

PROGETTO S5L5:

Esercizio del Giorno: Simulazione di un'Email di Phishing

Esempio 1:

1. Scenario Dettagliato

Contesto realistico:

Un dipendente di un'azienda medio-grande (es. "Iveco Group") riceve un'e-mail apparentemente inviata da Microsoft Security. L'email segnala un tentativo di accesso non autorizzato al suo account Microsoft 365 da una posizione insolita (Cina), e lo invita ad accedere urgentemente a un portale per "verificare la propria identità".

Obiettivo del phishing:

Indurre il dipendente a inserire le proprie **credenziali di accesso aziendali** (e-mail e password) su un sito **fasullo** che replica la pagina di login di Microsoft 365.

Contesto aziendale:

Iveco Group N.V. è una multinazionale attiva nel settore dei veicoli industriali, autobus, motori e trasporto commerciale. L'azienda ha sede legale nei Paesi Bassi e una forte presenza operativa in Italia e nel resto d'Europa. Dispone di numerose business unit, tra cui Iveco, FPT Industrial, Heuliez Bus e Magirus.

Con oltre 35.000 dipendenti e sedi in più di 20 paesi, Iveco Group fa uso quotidiano di **infrastrutture IT complesse e distribuite**, molte delle quali basate su tecnologie Microsoft, come:

- **Microsoft 365** per posta elettronica, Teams, SharePoint e OneDrive;
- **Azure AD** per la gestione delle identità e degli accessi;
- **Endpoint Management** per la sicurezza degli asset.

2. E-mail di Phishing

Mittente: Microsoft Security Team <no-reply@microsoft-support.com>


Oggetto: 🛡️ [Azione richiesta] Accesso non autorizzato rilevato nel tuo account Microsoft 365


Data: 01 Agosto 2025 – 08:32


Destinatario: mario.rossi@ivecogroup.com

Gentile Mario Rossi,

Il nostro sistema di sicurezza ha rilevato un **tentativo sospetto di accesso** al tuo account Microsoft 365 da un dispositivo non riconosciuto:

 **Località:** Shenzhen, Cina

 **IP:** 202.140.11.55

 **Data/Ora:** 01/08/2025 06:47 UTC

Per **proteggere la tua identità e i dati aziendali**, il tuo account è stato **temporaneamente bloccato**.

Ti invitiamo a **verificare immediatamente la tua identità** per evitare la disattivazione permanente dell'account.

 **Verifica Attività e Ripristina Accesso**

⚠ **Importante:** Se non completi la verifica entro le **prossime 24 ore**, il tuo account verrà **disabilitato automaticamente** per motivi di sicurezza in conformità con il Regolamento Microsoft 365 per aziende.

Se ritieni che questo messaggio ti sia stato inviato per errore, ti invitiamo a ignorarlo.

Grazie per la collaborazione,

Microsoft Security Team

Divisione Account Business & Protezione Identità

<https://security.microsoft.com>

3. Analisi dello Scenario

Perché l'e-mail è credibile

- Utilizza **nomi e strumenti reali** (Microsoft 365, IP, data/ora, dominio aziendale).
- Appare urgente e **rilevante per il lavoro** dell'utente.
- È **ben strutturata**, con icone, grassetti, e un tono professionale.
- Include un **link cliccabile** simile a un vero URL Microsoft.
- Firma apparentemente "ufficiale" con un dominio reale a piè di pagina.

Segnali di allarme (red flags)

Elemento	Descrizione
Mittente	L'indirizzo e-mail contiene "micr0soft" con uno zero (0) al posto della "o". Non è un dominio ufficiale.
Link sospetto	Il link mostra un testo rassicurante ("Verifica attività") ma punta a un dominio truffaldino : micr0soft365-verifica.com
Minaccia e urgenza	Fraasi come "verifica entro 24 ore" o "disabilitazione automatica" sono tecniche comuni nei phishing per creare ansia.
Lingua troppo generica	Sebbene sembri personalizzata (nome e azienda), alcuni termini sono vaghi o copiati da template generici .
Mancanza di contatti ufficiali	Nessun numero verde, firma condivisione reale Microsoft, né collegamenti all'helpdesk ufficiale.

Esempio 2:

1. Scenario Dettagliato

Contesto realistico:

Un dipendente dell'ufficio contabilità di un'azienda riceve un'e-mail apparentemente da parte di un noto fornitore di servizi digitali (es. Aruba, Register.it, ecc.), in cui si segnala una **fattura non pagata**. La mail contiene un link per scaricare la "fattura", che in realtà è un **file dannoso** (es. un file ZIP con malware o un link a un sito fake di login).

