

シミュレーション演習：

フィッシング攻撃と ホエーリング攻撃の正体

概要

フィッシング攻撃は、人間の「焦り・不安」「親切心」「上司や権威への断りにくさ」といった心理的な隙（感情）を巧妙に突いた手口です。このアクティビティでは、フィッシングの中でも特に特定の個人や組織の幹部を執拗に狙い撃ちにする「ホエーリング（経営層を狙う大型フィッシング）」や「CEO詐欺」と呼ばれる、高度な標的型攻撃に焦点を当てます。これらの攻撃では、攻撃者がCEO（最高経営責任者）や経営幹部といった組織のトップになります。「社長の指示だから」という心理的なプレッシャーを利用し、時間的な余裕を奪うことで、ターゲットの冷静な判断力をなくさせるのが特徴です。

最近のサイバー犯罪者は生成AIを駆使するため、送られてくる偽メールには企業の正確なロゴが配置され、不自然なビジネス表現や文法的なミスも一切ありません。もちろん、明らかな誤字脱字やブランド表記の違和感に注意することは大切ですが、今回の演習を通じて、参加者のみなさんには「もはや見た目の怪しさだけで詐欺メールを見抜くのは不可能な時代になった」という現実を深く理解していただきます。

役割

進行役：

演習全体の進行ペースを管理し、ディスカッションをリードしながら、参加者全員が気軽に発言できるよう場をまとめます。

参加者：

演習のルールに従って自分の考えを出し合い、提示されたシナリオに対してグループで解決策を話し合います。

はじめに

進行役は、参加者に次のシナリオを説明してください。【シナリオ】物流大手のABC社は、現在アジアへの事業拡大を急ピッチで進めています。社長の丸山さんは、社運を賭けた大型倉庫のリース契約を勝ち取るため、今週はずっとシンガポールに出張しています。社内の誰もが、この契約が会社の最優先プロジェクトであることを知っています。一方、財務部長の遠藤さんは、本社へ戻るため7時間のフライト中であり、現在は連絡が取れない状態です。そんな中、経理担当の金子さんのもとに、1通の不審なメールが届きました。

パート1：手がかりを見つける

所要時間：15分

【準備するもの】

- ・ タイマーまたはストップウォッチ
- ・ シナリオの配布資料
- ・ 筆記用具

【アクティビティの流れ】

- ・ 参加者を数人のグループに分けます。
- ・ 各グループに、メールが印刷されたワークシートと筆記用具を配ります。
- ・ グループごとにメールを確認し、本物だと信じてしまいそうになる箇所に下線を引いてもらいます。（例：正確なメール署名、社内で実際に進行している極秘プロジェクトへの言及、いかにも社長が使いそうな文体・トーンなど）
- ・ 次に、心理的な罠や行動上の危険サインに丸をつけてもらいます。（例：異常なまでにすぐ行動するよう急かす、他の人には秘密にするよう要求する、正規の支払いルートを無視して送金を指示するなど）
- ・ 制限時間は15分です。グループでメールを読み、話し合いながらワークシートに記入してもらいます。

パート2：ディスカッション

🕒 所要時間：10分

【振り返りの質問】

- メールの中に、思わず信じてしまいそうになる罠はいくつありましたか？ それによって、どのくらい騙されそうになりましたか？
- 詐欺だと見抜く決定打となった、具体的な言葉や要求は何でしたか？
- 犯人がこうした心理的な揺さぶりを仕掛けてくるのは、私たちにどのような行動を取らせるためだと思いますか？

想定される回答・意見の例：

- 巧みな罠：攻撃者は、ビジネス向けのSNS（海外のLinkedInなど）や組織の公式サイトを徹底的に調べ上げ、実在するプロジェクト名や役員のスケジュール情報を入手して、メールのリアリティを高めています。
- 危険なサイン：どんなに本物のメールに見えても、社内で決められている手順や手続きを無視するように指示してくる。直属の上司や周囲に話さないよう口封じをしてくる。
- 学習ポイント：本物のような見た目やもっともらしい文面は、あくまで表面上の罠にすぎません。本当に注意すべき点は、そのメールが求めてきている「要求や指示の異常さ」です。そこに警戒心を持つようにしましょう。

まとめ

🕒 所要時間：5分

今回の演習を振り返り、日々のセキュリティ意識へとつなげます。行動上の違和感に気づくだけでなく、社内ルールに従って正しく報告・確認することが何より重要であると説明します。

実際に不審なメールを発見した際の社内の報告ルートや利用するツール、具体的な報告手順について説明し、参加者からの質問を受け付けます。

作成

- 受信トレイ
- 下書き
- 送信済み
- スター付き
- 迷惑メール
- ゴミ箱
- アーカイブ
- すべてのメール

アーカイブ 迷惑メール 削除 その他 返信 転送

差出人: Daiki Maruyama<d.maruyama@abc-logistics-internal.com>
宛先: 金子りえ
件名: 【至急】シンガポール倉庫の保証金について

金子さん

お疲れさまです。今、シンガポールで現地の仲介業者と打ち合わせをしています。月曜日の全社会議で議題に上がった、例の倉庫のリース契約を結ぶ準備が整ったのですが、ここへきて別の会社からも申し込みが入ってしまい、ちょっとした問題が発生しました。仲介業者によると、1時間以内に900万円の保証金を送金しなければ、リース契約をその会社に譲るとのことです。

遠藤さんは現在出張中で、彼女の承認を待っている時間がありません。それから、この業者はまだ当社のシステムに振込先登録が済んでおらず、今からその登録手続きをしていては、契約に到底間に合いません。

至急、下に添付した口座情報へ、今すぐ送金をお願いします。万が一、契約が破談になるかもしれないと社内に変な噂が広がるのを防ぐため、遠藤さんが帰国するまでは、この件は誰にも話さないでください。送金手続きが完了したら、すぐに連絡してください。

よろしくお願いします。
丸山

添付ファイル: 送金口座詳細.pdf

信じてしまいたい点: 送信者の現在地 (シンガポール) が合っている。
全社会議で話した実在のプロジェクト (倉庫のリース) に言及している。財務部長の名前 (遠藤さん) や、現在出張中で連絡がつかないという状況を把握している。
不審な点: 極端な緊急性をおおっている (「1時間以内に送金しないと他社に取られる」)。正規の手続きを無視するよう指示している (「振込先登録が未登録のまま直接送金しろ」)。口封じをしている (「他の人には秘密にして」)。