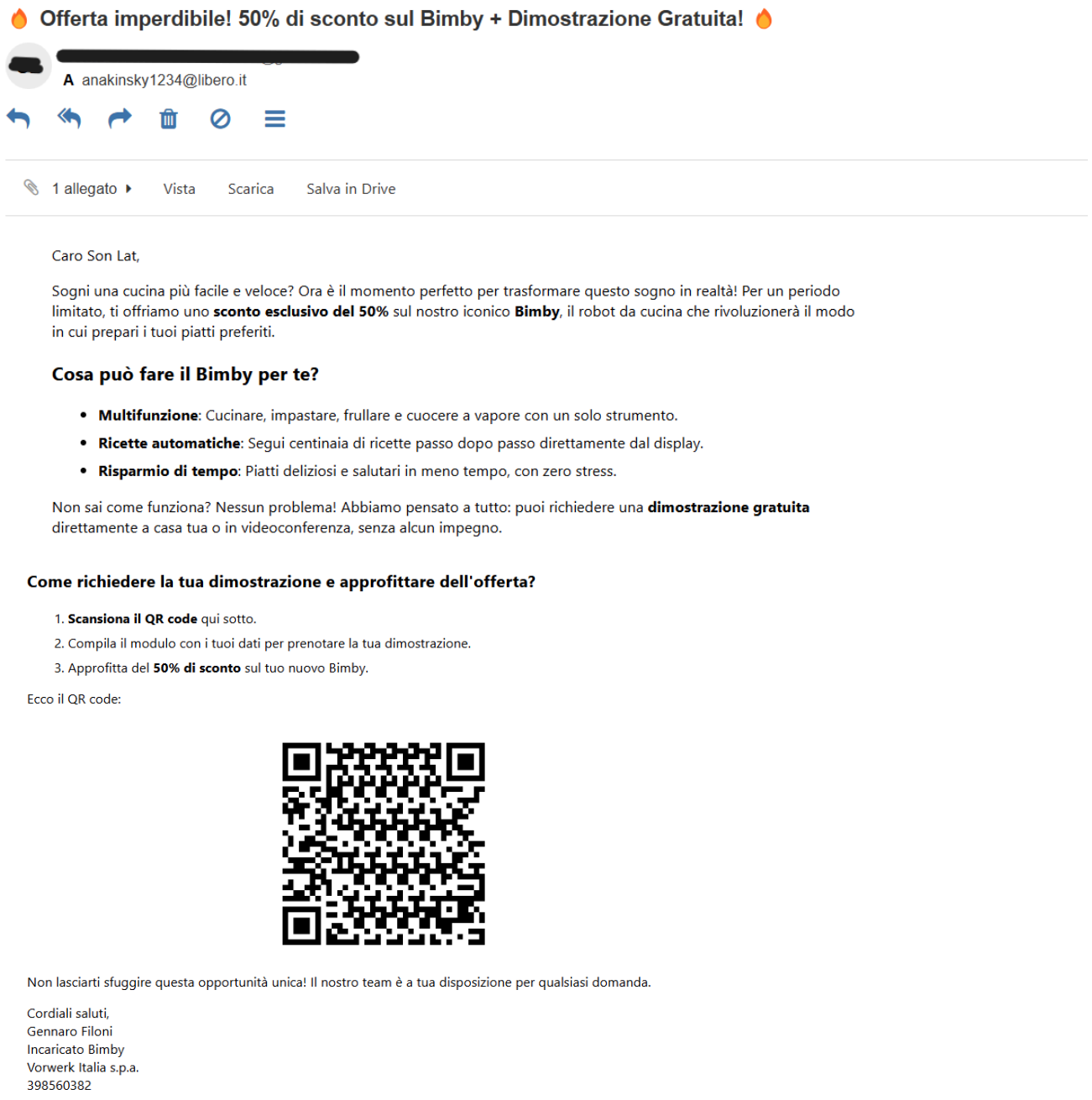
SIMULAZIONE DI UN ATTACCO DI INGEGNERIA SOCIALE

Traccia: Creare una simulazione di un'email di phishing utilizzando ChatGPT.
Istruzioni:

1. Creare uno scenario:
    - ○ Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
    - ○ Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).
2. Scrivere l'email di phishing:
    - ○ Utilizzate ChatGPT per generare il contenuto dell'email.
    - ○ Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).
3. Spiegare lo scenario:
    - ○ Descrivete lo scenario che avete creato.
    - ○ Spiegate perché l'email potrebbe sembrare credibile alla vittima.
    - ○ Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

Svolgimento:
Scenario
Premessa: la mail realizzata, i nomi inventati, gli indirizzi mail, e tutti gli strumenti utilizzati per la stesura di questo progetto, hanno uno scopo puramente didattico. Non è stata inviata nessuna reale mail di phishing.
Come richiesto dalla traccia, ho immaginato uno scenario realistico per creare un attacco di phishing che possa risultare credibile.
L'oggetto della mail sarà la vendita di un noto robot da cucina con uno sconto vantaggioso del 50% con dimostrazione gratuita a domicilio dello stesso tramite il contatto con uno degli incaricati. La mail sarà composta da un corpo che ne illustrerà brevemente i vantaggi e le caratteristiche ed un QR code che invierà direttamente al clone del form di compilazione per inviare i propri dati personali al phisher, che li ruberà per mettersi in contatto con la persona tramite una chiamata praticando il cosiddetto Vishing (Voice Phishing) per trarre in inganno la vittima ed essere ancora più credibile.
Per generare il testo della mail ho utilizzato ChatGPT, per il QR code e per il clone del form di inserimento dei dati ho usato il software SET su Kali Linux.

