INGEGNERIA SOCIALE - 02/05/2025

Target: Luxottica Group S.p.A.
Autore: Francesco Fontana
Data: 02/05/2025
Strumenti utilizzati: IA - Google - Mail certificata interna - Teams
Obbiettivo: L'obiettivo è fornire a Luxottica Group S.p.A. un quadro completo dalla progettazione dell'attacco alla misurazione dei risultati, per ottimizzare le future campagne di sicurezza e consapevolezza

1. SCENARIO DI CONTESTO: DEFINIZIONE E STRUTTURAZIONE

1.1 Obiettivo Strategico

- **Prime metriche di successo**
    - **Open rate > 90%**: il 90% dei destinatari deve aprire l'email.
    - **Click-through rate (CTR) 20–30%**: percentuale di utenti che cliccano sul link.
    - **Credential submission rate ≤ 5%**: percentuale di utenti che inseriscono effettivamente username e password.

- **Benefici attesi**
    - Mappatura dei "punti caldi" di vulnerabilità interna (dipartimenti più esposti).
    - Evidenziazione di eventuali "super-clickers" ossia utenti che cliccano ripetutamente senza verificarne la legittimità.
    - Raccolta di best practice di timing e linguaggio più efficaci per gli scenari reali.

1.2 Profilo del Target

- **Ruoli aziendali coinvolti**: HR, Amministrazione, Supply Chain, Business Intelligence, Vendite
- **Livello di competenza IT stimato**: medio–alto (ma con varianza generazionale)
- **Canali di comunicazione abituali**: Intranet, instant messaging (Teams), email certificata interna

1.3 Tempistica e Frequenza

- Invio in giornate d'ufficio (lunedì–giovedì) per massima visibilità
- Orario strategico: tra le 9:00 e le 10:30 (picco di consultazione della posta)
- Richiamare l'email con un reminder 4 ore prima della scadenza: testare reazioni a "seconda chance"

1.4 Email di Phishing Utilizzata

Da: IT Helpdesk Luxottica <helpdesk@luxottica-securemail.com>
Oggetto: URGENTE: Azione Richiesta – Scadenza Password Intranet OGGI

Gentile Collega,

Per garantire la massima sicurezza dei dati aziendali, **è obbligatorio** procedere al rinnovo della tua password Intranet entro **oggi alle 18:00**.
Il nostro sistema di monitoraggio ha rilevato un'attività insolita sul tuo account, pertanto è necessario confermare la tua identità e aggiornare la password per evitare il blocco dell'accesso.

▶ Clicca QUI per accedere alla procedura di verifica e aggiornamento
https://luxottica-helpdesk.secure-update.com/login

Ti ricordiamo che, in caso di mancata risposta entro i termini, il tuo account verrà temporaneamente disabilitato.

Per assistenza, rispondi a questa email o contatta il numero interno **1234**.

Grazie per la collaborazione.
IT Helpdesk Luxottica
"Proteggiamo insieme i dati dell'azienda"

2. EMAIL DI PHISHING: ANATOMIA E LINGUAGGIO PERSUASIVO

2.1 Struttura del Messaggio

Sezione	Obiettivo persuasivo
Header	Richiama l'"IT Helpdesk Luxottica" per autorevolezza
Oggetto	"URGENTE: Scadenza Password OGGI" → attiva risposte emotive legate all'urgenza
Apertura	"Gentile Collega," → tono familiare ma formale
Body principale	Descrive attività insolita monitorata inserendo un obbligo d'azione
Call-to-Action	Link e bottone grafico fittizio ben visibile
Footer	Contatti di supporto + slogan aziendale per credibilità

2.2 Tecniche di Social Engineering

1. **Autorità**: richiamare un dipartimento IT riconosciuto.
2. **Urgenza**: deadline stretta ("entro oggi alle 18:00") per ridurre la razionalità critica.
3. **Scarsità**: minaccia di disabilitazione account se non si agisce subito.
4. **Familiarità**: utilizzo di formule di cortesia interne e contatti aziendali reali.
5. **Invisibilità del dominio reale**: dominio differente ma contenente parole chiave aziendali per confondere.

