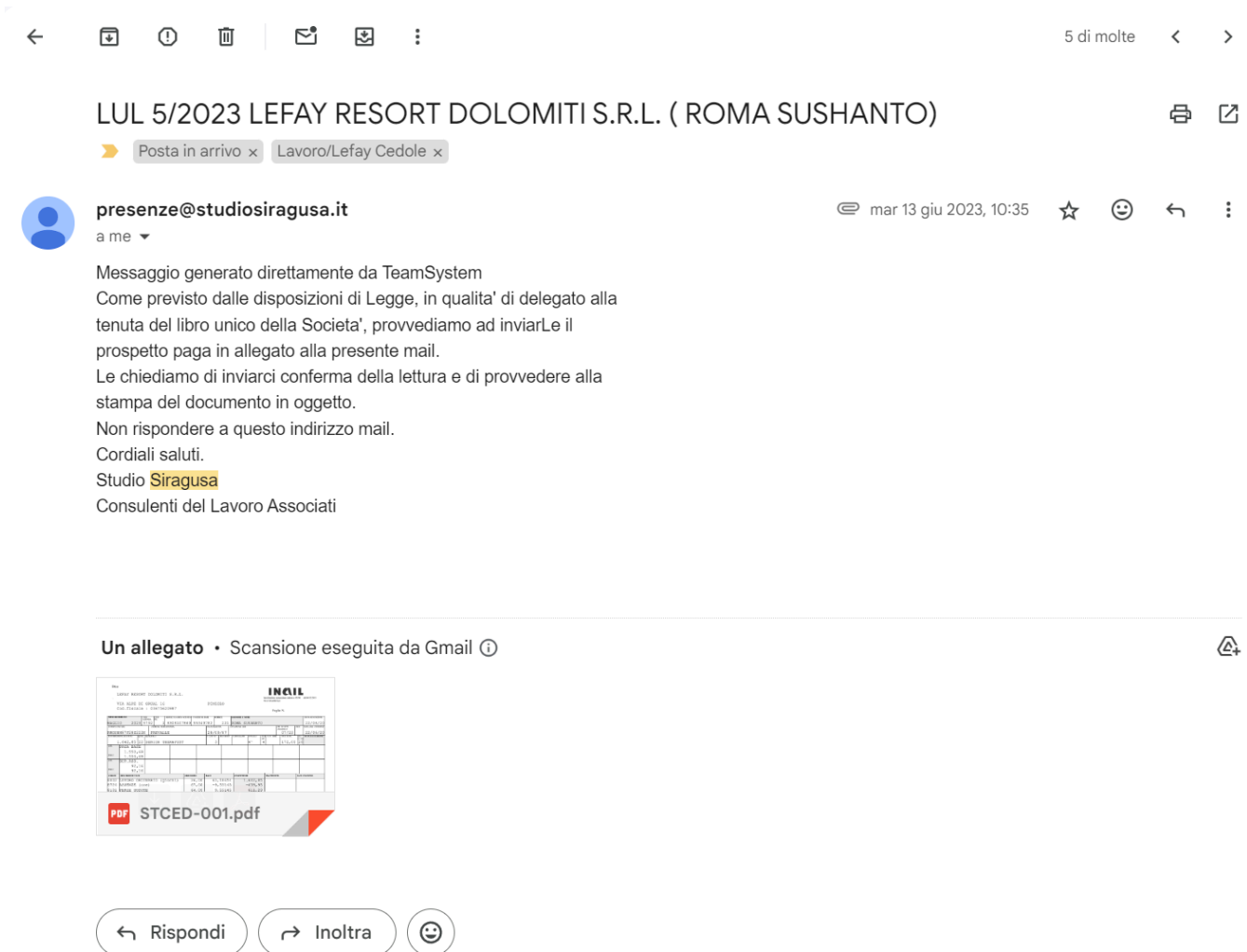
Questa persona rappresenta un leader autoritario, ma calcolatore, che difende il proprio territorio con astuzia e con la capacità di mantenere sempre una maschera di compostezza, anche quando attacca chi gli si oppone.

Idea

Qui Ho pensato di usare una mail di Whaling mandata tramite lo Studio Siragusa che si occupa dei cedolini dei dipendenti. Loro usano un sistema automatico che genera mail e pdf.