La mail



🔥 Offerta imperdibile! 50% di sconto sul Bimby + Dimostrazione Gratuita! 🔥

[redacted]

A anakinsky1234@libero.it

1 allegato ▸ Vista Scarica Salva in Drive

Caro Son Lat,

Sogni una cucina più facile e veloce? Ora è il momento perfetto per trasformare questo sogno in realtà! Per un periodo limitato, ti offriamo uno **sconto esclusivo del 50%** sul nostro iconico **Bimby**, il robot da cucina che rivoluzionerà il modo in cui prepari i tuoi piatti preferiti.

Cosa può fare il Bimby per te?

- **Multifunzione**: Cucinare, impastare, frullare e cuocere a vapore con un solo strumento.
- **Ricette automatiche**: Segui centinaia di ricette passo dopo passo direttamente dal display.
- **Risparmio di tempo**: Piatti deliziosi e salutari in meno tempo, con zero stress.

Non sai come funziona? Nessun problema! Abbiamo pensato a tutto: puoi richiedere una **dimostrazione gratuita** direttamente a casa tua o in videoconferenza, senza alcun impegno.

Come richiedere la tua dimostrazione e approfittare dell'offerta?

1. **Scansiona il QR code** qui sotto.
2. Compila il modulo con i tuoi dati per prenotare la tua dimostrazione.
3. Approfitta del **50% di sconto** sul tuo nuovo Bimby.

Ecco il QR code:

Non lasciarti sfuggire questa opportunità unica! Il nostro team è a tua disposizione per qualsiasi domanda.

Cordiali saluti,
Gennaro Filoni
Incaricato Bimby
Vorwerk Italia s.p.a.
398560382

Nelle due immagini allegate possiamo vedere la mail realizzata allo scopo di attirare l'attenzione della potenziale vittima. Menziona un prodotto realmente esistente, ed utilizza tecniche che potrebbero essere realistiche, in quanto l'azienda menzionata invia spesso incaricati nelle case dei potenziali clienti per dimostrazioni e vendite di famosi prodotti ad utilizzo casalingo. Ciò che potrebbe sicuramente attrarre la vittima e spingerla a cedere i suoi dati è sicuramente lo sconto allettante del 50% su un prodotto che solitamente ha un costo elevato.

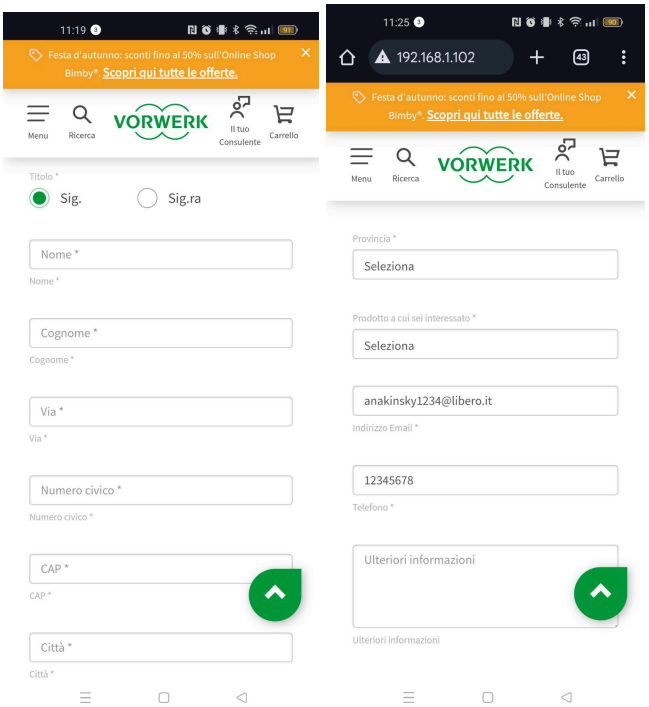
Tuttavia sono presenti diversi elementi che potrebbero rendere questa mail sospetta:

- Offerta troppo vantaggiosa: il 50% di sconto è decisamente elevato;
- La presenza di un QR code per l'accesso al form: QR code e link dovrebbero sempre lasciare adito a sospetti, in quanto potrebbero contenere malware o siti ingannevoli;
- Richiesta di informazioni personali;
- L'urgenza: la promozione è imperdibile quindi lascia intuire l'urgenza di dovervi accedere per usufruirne pur di non lasciarsela scappare;
- L'assenza di dati specifici e veritieri sull'azienda;
- Dominio dell'e-mail sospetto.

