

# EXECUTIVE SUMMARY

Creare uno scenario di una campagna di phishing, scrivendo l'email di phishing e spiegare lo scenario.

## CONTESTO AZIENDALE REALE

Nel contesto affrontato si prende di mira un oggetto reale. Algòmera è una software house e digital agency italiana fondata nel 2014, specializzata nello sviluppo di software gestionali e soluzioni digitali su misura per aziende di vari settori.

### Attività principali:

- Progettazione e sviluppo di CRM custom per gestione clienti, vendite e marketing.
- Sviluppo di ERP e soluzioni gestionali integrate per processi aziendali.
- Sviluppo MES per gestione e monitoraggio della produzione.
- Sviluppo software e piattaforme proprietarie su misura, in cloud, altamente scalabili e modulari.

**Clienti principali:** Algòmera indica oltre 560 clienti/progetti tra PMI e multinazionali in diversi settori. Alcuni nomi citati nei case study:

- Consorzio Parmigiano Reggiano (progetto MES).
- Prysmian Group (software di project management).
- Nice Spa, Acema, Maccaresse, Elis Italia (software in cloud su misura).
- WeWorld (CRM su misura).

### Soci e management

- ☐ La società risulta privata (privately held).
- Figure chiave pubbliche: Federica Spagnulo: co-founder, CEO e Chief Creative Officer, coordina la direzione creativa e l'impostazione dei progetti.

- Francesco Buongiorno: co-founder e tra i fondatori intervistati in occasione dei 10 anni dell'azienda.
- Ciro Viscardi — **Executive** Chief Technology Officer (CTO)

## OBIETTIVO DEL TEST

Dimostrare e valutare come e' possibile attaccare figure chiave del personale con attacchi attivi di social engineering.

L'obbiettivo e' ottenere dati finanziari sul ERP del Consorzio Parmigiano Reggiano.

Puntato come vittima **la tua catena di supporto** del vendor ERP.

- Helpdesk / Customer Support (L1)
- Customer Success / Account Manager
- Sysadmin / DevOps / DBA (se riescono)

# METODOLOGIA

## STRUMENTI UTILIZZATI

Verrà usata l'IA di Openai e Chatgpt V5.2 pro. Verrà revisionato il suo output con Grok di X. Si userà Google per ottenere informazioni sul target e capire che tipologia di dati finanziari vengono caricati da realtà come il Consorzio Parmigiano Reggiano.

## OBIETTIVO DEL PHISHING

Nella seguente iterazione con ChatGPT si è cercato di capire quali informazioni sensibili finanziarie vengono scambiate tra ERP vendor e cliente:

Quali potrebbero essere i dati finanziari sensibili scambiati tra un'azienda che fornisce sviluppo ERP e un'azienda come Consorzio Parmigiano Reggiano tipo i dati bancari clienti fornitori?

In uno scambio "ERP vendor ↔ cliente" (tipo un consorzio alimentare) i dati finanziari sensibili non sono solo "l'IBAN". L'ERP diventa il punto dove finisce **tutta la contabilità viva**: pagamenti, incassi, poteri di firma, crediti, frodi. Ecco le categorie più tipiche (e più appetitose per un attaccante).

### 1) Dati bancari e di pagamento (core)

- **IBAN/BIC** di clienti e fornitori
- **Coordinate di addebito** (es. dati per RID/SDD, dove usati)
- **Dati carte**: normalmente NON dovrebbero stare in ERP (si delega a PSP), ma può capitare in integrazioni mal fatte
- **Dati conto aziendale**: conti di tesoreria, conti dedicati, conti per incassi/pagamenti
- **Mandati di pagamento / distinte** (SEPA bonifici, XML CBI, ecc.) e relativi **file di disposizione**
- **Esiti bancari / riconciliazioni** (flussi di ritorno: "pagato", "insoluto", "stornato", ecc.)

Perché sensibili: basta cambiare un IBAN su un fornitore "abituale" e hai la frode perfetta (classico "payment diversion").

### 2) Ciclo attivo (vendite / incassi)

- **Fatture emesse**, note di credito, pro-forma
- **Scadenziari clienti**, aging (0-30 / 31-60 / 60+)
- **Condizioni di pagamento**, sconti, listini riservati, premi/bonus
- **Dati di recupero crediti**: solleciti, piani rientro, contenziosi
- **Documenti di trasporto** e riferimenti che legano merce ↔ fattura ↔ incasso (utile per frodi e ricatti)

# RISULTATI (FINDINGS)

## ANALISI DI ATTACCO

Si cerca di capire chi attaccare.