2.3 Elementi "Red Flag"

- **Dominio del mittente**: helpdesk@**luxottica-securemail.com**
- **URL di destinazione**: **https://luxottica-helpdesk.secure-update.com/login**
- **Errori lievi di formattazione**: grassetti non uniformi, punteggiatura a volte forzata
- **Glossario IT impreciso**: "procedura di verifica e aggiornamento" senza dettaglio sui protocolli MFA (Multi-Factor-Authentication)

- **3. SPIEGAZIONE PSICOLOGICA E COMPORTAMENTALE**

3.1 Bias Cognitivi Sfruttati

Bias	Descrizione	Impatto nel Phishing
Urgenza	Reazione impulsiva a scadenze ravvicinate	Riduce tempo per validare autenticità
Autorità	Maggiore tendenza a obbedire a figure percepite come “superiori”	Gli utenti tendono a fidarsi dell’IT Helpdesk
In-group	Fiducia verso messaggi percepiti come interni all’organizzazione	Elementi di branding e contatti familiari

3.2 Analisi del Flusso Mentale dell’Utente

1. **Ricezione e apertura**: vede mittente noto → apertura quasi automatica.
2. **Lettura rapida**: “attività insolita” + “oggi” → genera ansia breve.
3. **Click sul link**: percepita come “azione semplice e veloce” per ripristino accesso.
4. **Inserimento credenziali**: convincimento che si tratti di portale ufficiale.
5. **Fine**: credenziali trasmesse al server di phishing; l’utente non avverte direttamente danno.

4. DETTAGLI TECNICO OPERATIVI

4.1 Infrastruttura di Phishing

- **Hosting Web**: server VPS in offshore, con certificato SSL auto-firmato.
- **Replica interfaccia Intranet**: uso di HTML/CSS copiati per somiglianza (logo, moduli, footer).
- **Logging e notifiche**: script lato server per invio in tempo reale delle credenziali rubate via webhook interno (Slack/Teams).
- **Persistence**: link unico per ogni invio, per tracciare chi clicca e chi inserisce dati.

4.2 Contromisure Tecniche

- **SPF/DKIM/DMARC**: assicurarsi che i messaggi non provenienti dai server autorizzati vengano rifiutati o finiscano in quarantena.
- **URL rewriting**: soluzioni di Secure Web Gateway per evidenziare link esterni rispetto a luxottica.com.
- **MFA obbligatoria**: rendere necessario un secondo fattore, così anche inserendo user/pass non si ottiene accesso completo.

5. PIANO DI MISURAZIONE E REPORTING

5.1 Metriche da Raccogliere

KPI	Metodo di raccolta	Obiettivo
Open rate	Report server SMTP / MailTracker	> 90%
Click-through rate (CTR)	Link tracciato con parametri UTM univoci	20–30%
Form submission rate	Logging lato server phishing page	≤ 5%
Tempo medio di clic	Δ tra ricezione email e click	Analisi di velocità

5.2 Reportistica e Analisi

- **Dashboard dinamico** (Power BI o Grafana) con aggiornamento giornaliero
- **Breakdown per dipartimento**: mappare aree più vulnerabili
- **Analisi temporale**: orari con picco di clic e aperture

5.3 Debriefing Post-Campagna

- **Sessioni di feedback** in piccoli gruppi (max 10 persone)
- **Quiz interattivo**: presentare esempi reali e chiedere di individuare i “red flag”
- **Materiale formativo**: infografiche e video brevi (1–2 minuti) da distribuire via Intranet

6. RACCOMANDAZIONI FINALI E ROAD-MAP

1. **Phishing simulations trimestrali**: alternare scenari (banking, fornitore esterno, comunicazioni interne).
2. **Implementazione di un Phish Report Button**: plugin di Outlook/Teams per segnalare email sospette con un click.
3. **Aggiornamento policy password**: password manager aziendale + rotazione semplificata, meno inviti temporanei.
4. **Formazione mirata**: focus sui bias cognitivi e su come verificare in modo rapido mittente e link.
5. **Verifica periodica di SPF/DKIM/DMARC**: audit semestrali per confermare corrette configurazioni.

7. CONCLUSIONI

Con questa analisi strutturata, Luxottica Group S.p.A. disporrà di uno strumento di assessment completo.

Dalle tecniche persuasive allo stack tecnologico, fino alle metriche di misurazione, per rafforzare la propria difesa contro le minacce di phishing.

La roadmap proposta aiuterà a costruire un programma di security awareness robusto e sostenibile nel tempo.