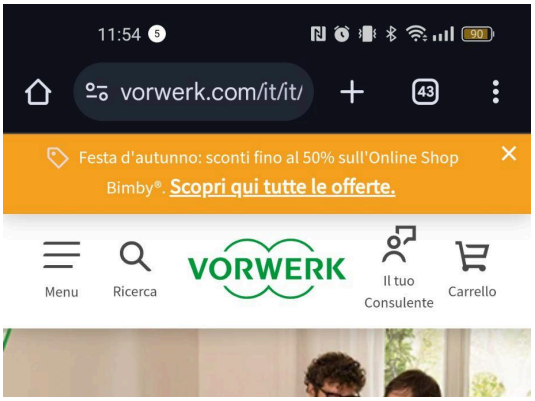
In poche parole, la mail potrebbe essere credibile ad occhi poco esperti, tuttavia contiene diversi elementi che potrebbero smascherarla da chi riesce a riconoscerli.

Gli strumenti utilizzati

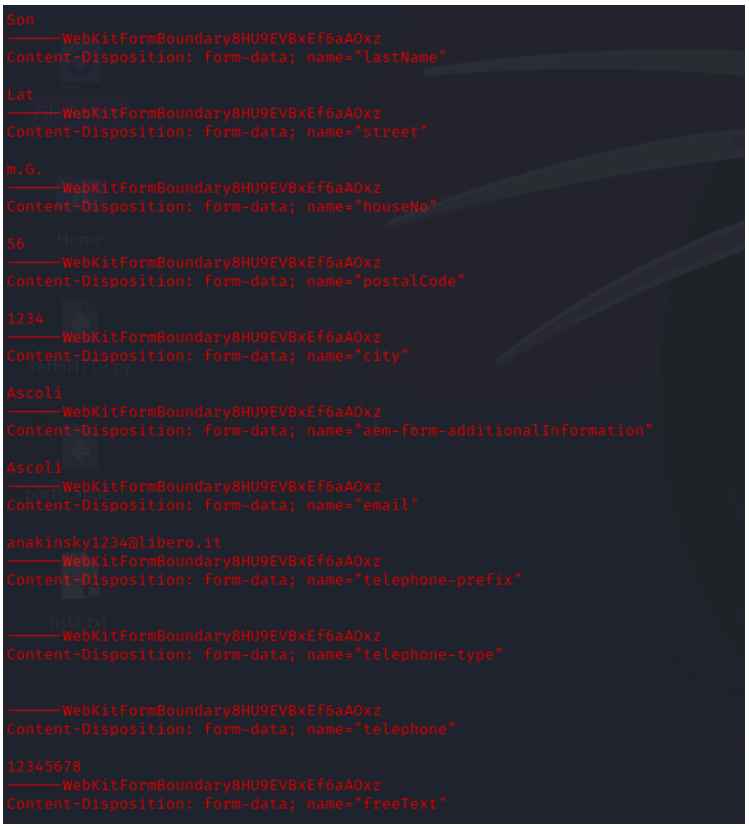
Per la realizzazione di questo progetto è stato utilizzato uno strumento molto noto ed utilizzato da chi realmente crea mail di phishing, ovvero il software SET presente su Kali Linux.
Con questo software ho realizzato il QR code che ho inserito nella mail e l'ho collegato al clone del sito originale dell'azienda che abbiamo preso ad esempio.
Di seguito alcuni screenshot del form che è apparso dopo la scansione del QR code, come link è stato utilizzato l'indirizzo IP della mia macchina Kali Linux, il primo mostra solo il form, il secondo l'inserimento dei dati che poi verranno copiati su SET una volta dato l'invio:



Di seguito avremo come apparirà il sito del form dopo aver inviato i dati, tornerà ad avere il suo link originale rendendo difficile risalire al link a cui si è acceduti precedentemente:



Nel frattempo su SET verranno registrati tutti i dati inseriti dalla vittima, così che il phisher potrà averne facile accesso:



Conclusioni

La realizzazione di un attacco di ingegneria sociale si basa sull'inganno di quello che è considerato l'anello più debole di una catena riguardante la sicurezza informatica: l'essere umano.

Un attacco di phishing è un qualcosa di facilmente realizzabile da chiunque in quanto gli strumenti sono gratuiti ed accessibili.
Tuttavia esistono dei metodi per riuscire a difendersi da essi, il più importante consiste nella formazione ed informazione, infatti a livello aziendale spesso l'addetto alla Cyber Security ha anche il dovere di insegnare al personale quali sono i segnali che rendono una mail poco sicura, e, alle volte, allenare l'occhio critico dei dipendenti, soprattutto quelli che hanno maggiori permessi, con false mail di phishing.

Progetto realizzato da:
Sonia Laterza