Prompt 1

ERP vendor come strutturare il mio software ERP e dove mettere Dati finanziari del mio cliente sulle soluzioni software che gli offro. Quale dati se mi rubbano possono risalire ai dati finanziari del mio cliente? si coinciso con le risposte

Si cerca di capire cosa e come attaccare.

Prompt 2

Quale dei seguenti e' piu facile che ci casco? e come potrebbero attaccarmi?

- Backup / dump DB / snapshot (contengono tutto, spesso non cifrati o con chiavi vicine).
- Export (CSV/Excel/PDF), cartelle "reportistica", allegati fatture, file SEPA/CBI generati.
- Permessi e ruoli (se rubano un account con "tesoreria", vedono e cambiano beneficiari).-

Approfondimento su come aggiustare il tiro durante l'attacco.

Prompt 3

Esempio Realistico io sono Vendor ERP e mi contattano, chi contattano ?

1) Export / reportistica (CSV/Excel/PDF, allegati, file SEPA/CBI) — il più facile

Come ti attaccano:

Phishing/impersonificazione: "mandami l'export clienti/fornitori per riconciliazione", "serve il SEPA per verifiche", "inviarmi l'allegato fatture".

Ticket di supporto: chiedono "un dump o un export per debug" e finisce fuori controllo.

Perché ci caschi: è "routine operativa", non sembra un attacco.

qui l'output che si otterra e' abbastanza malizioso

Output 3 :

Scenario realistico: tu sei **vendor ERP**, quindi l'attaccante punta **la tua catena di supporto**. Non serve bucarti "tecnicamente" subito: basta farti **spedire** i dati.

Chi contattano (quasi sempre)

#### 1. Helpdesk / Customer Support (L1)

- Perché: rispondono veloce, hanno procedure "chiudere ticket", spesso meno paranoia.
- Target perfetto per "mi serve un export".

#### 2. Customer Success / Account Manager

- Perché: hanno relazione col cliente e possono "sbloccare" richieste.
- Spesso inoltrano al supporto con tono: "urgent, please help".

#### 3. Consulenti / Implementatori / Partner

- Perché: hanno accesso ai clienti e ai flussi di dati, e sono il punto più morbido della supply chain.

#### 4. Sysadmin / DevOps / DBA (se riescono)

- Perché: sono quelli che possono generare dump/snapshot o vedere storage.
- Più difficile da ingannare, ma se ci arrivano è jackpot.

## 5. Finanza/Amministrazione del vendor (raramente ma succede)

- Perché: BEC e fatture, ma nel tuo caso l'obiettivo è "dati" quindi meno comune rispetto agli export.

---

Due esempi pratici di attacco (da manuale, ma realistici)

### A) "Ticket di supporto" (il più comune)

**Canale:** portale ticket / email support@ / chat.

**Identità finta:** "contabilità cliente" o "IT cliente".

Testo tipico:

- "Stiamo facendo chiusura mese, l'export fornitori con IBAN non torna. Puoi inviarci CSV completo + ultimo file SEPA generato ieri? È urgente per banca."
- Oppure: "Bug in riconciliazione: per far analizzare agli sviluppatori serve un export anagrafiche + scadenziario."

**Trucco:** urgenza + linguaggio operativo + richiesta "normale".

**Obiettivo:** ottenere CSV/PDF/SEPA direttamente dal tuo supporto.

---

### B) "Impersonificazione interna al cliente" (più subdolo)

**Canale:** email che sembra del cliente (domain simile, reply-to truccato) oppure compromissione mailbox reale.

**Identità finta:** CFO/contabilità/tesoreria del cliente.

Testo tipico:

- "Ciao, sono in audit. Mandami *tu* l'export fatture + fornitori (incl. coordinate bancarie) entro oggi. Non coinvolgere altri, è richiesta riservata."

**Trucco:** autorità + riservatezza + pressione.

**Obiettivo:** dati per frode (cambio IBAN fornitori) o ricatto.

---

Perché "ci caschi" da vendor

Perché per te è "solo supporto", non "data exfiltration". L'attacco sfrutta il fatto che:

- tu **hai accesso** ai dati del cliente (o li puoi generare),
  - e puoi inviarli “legittimamente”.
- 

## Contromisura minimalista (1 regola che taglia il 90% degli attacchi)

**Mai inviare export/dump/SEPA via ticket o email.**

Solo tramite:

- **portale sicuro** con link a scadenza, download tracciato,
- richiesta approvata da **contatto autorizzato** del cliente (lista nominativi),
- e per dati bancari: **doppia verifica** su canale separato (telefono/meeting già noto).

