フィッシング詐欺における攻撃者への信頼の判断を左右する心理的要因の概説

稲葉　緑*

概 要

本稿では、フィッシングメールを信頼できるとの直感的な判断を促進する要因を心理学的観点から概観し、そのことで、ユーザにとって分析的な処理による判断がいかに難しいかについて示す。また、直感的に正しい信頼判断へと導く対策について考察する。

1 はじめに

フィッシング詐欺とは、金融機関や小売店などを装って電子メール（以下、「メール」と呼ぶ）を送り、重要な個人情報（住所、氏名、銀行口座番号、クレジットカード番号、パスワードなど）を搾取する行為を指す（フィッシング対策協議会 a, 2017）。典型的な例は、フィッシング詐欺の攻撃者から送信されたメール（「フィッシングメール」と呼ぶ）にリンクが貼り付けられている。メールを受け取った人（「以下、「ユーザ」と呼ぶ」がそのリンクをクリックするとフィッシングサイト（攻撃者が用意した個人情報を盗むためのサイト）が表示され、ユーザに個人情報の入力を求める。

このような攻撃に対し、膨大な数のフィッシング対策技術が研究され、導入されている（加藤ら, 2010；Dong, Clark, & Jacob, 2010; Mohammad, Thabtah, & McCluskey, 2015；Salah et al.,2013; Zhang et al., 2011; Purkait, 2012 for a review）。それにもかかわらず攻撃数に変化はない。2016年度末の時点で、世界に存在するフィッシングサイトの件数は60万件を超える（APWG, 2016)。また、フィッシングサイトに誘導するためのフィッシングメールについては、約23万種類が報告されている。日本ではフィッシング情報の届出件数は減ったものの、フィッシングサイト数は横ばいである（フィッシング対策協議会, 2017）。このことは、攻撃者がフィッシング攻撃の手を緩めていないということを意味する。その理由として、この種の攻撃が収益を上げているからであり、その背景には、ユーザの詐欺に対する脆弱性がある。

これに対し、なぜユーザがフィッシング詐欺に引っかかるのかという問いへの取り組み、効果の高い対策について検討した研究はほとんど見られないことが問題視されている（Halevi et al., 2013; Jakobsson & Ratkiewicz, 2006）。多くの組織や企業は、インターネットやメールに関する技術的な知識（例えば、ポインタをリンクの上に置いてステータスバ

* 情報セキュリティ研究科 准教授

ーに表示されるURLを確認する、など。このような知識を以降、「技術的知識」と呼ぶ）を使ってメールを確認し、送信元を信頼できるかどうか判断するといった対策の実行をユーザに呼び掛けている。これらの対策がユーザ間で浸透した様子はみられていないにもかかわらず、多くの先行研究は、技術的知識を習得させることを目指した教育の効果を検証するに留まっている（Kumaraguru et al., 2009; Sheng et al., 2007; Moreno-Fernández et al., 2017; Yan & Gozu, 2012）。さらにこれらの研究の中には、その有効性を支持しない結果について報告したものもある（Kearney & Kruger, 2014）。しかし、人間の心理や情報処理の特徴の観点から、どのような対策が効果的なのか体系的に明らかにしようとするアプローチはなされていない。

本稿では、効果的なユーザ向けの対策について考察することを目的とし、フィッシング詐欺の成否に影響を及ぼす要因についての知見を心理学的観点から概観する。特に、次の 2 点に焦点を当てる。第一に、ユーザのフィッシングメールへの信頼に注目する。先行研究でも指摘されているように、フィッシング詐欺に関する先行研究の多くは、ユーザがフィッシングメールからフィッシングサイトに移行した後に詐欺を見抜くことをテーマとしている（Anandpara et al., 2007; 小倉, 2017）。しかし、著者はフィッシングサイトに移行した時点でユーザが詐欺に気づくことは難しいと推察する。ほとんどのユーザは、フィッシングメールが信頼できないものであると認識すれば、そのメール内のリンクをクリックしない。フィッシングサイトを見ているユーザは、フィッシング詐欺の攻撃者について信頼する、あるいは、不審に思う点は無いか少ない、との自身の判断を前提としてサイトを見ている。すなわち、そのようにして見ているサイトがフィッシングサイトかどうかを見抜こうとする行為は、自分の下した判断に反する証拠を見つけようとする行為であることを意味する。これは人間の心理上、非常に困難である（Kray & Galinsky, 2003）。したがって、フィッシングメールを送信した送信者（以下、「送信元」と呼ぶ）とユーザとの信頼関係が確固なものとなる前のフィッシングメールを処理する段階で、ユーザが送信元を信頼できないと認識することが重要であると考える。

第二に、フィッシングメールへの反応を左右する各要因と、ユーザの適応的な処理との関係に焦点を当てる。心理学には、我々が意思や判断を決めるにあたり、複数の処理が並行して機能すると考える伝統的なモデルがある（Ajzen, 1999; Chaiken & Duckworth, 1999; 神山, 2002; Petty & Cacioppo, 1986）。これらの処理は大きく 2 つに分類される。一つは、詳細な条件や目の前の問題に関係する事例の記憶を思い出して使ったり、複数の選択肢についての長所・短所を精緻的に比較したりして解を出す「分析的処理」である（「統制的処理」や「意識的処理」とも言う）。本人が「よく考えよう」という意思をもって丁寧に問題を検証する処理であり、注意力も時間も要することが多い。もう一つは「自動的処理」である（「無意識的処理」とも言う）。過去に処理した問題に関するイメージやそこからの類推に頼ったり、情報の一側面を手がかりにしたりして、問題の「おおまかな正解」を出そうとする。本人の考えようとする意思を伴わないまま進み、注意力も少なくて済むだけでなく、解を出すまでの時間も概ね短い処理である。特にこの自動的処理に大きく依存した意思決定方略は「ヒューリスティックス」と呼ばれる（Chaiken, 1980; Tversky & Kahneman, 1974）。我々は常に、音や匂いの知覚といった自覚していないレベルの問題から、頭をフル回転させて正解を求めようとする試験問題のようなものまで、複数の問題への対応を同時に求められている。このような問題全てに対して分析的処理をしようと思っても時間や処

