啓発教材の提示順が
セキュリティ意識に与えた影響の定着度評価

敷田 幹文 教授　Communication and Collaboration Lab
高知工科大学 KOCHI UNIVERSITY OF TECHNOLOGY

背景・目的

- 近年，情報保護に関する事件や事故は増加傾向
  - 特に**フィッシング**が増加
- 原因は**人的ミス**が過半数
  →システムの向上だけでは防ぐのは難しい
- **疑似フィッシングメール**を啓発教材に
  - 掲示するフィッシングメールの判別難度の順序がユーザに与える影響を分析
    - 易→難，難→易，難度一定の3方式
- 場面ごとに最適なセキュリティ啓発手法を検討

フィッシング対策協議会に寄せられたフィッシングの報告件数の推移
https://www.lac.co.jp/lacwatch/report/20221219_003234.html

フィッシングとは？
- 公的な企業や組織を装ったメールやメッセージで悪質のサイトへ誘導を行い，個人情報を搾取する行為

例）電子メールを送り付けて偽リンクを踏ませて個人情報を盗み出す

ユーザ個人のセキュリティリテラシーを高める！

実験

演習後の**セキュリティ知識の定着度**への影響を調査する
5種類の判別難度の異なるフィッシングメール画像を提示し，メールの印象に対するアンケートを実施

【掲示順】
- A方式：判別難度を徐々に上げる(Lv1→Lv5)
- B方式：判別難度を徐々に下げる(Lv5→Lv1)
- C方式：判別難度が一定(Lv4)
  - Lv.4:一般的なフィッシングメールの注意喚起資料レベル

【実験参加者】
- A方式：136名
- B方式：110名
- C方式：120名

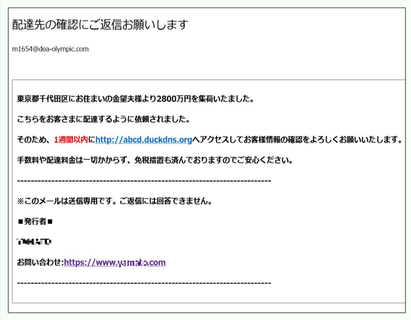
- Q1. 啓発受講経験の有無(事前/追跡)
- 無効感を推測する質問(事前/事後/追跡)
  - Q2. 作成・送信に知識が必要だと思うか
  - Q3. 対応のルールが必要だと思うか
  - Q4. 実際に詐欺メールに遭遇した際に本調査を思い出すか
- 対策への意欲確認
  - Q5. 今月中にフィッシングを疑った頻度(追跡)
  - Q6. 今月中に詐欺メールを目にした回数(事前/追跡)

【実験スケジュール】
- 1回目調査
  - **事前**アンケート
  - 演習
  - **事後**アンケート
- 2回目調査(1回目から2週間後)
  - **追跡**アンケート
  - リテラシー確認問題

【リテラシー確認問題】
- メールを目にしたときに注目する箇所の順位付けを行う
- 注目順位3位以内で選択したときの合計点数を各レベルで比較
  - **メールアドレス(A)：2点**
  - ロゴ(B)：0点
  - 赤字で強調(C)：0点
  - **マスクされたリンク(D)：1点**
  - 発行者(E)：0点
  - **リンクの中身(F)：3点**

参加者を以下に分類
- Low：0-1点
- Mid：2-3点
- High：4-6点

メール内容



Lv1(易)
- メールアドレスが**ランダムな文字列**
  m1654@dea-olympic.com
- URLベタ書き
  https://abcd.duckdns.org
- 誤字脱字あり
  「いたました」

Lv2
- 誤字脱字を**あり**から**なし**に変更

「いたました」
→「いたしました」

Lv3
- URLを**ベタ書きから隠す形式**に変更
  https://abcd.duckdns.org
  →こちら

Lv4
- **ロゴ**を付けた
- メールアドレスを企業名の誤字verに変更

Lv5(難)
- メールアドレスを実際の企業名に変更

（ロゴは5種類実験に使用）
（各社に許可取り済み）

アンケート評価

A方式（易→難）
【全てのアンケート】
- 有意差が見られる項目なし

→演習が印象に残っていない

有意差とは？
- ある数値間の差が「たまたま起こった差ではなく，意味のある差」であることを指す

B方式（難→易）
【事前ー追跡アンケート】
- Q2が有意に高まる傾向

→フィッシングに対し脅威を感じる傾向
- Q3が有意に高まっている

→ルールの必要性を感じ、対策への意欲が高まっている

C方式（難度一定）
【事前ー追跡アンケート】
- Q2が有意に高まっている

→フィッシングに対し脅威を感じている
- Q4が有意に高まる傾向

→事前アンケートと演習が印象に残る傾向

定着度評価

- メールの構成要素において**ロゴ**は注目を集めやすい


←今回のロゴ

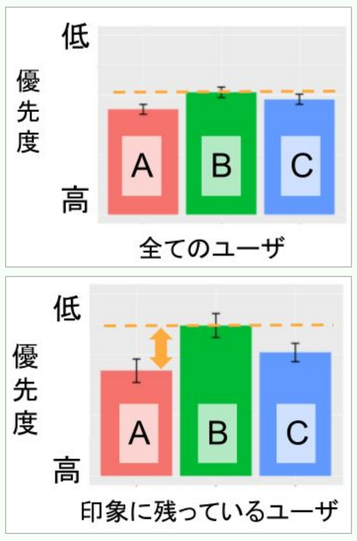
→昨今のフィッシングメールにおいて常習的に用いられる
- 1回目演習解説でロゴは**「メールの正当性を判断する要素として不適切」**と示す

→啓発内容が定着しているユーザとそうでないユーザで最も差が顕著に表れる要素

【ロゴ(B)への優先順位付けの傾向】
右上の図：全てのユーザを演習方式で分類
- **徐々に難度を下げる方式**(B方式)のユーザ群が比較的**ロゴへの優先度を低く**設定
- A-B方式間で有意傾向がみられる

右下の図：アンケートで演習実施が印象に残っているユーザを演習方式で分類
- 全てのユーザの図と比較して**方式間の差がより顕著**になっている
- A-B方式間に有意差，B-C方式間に有意傾向がみられる

ステップダウン形式で演習を行うB方式は啓発内容を定着させる！



まとめ

各方式の特性を場面に合わせて使い分ける！

- 各演習方式の特性が分かった
  - 徐々に難度を上げる方式(A方式)
    - 演習直後の**無効感**を高める
  - 徐々に難度を下げる方式(B方式)
    - **定着度**が高い
  - 一定の難度を保つ方式(C方式)
    - **リテラシーレベルのの高い層に**印象に残っている

無効感とは？
- 攻撃者に対する偏見から自分自身がセキュリティ対策行動を取っても何の意味もないと感じること

- 応用例
  - 徐々に難度を上げる方式(A方式)
    例）**講演型啓発の冒頭**にデモで用いることが有効
  - 徐々に難度を下げる方式(B方式)
    例）**オンライン型啓発**に有効
  - 一定の難度を保つ方式(C方式)
    例）リテラシーレベルが高いと予想できる**会社内の部署ごとの啓発**に有効