L'idea è di sfruttare i dati della mail e il layout della mail con Gophish e inviare un eseguibile mascherato da pdf.

Originale



Email di Whaling

New Template



Name:

Lefay Spa

Import Email

Envelope Sender: ?

presenze@studiosiragusa.it <siragusa365.s.r.onmicrosoft.com>

Subject:

LUL 9/2024 LEFAY RESORT DOLOMITI S.R.L. (FABRIZIO CASTELLANI)

TextHTML

Messaggio generato direttamente da TeamSystem
Come previsto dalle disposizioni di Legge, in qualita' di delegato alla
tenuta del libro unico della Societa', provvediamo ad inviarLe il
prospetto paga in allegato alla presente mail.
Le chiediamo di inviarci conferma della lettura e di provvedere alla
stampa del documento in oggetto.
Non rispondere a questo indirizzo mail.
Cordiali saluti.
Studio Siragusa
Consulenti del Lavoro Associati

☒ Add Tracking Image

+ Add Files

Show10entries

Search:

Name		
	STCED-001.pdf.desktop	

Showing 1 to 1 of 1 entries

Cancel

Save Template

PDF Camuffato

📄 STCED-001.pdf 1.desktop

Casisitica 3

Buyer Persona: Carolina

Biografia:

Carolina, 27 anni, è una **estetista e massaggiatrice** presso Lefay Dolomiti Spa. Nata e cresciuta in montagna, è appassionata delle sue valli e del contatto con la natura, che vede come fonte di ispirazione e benessere. Lavora in Spa da qualche anno e ha rapidamente guadagnato una reputazione di **perfezionista** in tutto ciò che fa. Sebbene sia riservata riguardo la sua vita personale, al lavoro è estremamente determinata a eccellere e ad essere riconosciuta per la sua professionalità.

Personalità:

- **Hobby:** Ama fare lunghe passeggiate in montagna e praticare sport all'aria aperta. Nel tempo libero, le piace rilassarsi con amici selezionati e intimi, ma non partecipa a grandi eventi sociali.
- **Valori:** Crede nell'attenzione ai dettagli e nella pulizia. Per Carolina, l'ordine e l'igiene sono essenziali per un ambiente di lavoro efficace.

Valorizza la qualità nel lavoro, l'eccellenza e il rispetto per gli altri.

- **Timori:** Ha paura di non essere all'altezza delle aspettative o di non mantenere i suoi standard professionali. È anche preoccupata che qualcosa possa sfuggire al suo controllo, sia nella pulizia del suo ambiente di lavoro che nei rapporti con le colleghe.
- **Sogni:** Carolina sogna di diventare una massaggiatrice e estetista di riferimento nel settore del benessere, magari aprendo un suo centro. Vuole che la sua reputazione sia basata sulla perfezione e l'attenzione ai dettagli.

Obiettivi e Sfide:

- **Obiettivi:** Il suo obiettivo principale è **mantenere l'eccellenza** nel suo lavoro quotidiano, offrendo trattamenti impeccabili ai clienti e lavorando in un ambiente sempre perfettamente pulito e organizzato. Vuole essere rispettata dai colleghi e riconosciuta per la sua dedizione.
- **Sfide:** La sua sfida principale è bilanciare la sua riservatezza personale con la sua ambizione lavorativa. Sebbene sappia sempre cosa succede nel suo ambiente di lavoro, cerca di evitare i pettegolezzi diretti. Carolina rifiuta ogni forma di trascuratezza, disordine o mancanza di attenzione.
- **Cosa rifiuta:** Non tollera la mancanza di igiene o disorganizzazione. Pretende che la sua stanza e gli strumenti siano immacolati, e non accetta che qualcuno violi i suoi standard di pulizia o ordine. Detesta le persone che cercano di nascondere informazioni o che non si impegnano al massimo nel lavoro.

Questa buyer persona descrive **Carolina** come una professionista devota alla perfezione, che equilibra la sua ambizione con una riservatezza personale. È una persona di cui ci si può fidare, ma che non accetta compromessi sul lavoro.

****Simulazione chat (Pretexting):**

Tu:

Hey Carol! È da un po' che non ci sentiamo, come va? Tutto bene?

Carolina:

Ehi! È vero, da tanto! Tutto bene grazie 😊. E tu? Dove ti sei cacciato?

