セキュリティ対策行動を促す啓発手法の提案と評価

1255116　藤原 晴　【 コミュニケーション & コラボレーション研究室 】

Promotion of Security Awareness: Proposal and Evaluation of Enlightenment in an Opportunity for Voluntary Security Action

1255116　Haru Fujiwara　【 Communication and Collaboration Lab. 】

1　はじめに

近年, セキュリティインシデントが増加傾向にあり, 組織や企業を装ったメールによって, 悪性サイトへ誘導を行い個人情報を騙しとるフィッシングが増加している. フィッシングをはじめとしたインシデントの発生原因はシステム上の問題よりも人間の不注意や社内ルールの不遵守に起因する人的ミスが過半数を占めており, システム的な保護のみならずシステムを操作するユーザに対して啓発を行っていくことが重要視されている [1].

そこで本研究では, 組織・企業のように幅広い層のユーザが混在する環境においてもインシデント発生防止に寄与する啓発手法を提案・評価することを目的としている. ヒューマンファクタ (以下: HF) に着目したセキュリティ演習方式を設計し比較することで, 対策意欲の向上に有効な要素とユーザ特性との関連を調査すると共に演習実施から一定期間をおいての追跡調査により定着度を評価する.

2　演習方式の設計

2.1　参考とするヒューマンファクタ

本研究では, フィッシングメールを題材とした演習を実施した. 演習方式設計に際して, 対策意欲に有意な影響を与えるとされる HF である「攻撃者のスキルに対して自身の対策は無意味と感じると負の影響 (以下: 無効感)」と「社会的に情報セキュリティが必要と感じると正の影響 (以下: 関心)」を参考としている [2]. 無効感と関心はリテラシレベルをはじめとしたユーザ特性の影響をうけることを考慮し, 段階的にフィッシング判別難度 (以下: Lv) を変動させることで幅広いユーザ層に対して, HF を有意に作用させることを狙った演習方式を 2 つ設計した. 演習方式は Lv1-5 と徐々に判別難度を高めることで関心を作用させることを狙った A 方式, Lv5-1 と徐々に判別難度を下げることで, 無効感の低減を狙った B 方式とする.

2.2　提示メールの設計

各演習では, フィッシング判別難度の異なるメールを 5 種類ずつ提示した. 判別難度はメールの正当性を人が判断する上で, 着目する要素をアイトラッキングと聞き取り調査により分析した研究を参考として, 表 1 のように分類している [3].

表 1　提示メールの構成要素

Lv	メールアドレス	ロゴ	リンク	誤字
1	ランダム文字列	なし	マスクなし	あり
2	ランダム文字列	なし	マスクなし	なし
3	ランダム文字列	なし	マスクあり	なし
4	ランダム文字列	あり	マスクあり	なし
5	本物と類似	あり	マスクあり	なし

3　演習実施後の対策意欲分析

3.1　実験

Web 上で演習とアンケートを実施し, A 方式 99 名, B 方式 97 名を対象として分析を行った. 被験者には無効感と関心の度合いを推測するための質問と対策意欲を比較するための質問を演習実施前後にそれぞれ 5 段階評価で回答させた. また, 被験者のリテラシー自信度を測るために複数の IT 用語についての理解度を 4 段階で回答させたデータを基に両方式で被験者を 3 段階に分類した.

また, 対面実験形式で無効感軽減を攻撃者を模した演習により実施し, 関心を高める演習をメール判別で行う実験も実施している. こちらについては, どちらの演習を先に行うかでグループ分けを行っており被験者は 4 名ずつである.

3.2　結果と考察

対策意欲を比較する質問の回答をリテラシー自信度ごとに分類したものを図 1 に示す. このとき「自信あり」間でのみ有意差が見られた ($p < 0.005$). このことから A 方式の方が幅広いユーザ層に対して対策意欲を高めるのに有効であると言える.

「自信あり」のユーザ間にのみ有意差が確認された理由として, 演習直後については演習終盤に与えられた印象が被験者に強く現れる傾向にあり, 提示されたメールの判別難度の違いが影響したためであると考えられる. A 方式では最後に Lv5, B 方式では Lv1 が提示されていたことから B 方式の「自信あり」の被験者には簡単すぎると感じられたと推測される. この傾向は対面実験に

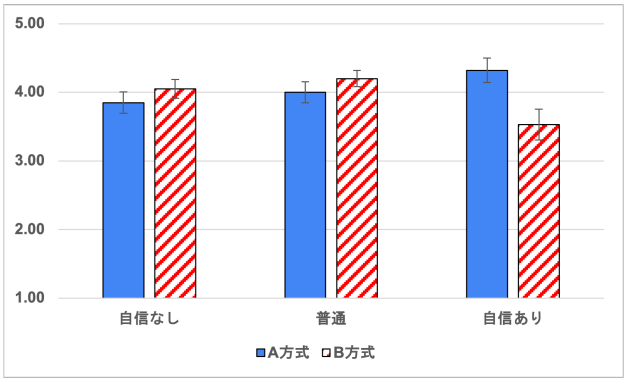

図 1　リテラシー自信度ごとの対策意欲 (平均)

て攻撃者側演習を最後に行ったグループにも同様の傾向がみられた. このことから, 無効感の軽減よりも関心を高めることを演習終盤に行うことが, 対策意欲の向上に有効であると考えられる.