理能力といった制約上、不可能である。これらを最適化するため、近似解を求めるヒューリスティックスを我々は多用しながら膨大な数の判断を下している。ヒューリスティックスを利用する傾向は、タイムプレッシャーなどによって冷静さを欠いたとき（「至急」「期間限定」などの言葉をみて焦ったときなど）や疲労時に特に強まるとされる（Shiv & Fedorikhin, 1999）。

次節でより詳細な仮説を述べるが、著者は、多くのユーザがメールの送信元を信頼できるかどうかについてヒューリスティックスを使って判断していると予測している。それに対し、推奨されている対策は、心理学的には、「分析的処理に大きく依る判断をしなさい」というものである。1 通 1 通のメールに対して追加的な分析的処理を実行しなければならないとしたら、ユーザの負荷は指数関数的に増加するはずである。このような膨大な負荷の増加が対策の展開を妨げる要因の一つであると推測し、ユーザが正しいヒューリスティックスへと導く方法を考案することが、現状の打開につながると考える。そのためにはまず、ヒューリスティックスによる誤った判断が何によるものなのか把握する必要がある。

以上から、本研究では、フィッシングメールへの信頼を対策する際、誤った解を出すヒューリスティックスを促す要因について探り、その後、ユーザの情報処理能力を考慮した対策について論じる。

2　ヒューリスティックス利用を促進する要因の選定およびその前提

本研究で論じるフィッシングメールは、Siadati, Jafarikhah, & Jakobsson (2016）のフィッシングメールの定義によるものとする。彼らは迷惑メールを「スパムメール」、「トロイの木馬」、「詐欺メール」に分類し、「詐欺メール」をさらに、「フィッシングメール（重要情報の盗難を目的としたメール）」、「前払い金詐欺メール」、「ビジネスメール詐欺」に分けている。本研究の概説は詐欺メール全般に当てはまるものであると思われるが、参照とした先行研究の範囲は「フィッシングメール」に関するものに限定している。ただし、企業や組織に侵入するために個人情報を盗もうとする「ビジネスメール詐欺」に関連した知見は参考としている。

次に、フィッシングメールへの信頼の判断に関するヒューリスティックスを促進する要因を選定するにあたって設定したユーザの判断に関する前提を説明する。

前提1．メールを「信頼する」姿勢をユーザはデフォルトとして持つ

人間は基本的に他者を信頼し、そのメッセージを真実だと捉える性質を持つとの知見に依る (Morgan & Laland, 2012; Ostrom, 1998; Penner et al., 2005; Hill & O'hara, 2005; Burgoon & Levine, 2010)。

前提2．送信元情報だけでなくメッセージを含むメール全体を、メールを信頼するかどうかの判断材料とする

正当な送信元から送られたメールかを判断する際、ユーザは送信元のメールアドレスだけでなくメッセージを重視するとの報告に基づく（Garfinkel & Miller, 2016）。

前提3．「メールを理解する」工程で、メールに対する信頼を判断する

複数の目標（あるいは課題）が存在するとき、我々はそれぞれの目標について重要度を評価し、重要度の高い目標に関する処理に注意力を向け、また、優先して実行する（Bada & Sasse, 2014; Förster, Liberman & Friedman, 2007）。メールの本来の目的がコミュニケーションである点を踏まえると、ユーザが届いたメールをみるとき、「メールがフィッシングメールかどうかを見極める」ことよりも「誰が何を伝えようとしているのか理解する（以下、「メールを理解する」と呼ぶ）」ことの方が重要であり、後者に関する処理が優先して実行されると考えられる。それでは、メールを理解した後に、そのメールがフィッシングメールかどうか改めて見極めようとするかというと、そのようなユーザは滅多にいないだろう。しかし、フィッシングメールに気づくこともあることから、我々はメールが信頼できるものか全く判断していないわけではないとも言える。ここから著者は、「メールを理解する」処理を通して、そのメールが信頼できるかヒューリスティックスを使って判断していると考える。メールの正当性について詳細に検証しようとする際も、多くの場合は、「メールを理解する」処理を通して生まれた不信感や違和感がきっかけとなると推測する。

3　ヒューリスティックスによるフィッシングメールへの信頼の判断を促進する要因

3 つの前提に基づき、フィッシングメールの成否を左右する要因についての先行研究を調査した結果、メールへの信頼を判断するためのヒューリスティックスに影響を及ぼすものは、次の 5 つの要因に集約された。

1. 既知のフィッシングメールとの形態的一致性
2. 感情的要素
3. 言語的間違い
4. ユーザとの関連性を認識させる要因
5. 送信元の知名度や規模に関する要因

このうち、フィッシングメールに限定されない「1. 既知のフィッシングメールとの形態的一致性」と「言語的間違い」については次節では触れず、ここで簡単に述べる。

ユーザはメールの送信元や伝えようとしている内容について理解しようとする前に、スパムフィルタ同様、形態的処理（パターンマッチング）を行うと考えられる。メールの中に過去に見たことのある、あるいは、よく知っているフィッシングメールのパターンや言葉（例えば、“Save up to 80% OFF”というタイトル）を見つけ、それがフィッシングメールかどうかはわからなくとも不審に思い、メッセージを見ずに廃棄する人も多いだろう。Downs, Holbrook, & Cranor (2006)でも、よく知られているフィッシングメールのパターンとの一致性が、調査参加者がメールを廃棄する一番の理由として報告している。

また、言語的な間違いもユーザのメールへの信頼感を顕著に低下させることが報告されている。我々は文を読むとき、先の文字や言葉を予測しながら文字を追っている。その予測から文法的に、あるいは、意味的に外れた文字や単語が現れたときに我々の中に違和感が生まれるまでは 0.5 秒も要しない（Bruni, Baceviciute, & Arief, 2014）。このような「おかしな言葉遣い」が含まれていると、早々と「きちんとした送信元ではない」と判断されやすい（Downs et al., 2006）。

