ISP およびメールボックスプロバイダー向けフィッシング対策のベストプラクティス

第 2.01 版　2015 年 6 月

M³AAWG（Messaging, Malware and Mobile Anti-Abuse Working Group）と APWG（Anti-Phishing Working Group）が共同作成した文書

1. 序論

フィッシングは、クレジットカード番号、暗証番号、口座データおよび他の情報などの個人データや個人情報を盗むように設計された電子メールや詐欺ウェブサイトを利用したオンラインの個人情報の窃盗の一種です。また、フィッシングは、金融機関、オンラインゲーム、電子メールプロバイダなどになりすます攻撃からユーザーをもっと保護するべきだと要求するユーザーからの圧力を受ける ISP やメールボックスプロバイダーにとっては大きな懸案事項です。

ISP やメールボックスプロバイダーは、近年、顧客離れや訴訟の可能性を軽減するために、フィッシング攻撃を減らす世界規模の取り組みに積極的に参加しています。本文書は、フィッシング攻撃に対抗するために、M3AAWG のメンバー（www.m3aawg.org）が利用するベストプラクティスについて記載しています。

2. インバウンド保護方式

1. フィッシングメッセージのインバウンドフィルタリング

   フィッシングメールに対抗するための最前線の防衛策で最もよく知られているのは、最初にメールを受信するメール転送エージェント（MTA）やメールサーバーにおいてフィッシング対策やスパム対策フィルタリング技術を利用することです。これは通常、ISP またはメールボックスプロバイダーがスパムの検出とフィルターのために配備しているスパム対策ソフトウェアを利用して実現されます。

   複数の対策技術が開発され、現在スパムのフィルターに利用されています。しかし、これらの技術の多くは、大量で利益が低く、カスタマイズの少ないスパムを捕捉するよう設計されています。少量でカスタマイズの多いフィッシングメッセージに対しては、うまく機能しないことがよくあります。

   多くのメッセージングセキュリティシステムでは、スパムはタグ付けされ、ユーザーの受信箱や特別な「スパム」用フォルダに配信され、ユーザーは配信されたメッセージを検閲し、スパムか

正規のメールかを自ら判別することができます。残念ながら、ユーザーがスパムフォルダに山積みとなったフィッシングメッセージを発見し、フィルタリングエンジンが判定を誤ったと思い込み、フィッシング詐欺師のサイトへのリンクをクリックするのはよくあることです。したがって、ISP やメールボックスプロバイダーは、検出したフィッシングメッセージをユーザーに配信するよりは、ユーザーがメッセージにアクセスしないようにするか、あるいは少なくともユーザーがメッセージによって被害を受けないようにするべきです。この動作は、メッセージを拒否して SMTP トランザクションで 550 レベルの応答を返信したり、リンクや添付ファイルさらには reply や reply all の機能を無効にしたり、あるいはメッセージを削除することによって実現することができます。

メッセージを受け付けた後うまく削除することにより、ユーザーがそのメッセージにアクセスして、フィッシングであるという判断を誤って覆してしまうことを防ぎます。しかし、これは危険性の高い方法です。なぜなら、メールフィルターがフィッシングメッセージであると誤って判断した場合、送受信側共に、メッセージが削除されたことに気付かないからです。送信側はメッセージが配信されたと思い込み、受信側は正規かつ重要であるかもしれないメッセージを受信したことに全く気付きません。

メッセージが認証されたことを示す視覚的合図は、慎重に使用しなければなりません。視覚的合図がユーザーの行動に影響を与えるという決定的な証拠はなく、実装が不十分であるとユーザーのセキュリティが低下します。認証されたすべてのメールに対して、送信側のレピュテーションを問わず視覚的合図を出した場合、ユーザーは認証と信頼を混同することからユーザーのセキュリティが低下します。信頼できる送信側が視覚的合図を得ることができる注意深く管理されたシステムのみが、メールを認証するよう送信者を促すことができます。