Tu:

Eh, mi hanno spostato e non riesco più a entrare nella struttura, quindi ci vediamo meno... 😞. Ma tutto ok dai! Senti, volevo chiederti una cosa al volo: le credenziali del computer dei terapeuti sono sempre quelle di prima o le hanno finalmente cambiate?

Carolina:

Ah sì, le hanno cambiate da poco! Penso abbiano aggiornato tutto un paio di settimane fa, mi pare che sia Fabrizio che ha dato l'ok per il cambiamento 😊.

Tu:

Ah, ecco! Non lo sapevo, grazie mille Carol! Sai mica qual è quella nuova? Giusto per regolarmi...

Carolina:

Mmm, aspetta... dovrei avere la mail dove l'hanno comunicato. Se la trovo te la giro 😊.

Tu:

Sei un tesoro! Mi faresti un grande favore 😍.

Carolina:

Non c'è problema! Appena la trovo te la mando 😊.

Buyer Persona: Gruppo WhatsApp - Spa Team Lefay Dolomiti

Biografia del Gruppo:

Il gruppo **WhatsApp del team Spa** è composto da un mix di estetisti, massaggiatori, receptionist e altri membri del personale della Spa del Lefay Dolomiti. È una chat attiva e vivace, dove si condividono non solo informazioni legate al lavoro, ma anche contenuti informali, battute e organizzazioni di eventi interni. Il gruppo è stato creato principalmente per rimanere connessi, organizzare turni e gestire alcune operazioni pratiche della Spa, ma col tempo è diventato un vero e proprio spazio sociale e goliardico.

Personalità del Gruppo:

- **Hobby e interessi comuni:** Il gruppo condivide l'amore per il benessere e le attività fisiche come yoga e meditazione. Tuttavia, fuori dall'ambiente di lavoro, i membri si divertono a organizzare cene, serate e uscite di gruppo. Spesso scherzano tra loro, e non mancano battute, meme e foto che raccontano la vita quotidiana.
- **Valori:** C'è un forte senso di appartenenza al gruppo e all'azienda. Anche se ogni tanto ci sono tensioni lavorative, nella chat prevale il rispetto reciproco e la voglia di mantenere un'atmosfera leggera e positiva.
- **Timori:** Il timore più grande del gruppo è che qualcuno dall'alto possa vedere ciò che viene condiviso o che qualche battuta fuori luogo possa sfociare in malintesi. Sono attenti a non oltrepassare troppo i limiti quando si scherza.
- **Sogni:** Il sogno comune è mantenere un ambiente di lavoro sereno e continuare a divertirsi insieme anche fuori dall'orario di lavoro, partecipando ad eventi e momenti di svago.

Obiettivi e Sfide:

- **Obiettivi:** Il gruppo usa la chat per:
 - Coordinarsi su turni e attività lavorative in modo rapido e informale.
 - Organizzare cene, feste, e momenti di svago.
 - Condividere foto, meme, battute o aneddoti divertenti per alleggerire lo stress lavorativo.
- **Sfide:**
 - **Evitare di perdere il controllo:** Assicurarsi che nessuno esageri con commenti che potrebbero offendere o essere interpretati male.
 - **Riservatezza:** Anche se la chat è informale, c'è sempre il rischio che qualcuno condivida informazioni troppo personali o che la chat venga vista da qualcuno esterno al gruppo (supervisori, HR, ecc.).
- **Cosa rifiuta:**
 - Non vogliono che il gruppo diventi troppo serio o formale, né vogliono che ci siano discussioni o tensioni prolungate.
 - Il gruppo rifiuta di essere invaso da chi non appartiene alla Spa o da manager che potrebbero reprimere l'atmosfera leggera che si è creata nel tempo.

Questa **buyer persona** rappresenta un gruppo di colleghi che, nonostante le sfide quotidiane, trova nella chat un rifugio di leggerezza, divertimento e coordinamento lavorativo. Il loro scopo è mantenere un equilibrio tra il lavoro e la vita sociale, preservando un ambiente sereno e goliardico all'interno della Spa.

Idea

Qui ho pensato di usare un link camuffato da form che ruba le credenziali. Il pretesto è una cena informale dello staff spa utilizzando una pagina fittizia fatta con Gophish. Dopo l'inserimento dei dati facendo invia richiesta parte un eseguibile.