上述した形態的処理における既知のフィッシングメールのパターンとの一致性、および、メールに含まれる言語的処理における文法上・意味上の間違いは、ユーザのメールに対する信頼を大きく損なわせる。ただし、これらの点で問題がないことは、他の正当なメールと変わらない。次節では、詐欺の成功に関与するフィッシングメール特有の要因に焦点を当てる。

3.1 感情的要素

ヒューリスティックスの一つに、感情ヒューリスティックスと呼ばれるものがある（Slovic et al., 2005）。心に湧き上がる感情やそれに伴う心身の反応を情報の一側面として利用する意思決定方略である。この仕組みを悪用し、攻撃者はユーザにメールへの誤った信頼の判断をさせようとしている。ただし、このような企みが成功する度合は、ユーザの特徴によって、また、同じ一人のユーザでも時と場合によって差がある。本節では、メールのタイトルやメッセージ（以降、合わせて「メールの内容」と呼ぶ）に含まれる感情的要素の影響と、その影響の受けやすさを左右するユーザ側の心の状態について、それぞれ解説する。

3.1.1 メールの内容に含まれる感情的要素

典型的な詐欺は、攻撃者の指示や提案に従えば利得を得られる可能性（「ベネフィット」とも言う）、あるいは、従わなければ損失を被る可能性（「リスク」とも言う）を示してユーザの感情を揺り動かし、騙そうとする（Langenderfer & Shimp, 2001; University of Exeter School of Psychology, 2009）。フィッシングメールも例外ではない。2017 年 9 月、米マイクロソフト社の名を語り、「あなたが使っているソフトのプロダクトキーが何者かにも不正に利用されている。メールに貼り付けられているリンクをクリックして登録されているユーザ本人かどうか確認できなければソフトを使えなくなる」という内容のフィッシングメールが送信された（フィッシング対策協議会，2017b）。これはソフトを使うことができなくなるというリスクを示し、ユーザの不安を喚起する例である。

人間は環境に適応し、生き抜くために、強い感情を引き起こすベネフィットやリスクなどに関連した情報に対して迅速に、かつ、集中して対応する情報処理の仕組みを備えてきたと考えられている（Lowenstein, 1996）。我々は感情的な要素を含む言語情報を無味乾燥な情報よりも注視し（稲葉 & 大平，2003）、また、労力をかけて処理する（Hofmann et al., 2009）。

フィッシング攻撃に対する人間の脆弱性について研究してきたJacobsson（Anandpara et al., 2007）は、「ユーザは何らかの損失を被るかもしれないと思うと、メールの詳細を理解せずとも、まずは反応してしまう」と嘆いているが、これは上述した人間の情報処理の仕組みに基づく感情的ヒューリスティックスに因る。攻撃者は「金（money）」や「痛み（pain）」といったベネフィットやリスクを直接的に表す言葉をタイトルやメール本体の冒頭など目立つ位置に配置する（University of Exeter School of Psychology, 2009）。感情を喚起する言葉をユーザの視界に入るようにすることで、攻撃者はユーザがじっくりと考える機会を奪い、リスクやベネフィットに対して直感的に反応させることを狙う。

3.1.2 ユーザの感情に関する状態

我々は誰しも、メールの内容に含まれる感情的要素に敏感に反応する。ただし、その程度には個人差があり、特に「性格」による差についての研究が進められてきた。また、性格のような変化の少ない状態ではなく、限られた時間のみ機能する感情についての研究報告もある。ここでは性格と一時的な感情による感情ヒューリスティックスの知見をそれぞれ紹介する。

(1)性格的要因

フィッシング詐欺の訓練を受けた後でも、どうしても詐欺にひっかかってしまうタイプの人がいる。例えば Caputo (2011)の実験では、訓練後も実験参加者の 20%の人がフィッシングメールを見抜けなかった。このような個人差を説明する要因として注目されているのが性格である。フィッシングメールへの反応を促進する性格特性として最も多くの研究で報告されているのは、「神経症的傾向」や「不安傾向」である(Halevi, Lewis, & Memon, 2013; Amichai-Hamburger & Ben-Artzi, 2000, 2003; Welk et al., 2015)。基本的に他者を疑うことが少なく(Enos et al., 2006)、情報の感情的要素に対して強く反応しやすい、気持ちが動揺しやすいなどの特徴を持つとされる(Digman, 1990)。送信元を信頼するかどうかをじっくり判断しようとする姿勢が弱い上に、感情ヒューリスティックスによる判断をしやすいと考えられる。

また、女性はフィッシングメールの検出が苦手であると示されているが(Sheng et al., 2010)、先の神経症的傾向の高さと女性という条件を両方満たした場合に、その検出率がさらに下がることが報告されている(Halevi et al., 2013; Amichai-Hamburger & Ben-Artzi, 2000, 2003)。男性に比べると、女性は他者から賞賛されるため、あるいは、嫌われないための行動への欲求が強く(小島, 太田 & 菅原, 2003)、情報の感情的要素に敏感であるとされる(Amichai-Hamburger & Ben-Artzi, 2003)。神経症的傾向により情報の感情的要素に敏感な傾向がさらに強まり、感情的ヒューリスティックスに依存しやすいと推察される。

一方、上述した性格の人に比べ、フィッシングメールの検出が得意な人もいる。落ち着きがあり、感情のコントロール能力が高い性格や(Welk et al., 2015)、計画的に物事を進めようとする性格(Modic & Leal, 2011)の人である。これらの性格を持つユーザは、感情的な要素を含む情報によって喚起された感情を抑制することができるために、この感情のみを使うヒューリスティックスによる判断をしにくいのかもしれない。

(2)一時的気分の要因

我々は嬉しい気分のときもあれば悲しい気分のときもある。このように一時的、あるいは、限られた時間に続く感情がフィッシングメールへの対応を左右することがある。例えば、技術的知識の教育よりも、フィッシングメールに対する嫌悪感や警戒感を刺激することによる感情ヒューリスティックスの方が、危険なメールを廃棄するという点において効果が高いことが示されている。Parsons et al.(2015)は正当なメールとフィッシングメールとを見分ける能力を調べる実験で、ある実験参加者群には事前に実験の真の目的を告げた。一方、別の参加者群には異なる目的を伝え、真の目的は実験後に明らかにした。2 つの参加者群