Obiettivo del phishing:

Indurre l'utente a scaricare un file contenente malware (es. trojan bancario) oppure fargli inserire le credenziali aziendali su una **pagina clone del pannello clienti**.

Contesto Aziendale:

Iveco Group N.V. è una multinazionale operante nel settore dei veicoli industriali, trasporto commerciale e servizi correlati. La società ha una struttura complessa, con sedi distribuite in più paesi, e numerosi reparti aziendali – tra cui finanza, acquisti, IT, produzione e logistica – che interagiscono quotidianamente con una rete globale di fornitori e partner tecnologici.

Il **reparto amministrativo/finanziario** (Finance Department), così come quello **procurement** (Acquisti), riceve regolarmente:

- notifiche di fatturazione da parte di fornitori internazionali;
- scadenze di pagamento automatizzate;
- promemoria su contratti digitali, manutenzioni software o servizi cloud (es. SAP, Aruba PEC, hosting per portali B2B, ecc.).

Il personale lavora con **decine di e-mail ogni giorno**, inclusi allegati, portali esterni e sistemi ERP. Le procedure, sebbene formalizzate, sono soggette alla velocità operativa: questo apre uno **spazio d'attacco** per campagne phishing ben coneggiate.

2. E-mail di Phishing – Simulazione Aruba

Mittente: Aruba Fatturazione <pagamenti@aruba-fatture.com>


Oggetto: [URGENZA] Fattura n. 029182 - Pagamento In Sospeso per ivecogroup.com

Data: 01/08/2025 – 09:36


A: ap.finance@ivecogroup.com

Gentile Cliente,

Con la presente La informiamo che la **fattura n. 029182**, relativa al **rinnovo annuale del dominio ivecogroup.com** e dei servizi PEC associati, **non risulta saldata** alla data odierna.

 **Importo dovuto:** € 498,80 IVA inclusa

 **Scadenza originale:** 24/07/2025

 **Penale per ritardo attiva dal:** 03/08/2025

Le chiediamo di effettuare il pagamento al più presto per **evitare la sospensione automatica dei servizi**.

 **Scarica la Fattura PDF**

Nel caso in cui il pagamento sia già stato effettuato, La invitiamo a **verificare e confermare** tramite la Sua **Area Clienti Aruba**:

 **Accedi all'Area Clienti**

Cordiali saluti,

Ufficio Fatturazione Aruba

Aruba PEC S.p.A. – P.IVA 01573850516

www.aruba.it

3. Analisi dello Scenario

Perché l'e-mail è credibile

Aspetto credibile	Descrizione
Nome dominio reale	L'email fa riferimento a <code>ivecogroup.com</code> , dominio corretto.
Contesto plausibile	Il Finance di Iveco gestisce regolarmente forniture, servizi IT, domini, PEC, ecc.
Tono formale e professionale	I contenuti e il linguaggio sono simili a una comunicazione reale di Aruba.
Importo credibile	La cifra è compatibile con un servizio aziendale annuale (es. PEC, hosting dominio).

Segnali di allarme (red flags)

Red Flag	Spiegazione
Dominio e-mail falso	<code>@aruba-fatture.com</code> non è un dominio ufficiale (@aruba.it)
URL sospetto	Link punta a <code>fatture-aruba.cloud</code> , non al sito ufficiale Aruba
Formato file ZIP	Aruba invia documenti in PDF, non file compressi o eseguibili

Urgenza e minacce	L'inserimento di penali e date limite serve a creare panico
Login fasullo	La pagina clone arubaclienti-support.com è una trappola per credenziali

Conclusione dell'Esercizio – Simulazione Phishing Iveco Group

Questa simulazione ha dimostrato quanto un'e-mail di phishing ben progettata, se adattata a un contesto aziendale specifico come quello di **Iveco Group**, possa risultare **altamente convincente anche per personale esperto**. Utilizzando un pretesto realistico (accesso anomalo a Microsoft 365 o una fattura Aruba non saldata), l'attaccante riesce a fare leva su:

- **Routine lavorative quotidiane** (es. ricezione di fatture, notifiche di sicurezza);
- **Servizi realmente utilizzati** (Microsoft 365, PEC, portali clienti);
- **Pressione emotiva** tramite urgenza e minacce di blocco/sospensione;
- **Grafica e linguaggio formale** coerenti con i canali ufficiali.