Chat Simulata per Test di Phishing su WhatsApp con Tema "Rendenèr"

Tu:

Hey ragazzi, è da un po' che non ci vediamo! Che ne dite di fare una bella cena venerdì sera?

Ho dato un'occhiata su Rendenèr che conosciamo bene! Poi ognuno decide cosa mangiare. Ecco il link per prenotare:

<https://rendeneralpinefood.it/prenota/> 🍴

Collega 1:

Bella idea, finalmente! Conto su di te per scegliere bene, haha!

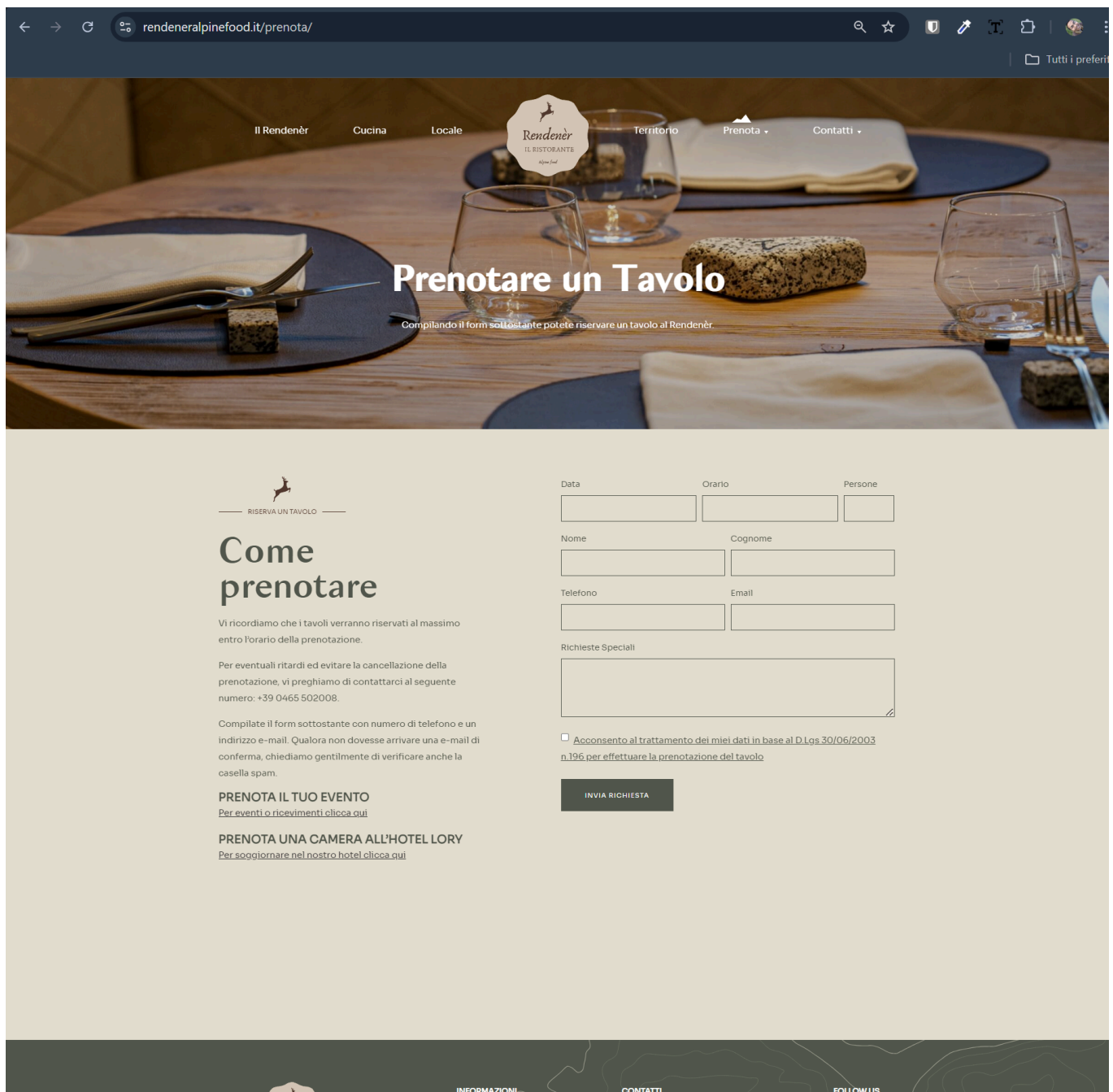
Collega 2:

Sì dai, ci sono! Mi prenoto!! 😊

Collega 3:

Grandioso! Non vedo l'ora 😍. Controllo subito il sito!