の違いは真の目的を告げたタイミングのみであるが、事前に伝えた群の参加者の方がメールをフィッシングメールであると分類した。これらの群の参加者の方が、フィッシングメールに騙されないための警戒感を持ったためであると思われる。ただし、Anandpara et al.（2007）の同様の実験では、正当なメールも悪意のあるメールであると参加者が廃棄しやすいことが確認されている。しかも、フィッシング攻撃に関する教材を読んだ後でさえ、正当なメールも廃棄する傾向は低下しなかったと報告している。

しかし、この効果は長く続かないと予測する。フィッシング攻撃に関する知見ではないが、Bullee et al. (2016) は実験参加者に、知らない人からファイルをダウンロードするように電話で勧められる攻撃に注意を促す情報セキュリティキャンペーンを行った。その 1 週間後、あるいは、2 週間後に警告した種類の模擬的攻撃を各実験参加者に対して実行した。結果、ファイルをダウンロードした人数の割合は、1 週間後に攻撃を受けた参加者のうち 9.1％であったが、2 週間後の場合には 54.6％に跳ね上がった。この割合は、事前にキャンペーンを受けずに攻撃を受けた場合と変わらなかった。我々には一つの感情を長期間強く持ち続けにくい性質があり、注意喚起によって被害を受けたくないという感情が低下すると、防御的な感情的ヒューリスティックスを使わなくなると考えられる。

3.2 メールの内容においてユーザとの関係性を暗示する要素

我々はメッセージの内容から、メールの送信元は過去に自分自身の情報を渡した相手だと思いこむことがある。あるサービスのアカウントに関する内容のメールであれば、アカウントを持っていることを知るサービス企業であると思うだろう。Jakobssonら（Jakobsson & Ratkiewicz, 2006）は米大手オークションサイトのユーザに対し、フィッシングメールを模したメールを実験的に送信した[備考]。このオークションサイトでは、正当なメールには必ずユーザ名がメールの冒頭に書かれているので、それを確認するようユーザに注意を促している。先の実験ではユーザ名を含むメール、あるいは、含まないメールを各実験参加者に送信したが、参加者からの返答率に違いがほとんどみられなかった。これは、我々は送信元が信頼できる相手であることの証拠がなくても、過去の経験や通例から自分と他者との関係を推し量るヒューリスティックスによって判断しているためであると解釈できる。

このヒューリスティックスによる判断をさらに促進するのが、名前など、ユーザ自身に特化した情報である。メールの内容に自分の情報が含まれていれば、送信元は自分のことをよく知る相手だと容易に推測する（Jakobsson & Ratkiewicz, 2006）。これを使った有名な攻撃手法が「スピアフィッシング」である。多くのフィッシング攻撃では不特定多数にメールが送られ、各メールに個人を特定する情報は含まれていない。しかしスピアフィッシングでは、何らかの形で攻撃者がユーザの名前などの個人情報を入手し、その情報をメールに反映する（岡野ら, 2017）。これは標的攻撃型メールであり、ユーザに添付ファイルを開かせることでマルウェアに感染させるなどの手口が多いが、個人情報の盗難を目的としたものもある。企業や組織の社員や職員（ユーザ）に対し、社員の上司、あるいは、情報システム部門の社員になりすましてメールを送り、企業や組織の機密情報や知的財産を手に入れるためのパスワードなどを聞き出そうとする事例などがあるとされる（McAfee Labs,

[備考] この実験方法の詳細は次の書面にまとめられている：Jakobsson, M., & Ratkiewicz, J. Real-World Phishing Experiments: A Case Study. Retrieved from http://docs.apwg.org/ events /papers/Markus_apwg-version.pdf

2016）。攻撃者が各ユーザの個人情報をメール1通1通に反映させるのは、個人情報を挿入せずに一斉にメールを配信するのに比べて手間がかかる。それでもこのような手間をかけることで攻撃の成功率が上昇し、手間、すなわちコストをかけた分、あるいはそれ以上の見返りが得られる (Jagatic et al., 2007; Rocha et al., 2015)。Ferguson（2005)が米陸軍士官学校内で実施したスピアフィッシングを模した実験では、実験参加者の80％が模擬的フィッシングメール内のリンクをクリックした。この人数は、スピアフィッシングではないメールを送信した場合の4.5倍にのぼる。

さらに、これらのヒューリスティックスは、ユーザのセキュリティに関する意識によっても強められると考える。例えば、多くのユーザは、自分の情報が攻撃者から狙われていると思っていない（Acquisti et al., 2015)。我々の多くは赤の他人の情報に興味がなく、その入手方法も知らない。そこから類推して、他人も同様だと考える。Facebookやインスタグラムなどの SNSに自らアップロードした名前や最近購入した商品、旅行の予定などの非常にプライベートな情報を自分と無関係の人が見て悪用しようとしているとは想像もしない。SNSにアップロードされていた情報に基づいて模擬的なフィッシングメールを送る実験で、実験参加者のうち80％が実験メールの送信元を友達であると思い込み、そのメール内にあったURLのリンクをクリックしたことが報告されている（Jagatic et al., 2007）。このように、自身が攻撃者から狙われているという認識の欠如が、メールの信頼判断におけるヒューリスティックスを促進させる。

ただし、通常は入手が難しいクレジットカード番号の最後の 4 桁などの情報がメールに含まれていたり、組織を狙ったスピアフィッシングなどで実際の上司とのやりとりを再現されていたりすると、そのメールが信頼できるものかについて正しい判断をすることは非常に難しい、あるいは、ほとんど不可能であるとされる（フィッシング対策協議会, 2017）。企業などを狙ったメールであれば、パスワードを共有する際のマニュアルなどを事前に決めておくことで、ユーザ一人の能力だけに依存しない対策を講じることが可能であるとされる（伊藤 & 高見澤, 2014）。しかし、個人を狙ったメールとなると、技術的な知識を使って綿密に検証する、メール内に記された連絡先ではなくユーザが改めて調べた連絡先に状況を確認する、といった作業をユーザ自身がしなければならない。ただし、ユーザがメールに不信感を全く感じていない段階で上述した分析的処理をできるかというと、著者は悲観的な立場である。