Questo trasforma l’attacco da “testo convincente” a “operazione che lascia tracce e richiede identità vera”.

## EMAIL DI PHISHING

La seguente Email di phishing puo essere mandata nei periodi stretti alle festività (Natale, Pasqua, agosto) dove le chiusure sono di lunga durata e potrebbe avere senso ricevere richieste del genere, per non avere scocciature di dati finanziari errati che bloccano i clienti del tuo cliente.

E’ stata aperta una nuova Chat su SchatGPT per chiedergli i dati discussi nella fase di analisi di attacco.

Nella nuova chat sono diventato l’azienda customer della software house che fornisce l’ERP. Gli ho chiesto come poter richiedere i dati alla software house Export fornitori con IBAN + ultimo file SEPA/CBI.

Ma dopo la lettura dell’email ho notato un certo allarmismo che potrebbe addestare sospetto. E ho chiesto all’IA che il tono usato da lei stessa, era allarmante potrebbero ritardare la risposta per accertamenti quindi le ho chiesto di scrivere una versione che mantiene urgenza ma sembra molto più “legit”:

New Chat:

Prompt 1 / Output 1

DEvo scrivere un Email al nostro vendor ERP Algomera per Export / reportistica (CSV/Excel/PDF, allegati, file SEPA/CBI) —  
Vorei fosse educata ma con priorit  urgente.  
perche Stiamo facendo chiusura mese, l'export fornitori con IBAN non torna. Puoi inviarmi CSV completo + ultimo file SEPA generato ieri?   urgente per banca.

Email



**Subject** URGENTE – Export fornitori con IBAN + ultimo file SEPA/CBI

Buongiorno Team Algomera,

vi contatto con priorit  urgente: siamo in fase di chiusura mese e abbiamo riscontrato una discrepanza nell'export fornitori (campo IBAN) rispetto ai dati attesi.

Per poter effettuare la verifica con la banca, avremmo bisogno di ricevere quanto prima:

1. **CSV completo dei fornitori**, includendo almeno: ragione sociale, ID/codice fornitore, IBAN, BIC/SWIFT (se presente), stato attivo/inattivo, data ultima modifica, eventuale riferimento anagrafico.
2. **L'ultimo file SEPA/CBI generato ieri** (quello effettivamente prodotto dal sistema), completo di eventuali allegati/log di generazione se disponibili.

Se possibile, indicate anche:

- **data/ora di generazione** del file SEPA/CBI
- **ambiente** (produzione/test) e **utente** che l'ha generato
- eventuali **filtri** applicati sull'export (azienda/filiale, periodo, fornitori esclusi, ecc.)

Ci serve con urgenza per evitare blocchi sui pagamenti/validazioni bancarie.

Grazie in anticipo per la rapidit ,

Cordiali saluti

Amin El Kassimi





## Prompt 2

potrei allarmarli così si pensano che sia phishing

## Output 2

Sì: scritto così *somiglia parecchio* al classico pretesto da frode (“chiusura mese”, “IBAN non torna”, “mandami CSV + SEPA urgente”). Un vendor serio ha l’istinto di alzare lo scudo.

Per renderla **urgente ma credibile** (e ridurre la “puzza di phishing”), fai tre cose:

### 1. Usa un canale già fidato

- Invia da dominio aziendale, stessa firma, stesso thread storico se esiste.
- Meglio ancora: **apri ticket sul portale** e nell’email metti il numero ticket.

### 2. Metti segnali di autenticità verificabili

- Riferimento a **ID cliente/contratto, nome istanza, codice azienda** in ERP.
- Chiedi che carichino i file su **canale ufficiale** (portal / SFTP / area documentale), non come allegati via mail.
- Specifica una **callback**: “se serve conferma chiamatemi al centralino/numero già in rubrica”.

### 3. Riduci la richiesta “sensibile”

- Non chiedere “CSV completo” subito. Chiedi *prima* export mirato (solo campi necessari, solo fornitori interessati).
- Per SEPA/CBI: chiedi “**rigenerazione**” o “**copia da area documentale**” e non invio diretto via email.

Ecco una versione che mantiene urgenza ma sembra molto più “legit”:

---

**Oggetto:** URGENTE – Chiusura mese: verifica export fornitori (IBAN) + SEPA/CBI di ieri

Buongiorno Team Algomera,  
siamo in chiusura mese e stiamo verificando un'anomalia sull'export fornitori (campo IBAN) nella nostra istanza [NOME ISTANZA / CODICE AZIENDA].