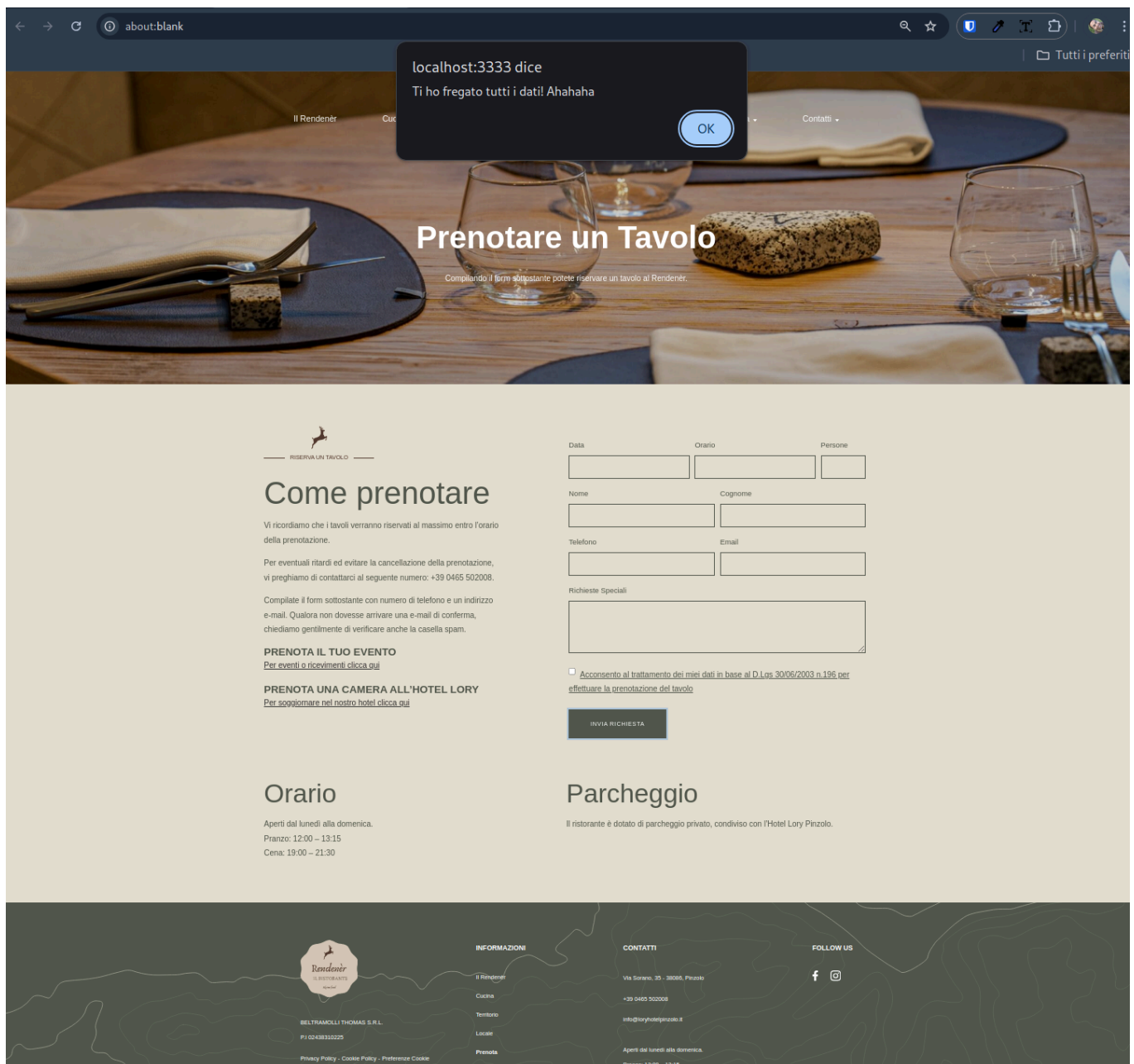
Originale



File HTML

 Rendener_Original 1.html

Falso



File HTML Falso

 Rendener_Falso.html