3.3 送信元の知名度や規模に関する要因

相手米アンチフィッシングワーキンググループ（APWG）によれば、2016 年に送信されたフィッシングメールにおいて攻撃者が装った送信元は、全体の 42.71％が小売店、18.67％が金融機関であった (APWG, 2016) 。いずれもクレジットカードの使用やアカウント、ソフトの使用権利などをユーザに提供し、そのために個人情報をやりとりする企業であるが、それに加えて、「有名である」「大手企業である」といった特徴があるように思われる。個人情報を扱い得る立場であっても、知名度が低い企業や小規模な個人経営の店の名前が使われることは格段に少ないようにみえる。

この理由には、不特定多数のユーザにメールを送信した場合でも、有名で大手の企業の方が、多くのユーザと過去に取引履歴などを持っている可能性が確率的に高く、疑われ

にくいことがある。ただし、それだけではないと考えられる。聞いてすぐわかる名前の企業を装った方が、ユーザがヒューリスティックスによって送信元を信頼すると判断しやすいと推測される。心理学では、信頼は相手に対する信頼度（trustworthiness）に大きく依存し、これは「能力」「博愛性」「正直さ」の要素から構成されると考えられている(Colquitt, Scott, & LePine, 2007; Mayer, Davis, & Schoorman, 1995)。我々は有名な企業や大手企業の方が、資金的・技術的にも豊かで、社会的な評判を気にして顧客を重視するというイメージを持ちやすいだろう。このようなイメージに基づいて、送信元の知名度が高く規模が大きいほど、個人情報を渡しても悪いようにはしないだろう、とユーザが思いやすい可能性がある。

また、聞いてもわからないような名前の企業や組織からメールが届けば、多くの人は、その送信元がどのような団体なのか調べようとする。調べられることで攻撃が明らかになる可能性を攻撃者は回避しなければならないとの事情もあるのだろう。

ユーザのメールへの信頼には、メールの内容が大きく影響するが、ユーザの送信元に関する情報もみている（Garfinkel & Miller, 2005）。特にドメインを手がかりとすることが示されているため、攻撃者はドメインに有名・大手の企業の名前やそれに類似したアルファベットの綴りを挿入しようとする（Jakobsson & Ratkiewicz, 2006）。また、クリックすることでフィッシングサイトへ誘導するためのメール内のリンクのURLについても、そのドメインの偽装に攻撃者は力を入れるとされる（Jagatic et al., 2007）。

4　考察

本節では前節での概説に基づき、フィッシング詐欺からユーザが身を守る方法について考察する。フィッシング詐欺の攻撃は何段階かに渡って行われ、各段階における対策を考案するべきであるとされるが（Moreno-Fernández et al., 2017）、本稿は、イントロダクションでも示したとおり、ユーザがフィッシングメールを信頼できないと判断するヒューリスティックスを促す対策に焦点を当てる。

そうは言っても、著者の知る限り、ヒューリスティックスによって正しい判断をさせることに有効な方法は、それほど多様ではない。メールの正当性に対して警戒感を持たせること、そして、既知の危険との類似性を認識させることなどに限られる。

前者は主に、防御的な感情ヒューリスティックスに対する働きかけを目的とする。そのための方法の一つとして、本研究では、スパムフィルタでブロックされた悪意のあるメールの数をユーザが知る機会を与えることを提案する。フィルタでブロックされるメールの数をユーザが知ることはほとんどない。迷惑メールボックスの中を見れば、フィッシングメールを含む迷惑メールの数を知ることができるが、これは悪意のあるメールのほんの一部である。人間は基本的に、危険の発生頻度を過小評価し、中でも自分だけはその危険に遭わないと考える（Chapin & Coleman, 2009）。このような、自分は安全な状況にあると思いこもうとする「正常バイアス」は、「自分が知りたくなかったこと」「対応したくないこと」の情報を提供されても修正されにくい（広瀬, 2006）。悪意のあるメールが世の中にどの程度まん延しているのか、自分がどの程度攻撃に晒されているのか知らなければ、ユーザには攻撃に対する警戒心も、自身を守ろうとする動機も生まれにくい。フィッシングメール対策に限ったことではないが、具体的で明確な情報を使ってユーザに大量の攻撃を受けている現実に直面

させることが、防御しようという感情の働きを高めるための必要条件であると考える。

2つ目の対策は王道ではあるが、訓練などの教育である。従来の教育プログラムには、ユーザが様々なメール画面の画像を見て、それがフィッシングメールかそうではないかを回答し、その後、答え合わせをしながらフィッシングメールを見抜くための技術的知識を学ぶものがある。ただし、Anandpara et al.（2007）は上述したテストの一つである「フィッシングIQテスト」[備考]で実験参加者に技術的知識を学ばせてから、事前の通知をせずに実験用の模擬的なフィッシングメールを送り、多くの参加者がフィッシングメールを検出できなかったと報告している。スピアフィッシングといった巧妙な攻撃に対抗するためにも技術的知識を習得することは重要ではある。ただし、届いたメールがフィッシングメールであることに気づくという点については効果に限界があることを示すものであろう。

一方、University of Exeter School of Psychology（2009）は、詐欺にひっかからない人ほど攻撃者から届いた詐欺のメールやチラシを一瞥して廃棄する傾向を報告し、このような傾向を育てることがユーザの耐性強化に最も効果的である可能性を提案している。本稿でもこのような教育方法について検討する。具体的には、ユーザの警戒感を上昇させる、また、「見たことがある悪意のあるメールに似ている」とのイメージを植え付けることで、ヒューリスティックスによる正解の導出に効果的な方法を考える。著者は、Jacobsson & Ratkiewicz（2006）が実験で使ったような、事前にユーザに知らせずに日常生活の中で他のメールと同様に訓練用の模擬的なフィッシングメールを処理させる方法の有効性に期待する。ユーザに関連のある文脈の内容とするなどの工夫を施し（Caputo et al., 2014; Davinson & Sillence, 2010)、各ユーザに擬似的な被害体験あるいはヒヤリハット体験を持たせることを目標とする。これは、フィッシング攻撃に対抗する訓練プログラムの効果は、学習者が攻撃に遭遇しただけではなく、その攻撃によって被害に遭うことにより明確になるとの示唆に基づく（Kumaraguru et al., 2009）。