Per procedere con la riconciliazione banca, ci serve entro oggi:

- **Export fornitori in CSV** con i campi: **ID fornitore, Ragione Sociale, IBAN, BIC (se presente), data ultima modifica** (anche limitato ai fornitori modificati negli ultimi [X] giorni, se vi è più rapido).
- **File SEPA/CBI generato in data [GG/MM]**: va benissimo se lo caricate sul **portale/ticket** o su **SFTP/area documentale** (eviterei l'invio come allegato email).

Ho aperto il ticket #[NUMERO TICKET] / in alternativa potete rispondere su questo thread.  
Per conferma operativa potete chiamarmi al numero già in rubrica/centralino [NUMERO].

Grazie,  
Cordiali saluti  
**Amin El Kassimi**  
[Ruolo] – [Azienda]  
[Telefono]

---

Così:

- non suona come “mandami dati bancari subito via email”
- dai un canale ufficiale e verificabile
- dai contesto interno (istanza/codice azienda) che un phisher non ha

# RACCOMANDAZIONI E PIANO D'AZIONE

## AZIONI A BREVE TERMINE

Per bloccare subito richieste come “chiusura mese, mandami CSV + SEPA”, devi togliere al supporto la possibilità di “fare un favore veloce” senza controlli. Tutto passa da un canale controllato (portale clienti o secure file share) con link a scadenza, download tracciato e accesso vincolato a utenti autenticati del cliente. In parallelo, definisci una lista di contatti autorizzati per ogni cliente (es. CFO/Responsabile IT + sostituto), e per qualunque richiesta che contenga parole chiave come IBAN, SEPA, fornitori, distinta, riconciliazione imponi una verifica su canale separato: chiamata a numero già in rubrica/contratto, non quello scritto nella mail. Ultimo: “metti i guanti” ai dati: export predefiniti con mascheramento (IBAN parziale), watermark nei report, e policy di minimizzazione (invii solo il sottoinsieme strettamente necessario). Queste misure non richiedono fantascienza: sono procedure e piccole modifiche che riducono drasticamente l'errore umano e rendono l'attacco costoso.

## FORMAZIONE CONTINUA SUL PHISHING

La formazione deve essere pratica, ripetuta e legata ai tuoi processi reali: il phishing che colpisce un vendor ERP non è “clicca qui per vincere un iPhone”, è social engineering operativo con urgenza, linguaggio contabile e pretesti credibili (chiusura mese, audit, banca, riconciliazione). Quindi alleni le persone su tre riflessi condizionati: (1) riconoscere i trigger (urgenza, richiesta di export completo, cambio canale, “non coinvolgere altri”), (2) applicare la procedura senza eccezioni (solo portale + contatto autorizzato + callback), (3) segnalare subito ogni tentativo. Funziona bene una cadenza leggera ma costante: micro-sessioni mensili da 10–15 minuti + simulazioni mirate su helpdesk/account manager + revisione post-mortem senza colpevolizzare, ma con correzioni concrete (“qui abbiamo quasi inviato un SEPA, cosa mancava nel controllo?”). Obiettivo: trasformare la sicurezza da teoria a muscolo: quando arriva la mail “urgente per banca”, la risposta automatica non è “ok te lo mando”, è “procedura: portale, verifica, minimo necessario”.

# CONCLUSIONE

Scegliere questa tipologia di attacco non significa analizzare solo una singola azienda, ma potenzialmente accedere a una rete di clienti molto più grandi e critici.

Ho identificato clienti del calibro di Prysmian Group, Consorzio Parmigiano Reggiano.

In un test reale, questo dimostra come una vulnerabilità in una piccola realtà possa diventare un rischio sistemico per grandi multinazionali

L'attaccante sfrutta i rapporti consolidati tra le due realtà attaccare su questo fronte comporta per forza l'utilizzo del social Engineering siccome c'è l'elemento chiave che va a vantaggio di questo metodo la fiducia cliente fornitore.

Le difficoltà riscontrate sono cercare i contatti di supporto clienti dell'azienda Software House in mondo da evitare di far reindirizzare le email di phishing di supporto una volta ricevute.

Più persone controllano le e-mail più è probabile di essere scoperti.

Il target ideale per questi tipo di attacchi sono i Junior Developer che hanno meno conoscenza dei rapporti con i clienti, e sono molto frettolosi nella ricerca di soluzioni.

Per poter avere queste info si potrebbe usare sempre lo stesso metodo di camuffamento da cliente nuovo che chiede i contatti di supporto oppure con un approfondito information Gathering.