4　演習啓発効果の定着度評価

4.1　実験

Web 上で両方式の演習と演習解説の提示を含めた 1 回目アンケートを実施した. その 2 週間後に 2 回目アンケートを行い, そこで回答した A 方式 138 名, B 方式 116 名を対象に分析を実施した. 被験者には啓発の受講経験の有無を答える質問と無効感と関心の度合いを推測する質問, フィッシングを認知した頻度, 1 回目を覚えているかを確認する質問を 5 段階評価で回答させた. また, 表 1 の Lv5 に相当するメール画像をフィッシングであると明言せずに提示し, 注目する箇所の優先順位を回答させた. 注目箇所の選択肢は, メールアドレス, ロゴ, クリックを促す赤字, マスクされたリンク, 署名, マウスオーバーで表示したリンクの 6 つとした.

4.2　結果と考察

定着度を評価するにあたって, 1 回目アンケートを覚えている可能性が高いユーザ群 (啓発の受講経験を有り, 1 回目を覚えているかの確認質問へ高い点数で回答, 以下: True 群) とそうでない群 (以下: False 群) に分類した. True 群が回答したロゴの優先順位は A 方式が 4.32(SE: 0.39), B 方式が 5.59(SE: 0.20) としていた. これに対して, False 群は A 方式が 3.43(SE: 0.18), B 方式が 3.86(SE: 0.18) であり, 大きな差がみられないことが確認できた. このことから演習実施を覚えていた場合, B 方式の方が明らかにロゴへの優先順位を低く設定していることが確認できた.

メールの構成要素においてロゴは非常に注目を集めやすく [3], 昨今のフィッシングメールにおいては常習的に用いられているため, 演習解説においてロゴの有無はメールの正当性を判断する要素として不適切であると示していた. 従って, 2 回目においてロゴの優先順位を低いと回答するユーザが多い B 方式は演習啓発の効果が定着したことが認められると考えられる.

表 2　B 方式ユーザ群の回答 (平均)

質問	True	False	p 値
フィッシングを疑った頻度	2.90	3.08	0.62
無効感を推測する質問 †	4.18	3.85	0.07
関心を推測する質問 *	4.09	3.58	0.01

$^{\dagger}p<0.1$ $^{*}p<0.05$

加えて, B 方式ユーザ群の回答を表 4.2 に示す. True 群はフィッシングに脅威を感じており対策意欲が高い傾向にあることが伺えたが, フィッシングに敏感となるといった意識変容は確認できなかった. このことから, 継続的に啓発事項を意識していた訳ではなく, 1 回目と似た形式の質問を目にしたことで, 啓発内容を想起し対策意欲も高まったと推測される.

5　議論

本稿において示した 2 つの演習方式は, 一長一短の特徴があることが確認できた. これを踏まえて適切な利用場面を設定していくことで, 啓発手法を確立することが望ましいといえる.

A 方式は演習実施直後に対策意欲を有意に高めるため, 講師を伴う啓発実施に際して脅威認知を促すためのデモ演習の設計に適応することで, 参加者の関心を高めて, 受講へ意欲的とさせるのに有用である. B 方式は期間をおいても啓発内容に基づいた回答を行えることが確認できたため, 各ユーザ個々人で実施させる演習の設計に適応することで留意事項を定着させることが期待できると考えられるが, インシデントの危険性が生じる際に想起するように留意事項を提示する必要がある.

6　まとめ

近年, 増加傾向にあるフィッシングメールを題材として, セキュリティ対策行動を促す啓発手法の提案と評価を行った. ヒューマンファクタをもとに演習方式を設計することで幅広いユーザ層の対策意欲を高める要素とユーザ特性の関連を分析した. 加えて, 演習実施から期間をおき啓発効果を確認することで定着度を評価した. これらの実験結果を踏まえて演習方式の特徴を活かした啓発手法を提案した.

参考文献

[1] JNSA 調査研究部会. 国内情報セキュリティ市場 2020 年度調査報告. https://www.jnsa.org/result/surv_mrk/2021/data/report2020.pdf. (Accessed on 01/2023).

[2] 諏訪博彦, 原賢, 関良明. 情報セキュリティ行動モデルの構築—人はなぜセキュリティ行動をしないのか. 情報処理学会論文誌, Vol. 53, No. 9, pp. 2204–2212, 2012.

[3] 閻鳳, 馬遠, 藤波努. フィッシングメールが人を欺く要因. 情報処理学会研究報告, Vol. 2022-SPT-46, No. 7, pp. 1–7, 2022.