ただし、従来の研究ではここまでの提案に留まっている。上述した教育手法は、Kolb（1983）が示した体験型教育手法の一部である。Kolbによれば、訓練の効果をより顕著なものとするためには、フィードバックが必要である。また、行動心理学の知見に従えば、このフィードバックは実際のベネフィットや賞賛と結びついたものであることが望ましいとされる（West, 2008）。我々はフィッシング攻撃によって個人情報漏洩の被害を受ければ、その後はより安全な行動をとるように行動を改めるだろうと想像しがちであるが、それが誤りである可能性が示されている。個人情報の漏洩被害者の半分は、被害を受けた後も自身の行動を変えないとの調査結果がある（Raytheon, 2015）。具体的には、社員（ユーザ）の所属する企業のシステム担当者、あるいは、ユーザがアカウントを持つインターネットプロバイダなどが、リンクをクリックしてすぐに個人情報を提供しなければユーザは損失を被るといった内容の訓練用メールをユーザに送る。ユーザがこのリンクに期限までにアクセスしなければ、期限直後に正しい判断だったことを知らせる。その際、ポイントなどを提供したり、組織内の訓練であれば社員の肯定的な評価に反映したりする。リンクにアクセスした場合は、アクセス先のウェブサイトで訓練であることを明かし、技術的知識について紹介しながら当該フィッシングメールについて解説する（木村, 2013）。

最も重要なのは、訓練や教育プログラムを1種類、1回のみ配信しただけでは不十分だ

[備考] この研究で利用されたテストには次の URL からアクセスできる:
https://www.sonicwall.com/ja-jp/phishing-iq-test

という点である。高い頻度である必要はないが、不定期に、様々な内容や送信元の訓練用フィッシングメールを使い、断続的に上述した訓練を実施する点にある。知術的知識は一回習得すれば、多くのパターンのフィッシングメールに対応できるはずである。しかし、ある特定のパターンのフィッシングメールを学習してそれを検出できるようになっても、パターンが異なると見抜けないとされる（Anandpara et al., 2007; Junger, Montoya, & Overink, 2017）。したがって、訓練用メールにバリエーションを持たせ、様々なパターンに対応させることで、過去の経験に基づいた正しいヒューリスティックスによる判断を促すことを目的とする。断続的に実施するのは、先に述べたように、教育によるユーザの攻撃に対する警戒心は、いつまでも持続するものではない（Bullee et al., 2016）ことによる。また、技術的知識を1回学習したユーザが自分のフィッシングメール検出能力が高まったと思い、学習後のフィッシングメールと正当メールとの弁別テストで正解率が低下したとの報告がある（Kearney & Kruger, 2014）。一方、攻撃に対して特に脆弱なユーザについても、1回の訓練ではフィッシングメールを検出する能力が十分に高まらないことが示されている（Caputo, 2011; Kumaraguru et al., 2009）。

これらの訓練は技術的には実施可能であると著者は考える。現実における最大の障壁は、訓練や教育プログラムを提供する企業や組織が負担する人的およびシステム的コストであると認識している。自社のウェブページやリーフレットでセキュリティ上の問題をユーザに通知したり、社員や職員向けに訓練を実施したりしており、被害防止に努めている企業や組織は多くあるが (Kirlappos & Sasse, 2012)、先に提案した訓練を実施することには躊躇するだろう。一般ユーザ向けの訓練となれば、訓練を実施するコストだけでなく、正解に対するポイントや追加的サービスというコストも必要となる。

しかも、特に企業は、顧客（ユーザ）からの評判に敏感である。ほとんどのユーザは訓練が自分に必要ないと考え（West, 2008）、訓練を時間の無駄であると思っている（LaRose, Rifon, & Enbody, 2008）。そのことで、訓練を強制する企業への評価を下げるかもしれない。そこで、一般ユーザに訓練を提供する企業は参加者に対し、参加することによるメリットを示すなどして、参加者を募るという方法が考えられる。ただし、「危険なユーザ」ほど訓練に参加しないだろう。例えば、自分が危険に晒されているとの不安に耐えられず、危険の存在自体を認めないユーザ（広田, 増田, & 坂上, 2002）や、危険に対応すべきはシステムや会社だと考える無関心なユーザ（West, 2008）である。

これらの問題を解消するためには、国や自治体などの教育の実施に対する強い働きかけが重要になると考える。社員および職員向け訓練を推進する企業や組織に対しては、その訓練実施に要する経費等の負担を軽減するための仕組みをつくる。訓練や教育プログラムを提供するビジネスの創発を支援する。そのほかにも、一般ユーザ向けにも訓練を実施するための指針を作り、訓練を実施する企業に顧客からの不満が向けられないようにする工夫が必要である。大がかりな取り組みではあるが、このようなトップダウンによる働きかけの効果は、教育を推し進めるだけではない。メールなどのサービスを利用するユーザ全てが国のセキュリティ対策に対する本気度を知れば、他人事意識を低下させ、能動的にセキュリティについて学び、対応する必要性を認識すると期待される。社会のサイバー攻撃耐性を高めるという点で、非常に強力な対策となり得ると言えるだろう。

5 おわりに

心理学分野でもヒューリスティックスは判断ミスをもたらし、分析的処理が正しい判断への正攻法と考える立場がある（カーネマン，2012）。また、本論で述べた通り、スピアフィッシング対策など、ヒューリスティックスによる判断では攻撃に対抗できない場合もある。このような事実を踏まえた上で、それでも著者はヒューリスティックスによる正しい判断を促す対策「も」重要だと考える。ユーザが全てのメールについてフィッシングメールかどうか分析的に判断することが難しく、しかし、真のフィッシングメールを選択して分析的に判断しなければならないのであれば、そのきっかけとしてこれらのメールに対し、ユーザが「怪しい」と感じることが重要になる。この「怪しい」という感覚を生み出すことにヒューリスティックスが寄与すると推察した。特に最近は、メールによるフィッシング攻撃だけでなく SNS によるスミッシング攻撃が盛んであることが報告され（フィッシング対策協議会，2017c）、信頼できる送信元からのメールであるかについての判断にユーザが使える情報は少なくなっている。ここから、ユーザのフィッシングメールに対する直感を磨くことが増々必要になると考えている。

参考文献

[1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

[2] Ajzen, I. (1999). Dual-mode processing in the pursuit of insight is no vice. Psychological Inquiry, Vol. 10, 110-112.

[3] Amichai-Hamburger, Y.A., & Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the Internet. Computers in Human Behavior, 16(4):441–449.

[4] Amichai-Hamburger, Y.A., & Ben-Artzi, E. (2003). Loneliness and Internet use. Computers in Human Behavior, 19(1):71 – 80.

[5] Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ tests measure fear, not ability. In Proceedings of the 11th international conference on financial cryptography and 1st international conference on usable security, 362-366.

[6] APWG. (2016). Phishing activity trends report, 1nd quarter 2016: Anti-Phishing working group (APWG). Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf.

[7] Bada, M., & Sasse, M. A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour?, Grobal Cyber Security Capacity Centre: Draft Working Paper. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf.

[8] Bruni, L.E., Baceviciute, S., & Arief, M. (2014). Narrative cognition in interactive systems: Suspense-surprise and the P300 ERP component. ICIDS 2014: Interactive Storytelling, 164-175.

[9] Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. Proceedings of the inaugural Singapore Cyber Security R&D Conference, 107-114.

[10] Burgoon, J. K., & Levine, T. R. (2010). Advances in deception detection. New directions in interpersonal communication research, 201-220.

[11] Caputo, D.D. (2011). Leveraging Human Behavior to Reduce Cyber Security Risk: Spear-Phishing Study Design, Results and Discussion. Retrieved from

http://www.thei3p. org/docs/events/humanbehaviorworkshop1011/deannaspearphishing.pdf.
[12] Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. IEEE Security and Privacy, 12(1), 28-38.
[13] Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion, Journal of Personality and Social Psychology, Vol. 39, 752-766.
[14] Chaiken, S., & Duckworth, K.L. (1999). When Parsimony Fails…. Psychological Inquiry, Vol. 10, 118-123.
[15] Chapin, J., & Coleman, G. (2009). Optimistic bias: What you think, what you know, or whom you know? North American Journal of Psychology, 11, 121-132.
[16] Colquitt, J.A., Scott, B.A., & LePine, J.A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance, Journal of Applied Psychology, Vol. 92, 909-927.
[17] Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior, 26(6), 1739-1747.
[18] Dhamija, R., & Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. In SOUPS 2005-Proceedings of the 2nd symposium on usable privacy and security.
[19] Digman, J.M. (1990). Personality structure: Emergence of the five-factor model. Annual Review of Psychology, 41, 417-440.
[20] Dong, X., Clark, J.A., & Jacoby, J.L. (2010). Defending the weakest link: phishing websites detection by analyzing user behaviors, Telecommunication systems, 45, 215-226.
[21] Downs, J.S., Holbrook, M.B., & Cranor, L.F. (2006). Decision strategies and susceptibility to phishing, In SOUPS 2006-Proceedings of the 2nd symposium on usable privacy and security.
[22] Enos, F., Benus, S., Cautin, R.L., Graciarena, M., Hirschberg, J., & Shriberg, E. (2006). Personality Factors in Human Deception Detection: Comparing Human to Machine Performance. *Proceedings Interspeech*, 2281-2284.
[23] Ferguson, A. J. (2005). Fostering e-mail security awareness: The West Point carronade. EDUCASE Quarterly, 28(1), 54-57.
[24] フィッシング対策協議会 (2017a) フィッシング対策ガイドライン 2017 年度版. フィッシング対策協議会.
[25] フィッシング対策協議会.(2017b). マイクロソフトをかたるフィッシング(2017/0904), 緊急情報, Retrieved from https://www.antiphishing.jp/news/alert/microsoft_20170904.html
[26] フィッシング対策協議会.(2017c). フィッシングレポート 2017 －普及が進むユーザ認証の新しい潮流－. フィッシング対策協議会ガイドライン策定ワーキンググループ.
[27] Förster, J., Liberman, N., & Friedman, R. S. (2007). Seven principles of goal activation: A systematic approach to distinguishing goal priming from priming of non-goal constructs. Personality and Social Psychology Review, 11(3), 211-233.
[28] Garfinkel, S.L., & Miller, R.C. (2005). Johnny 2: A user test of key continuity management with S/MIME and Outlook Express. Proceedings of the 2005 symposium on Usable privacy and security, 13-24.
[29] Halevi, T., Lewis, J., & Memon, N.D. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. Proceedings of the 22nd International Conference on World Wide Web, 737-744.
[30] Hill, C.A., & O'hara, E.A. (2005). A Cognitive Theory of Trust. Minnesota Legal Studies Research Paper No. 05-51.
[31] 広瀬弘忠 (2006). 人はなぜ危険に近づくのか. 講談社.

[32] 広田すみれ, 増田真也, & 坂上貴之 (2002). 心理学が描くリスクの世界. 慶応義塾大学出版会.
[33] Hofma, M.J., Kuchinke, L., Tamm, S., Võ, M.L.H., & Jacobs, A.H. (2009). Affective processing within 1/10th of a second: High arousal is necessary for early facilitative processing of negative but not positive words. Cognitive, Affective, & Behavioral Neuroscience, 9, 389-397.
[34] 伊藤史人, 高見澤秀幸 (2014). フィッシング攻撃に対する組織的対策と効果の考察. 学術情報処理研究, No.18, 3-15.
[35] 稲葉 緑, & 大平英樹 (2003). 情動的刺激に対する選択的注意が高不安者の再認記憶に及ぼす影響. 心理学研究, 74, 320－326.
[36] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.
[37] Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In 15th International Conference on World Wide Web (WWW).
[38] Jones, H. S., Towse, J. N., & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. International Journal of Cyber Behavior, Psychology and Learning, 5(3), 13-29.
[39] Junger, M., Montoya, L., & Overink, E.J. (2017). Priming and warnings are not effective to prevent social engineering attacks, Computers in Human Behavior, 66, 75-87.
[40] カーネマン, D.(村井章子 訳)(2012). ファスト&スロー:あなたの意思はどのように決まるか(上・下). 早川書房.
[41] 神山貴弥(2002).情報処理と説得:精査可能性モデル, 深田博己(編著)説得心理学ハンドブック―説得コミュニケーション研究の最前線―, 北大路書房, 418-455.
[42] 加藤 慧, 小宮山功一朗, 瀬古敏智, 一瀬友祐, 河野耕平, 吉浦裕 (2010). コンテンツベースフィッシング検知手法の大規模実例評価と改良. 情報処理学会 研究報告 2010 年 3 月, 1－7.
[43] Kearney, W. D., & Kruger, H. A. (2014). Considering the influence of human trust in practical social engineering exercises. Proceedings of the Information Security for South Africa (ISSA), 2014.
[44] 木村壮太 (2013). メール攻撃危険予知訓練システムの開発. 情報処理学会研究報告 2013 年 12 月, 1－6.
[45] 小島弥生, 太田恵子, 菅原健介 (2003). 賞賛獲得欲求・拒否回避欲求尺度作成の試み. 性格心理学研究, 11 巻, 86-98.
[46] Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. Security & Privacy, IEEE, 10(2), 24-32.
[47] Kolb, D.A. (1983). Experiential learning: Experience as the source of learning and development, FT Press.
[48] Kray, L.J., & Galinsky, A.D. (2003). The debiasing effect of counterfactual mind-sets: Increasing the search for disconfirmatory information in group decisions. Organizational Behavior and Human Decision Processes, 91, 69-81.
[49] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, 10(2), 1-31.
[50] Langenderfer, J. & Shimp, T.A. (2001) Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. Psychology and Marketing, 18 (7), 763-783.
[51] LaRose, R., Rifon, N., & Enbody, R. (2008). Promoting Personal Responsibility for Internet Safety. Communications of the ACM, Vol. 51, no. 3.
[52] Lowenstein, G.F. (1996). Out of control: Visceral influences in behavior. Organizational Behavior and Human Decision Processes, 65, 272-292.

[53] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20, 709–734.
[54] McAfee Labs (2016). 脅威レポート. McAfee.
[55] Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. Computer Science Review, 17, 1-24.
[56] Modic, D., & Lea, S. E. G. (2011). How neurotic are scam victims, really? The big five and Internet scams. Paper presented at the 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology, Exeter, United Kingdom. Retrieved from http://ssrn.com/abstract=2448130.
[57] Morgan, T. J. H., & Laland, K. N. (2012). The biological bases of conformity. Frontiers in Neuroscience, 6, 87.
[58] Moreno-Fernández, M.M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior, Vol. 69, 2017, 421-436.
[59] 小倉加奈代 (2017) ユーザのフィッシングサイト回避能力と心理特性との関係性の検討. 情報処理学会研究報告 2017 年 5 月, 1－6
[60] 岡野 裕樹, 木邑 実, 辻 宏郷, & 青木 眞夫 (2015) 標的型攻撃メールの例と見分け方. IPA テクニカルウォッチ, 独立行政法人情報処理推進機構セキュリティセンター.
[61] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. Computers and Security, 52, 194-206.
[62] Ostrom, E. (1998). A behavioral approach to the rational choice theory of collective action: Presidential address. American Political Science Review, 92, 1-22.
[63] Penner, L. A., Dovidio, J. F., Piliavin, J. A., & Schroeder, D. A. (2005). Prosocial behavior: Multilevel perspectives. Annual Review of Psychology, 56, 365-392.
[64] Petty, R.E., & Cacioppo, J.T. (1986). The elaboration likelihood model of persuasion. in I. Berkowitz (Ed.) Advances in experimental social psychology, Vol. 19, San Diego, Academic Press, 123-205.
[65] Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. Information Management and Computer Security, 20(5), 382-420.
[66] Raytheon. (2015). Securing our future: Closing the cybersecurity talent gap. Survey Summary.
[67] Rocha F, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. Information & Computer Security, 23(2), 178-199.
[68] Salah, K., Calero, J.M.A., Xeadally, S., Al-Mulla, S., & Alzaabi, M. (2013) Using cloud computing to implement a security overlay network. IEEE Security and Privacy, 11 (1), 44-53.
[69] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. Proceedings of the 3rd Symposium on Usable Privacy and Security, 88-99.
[70] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
[71] Shiv, B., & Fedorikhin, A. (1999). Heart and mind in conflict: Interplay of affect and cognition in consumer decision making. Journal of Consumer Research, 26, 278–282.
[72] Siadati, H., Jafarikhah, S., Jackobsson, M. (2016). Traditional Countermeasures to Unwanted Emails, In Jakobsson, M. Understanding Social Engineering Based Scams, 51-62.

[73] Slovic, P., Peters, E., Finucane, M.L., & MacGregor, D.G (2005). Affect, risk, and decision making, Health Psychology, Vol. 24, S35-40.
[74] Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases, Science, New Series, Vol. 185, No. 4157, 1124-1131.
[75] University of Exeter School of Psychology. (2009). The psychology of scams: Provoking and committing errors of judgement, Technical Report OFT1070, Office of Fair Trading. Retrieved from http://www.oft.gov.uk/shared_oft/reports/ consumer_protection/ oft1070.pdf.
[76] Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E., Mayhorn, C.B. (2015). Will the Phisher-Men Reel You In? International Journal of Cyber Behavior Psychology and Learning 5 (4), 1–17.
[77] West, R. (2008). The Psychology of Security. Communication of the ACM, Vol.51, No.4.
[78] Yan, Z., & Gozu, H.Y. (2012) Online Decision-Making in Receiving Spam Emails Among College Students. International Journal of Cyber Behavior, Psychology and Learning, 2 (1), 1-12.
[79] Zhang, H., Liu, G., Chow, T. W. S., & Liu, W. (2011). Textual and visual content-based anti-phishing: A bayesian approach. IEEE Transactions on Neural Networks, 22(10), 1532-1546.