推奨

a. フィッシングをフィルタリングするための重層的アプローチには、一部または全部技法を組み合わせることを推奨します。理想的には、ISP やメールボックスプロバイダーは、複数のソリューションを比較して、フィッシング攻撃を止めるための有効性を判断すべきです。

b. 可能であれば、電子メールメッセージを受け取る前に、フィッシングメッセージを拒否または破棄します。

c. ユーザーの要求により、あるいは ISP やメールボックスプロバイダーの方針や法基準により、メッセージを破棄することが難しい場合、ISP やメールボックスプロバイダーは、これらのメッセージがフィッシングメッセージであると特定されたことや、正規のメッセージのように見えるかもしれないが危険性があるので無視すべきであることをユーザーに示すべきです。ISP やメールボックスプロバイダーはさらに、フィッシングメッセージに含まれるリンクや添付ファイルを無効にするべきです。

d. ISP やメールボックスプロバイダーは、ユーザーのメールボックスにメッセージが配信された後にメッセージを検閲し、そのメッセージがフィッシングであるという情報が後で得られた場合には、これまでのフィルタリングの判定を覆すことができるようにする

べきです。

2. エンドポイントフィルタリングおよびクライアントサイドフィルタリング

ユーザーのメールソフトウェアのプラグインとして組み込まれ、フィッシングメッセージを特定する複数の無料および有料のエンドポイントセキュリティーソリューションが存在します。これらのソリューションは、ISP やメールボックスプロバイダーがサーバーレベルでフィッシングフィルタリングを提供できない場合に有効となる可能性があります。また、エンドポイントソリューションを推奨するのは、ISP やメールボックスプロバイダーのインフラ内に存在しない可能性があるものも含む複数のアカウントから、ユーザーがメールにアクセスする場合にユーザーを保護できることからです。

また、サーバサイドソリューションが、メールを配信するときに呼び出されるのに対して、エンドポイントセキュリティソリューションは、ユーザーがメールを読むときに呼び出されます。多くの場合、メールの配信と処理の間の待ち時間は、エンドポイントフィルターを更新するには十分であることからセキュリティが改善されます。

推奨

a. ISP やメールボックスプロバイダーは、フィッシングに対抗するためにローカルで動作する電子メールスキャンソフトウェアや、悪意のある添付ファイルに対抗するためにマルウェア対策ソフトウェアなどのエンドポイントセキュリティソリューションを採用するように、ユーザーに働きかけるべきです。

3. 送信ドメイン認証による偽造検出

Sender Policy Framework[1]（SPF）、Domain Keys Identified Mail[2]（DKIM）および Domain-based Message Authentication, Reporting & Conformance[3]（DMARC ）などの電子メール認証は、広く採用されるようになっています。電子メール認証は、送信者が自分の個人情報を偽造しているか否かを判定するのに利用することができます。フィッシング詐欺師は、多くの場合、メッセージが正規の組織から発信されたかのように見せるためにヘッダー内の情報を偽造しようとします。送信ドメイン認証は、利用可能であれば、偽造を検出するのに使用できる場合が多い。

推奨

a. ISP やメールボックスプロバイダーは、送信者の個人情報が偽造されていると明白に判断できる場合、電子メールをフィルタリングまたは拒否を行うべきです。

b. ISP は、組織の通知メッセージとユーザーの電子メールをそれぞれ異なるドメインから送信するべきです。つまり、notifications@isp.example や user1@isp.example の代わりに、

[1] http://tools.ietf.org/html/rfc7208
[2] http://tools.ietf.org/html/rfc6376
[3] https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base/?include_text=1

notifications@notifications.isp.example や user1@isp.example のドメインから送信するべきです。これらのシステム通知は、SPF、DKIM および DMARC を利用して認証するべきである。

4. 信頼できないソースからの画像の非表示

正規のメールを送信する信頼できる送信者と、正規のメールを送信しないフィッシング詐欺師とを識別するために、画像はデフォルトで無効とし、信頼できるメッセージに組み込まれている場合にのみ表示すべきです。

フィッシングの脅威を軽減する別の方法は、信頼できない電子メールに含まれるハイパーリンクを無効にすることです。これにより、フィッシング詐欺師がユーザーを騙して、詐欺サイトへのリンクをクリックさせることがさらに難しくなります。

推奨

a. ISP やメールボックスプロバイダーは、送信側の個人情報やレピュテーションを明らかにできないすべてのメッセージに関して画像を無効にして、ユーザーが画像を有効にする機能を提供すべきです。

b. ISP やメールボックスプロバイダーは、信頼できないソースからの HTML コンテンツ（新しいウインドウや iFrame など）の遠隔からのダウンロードを無効にするべきです。

c. ISP やメールボックスプロバイダーは、信頼できないソースからの電子メールに含まれるハイパーリンクはすべて無効にするべきです。

5. マルウェアが通常利用する添付ファイルの種類をブロック

マルウェアの作成者は通常、ユーザーにリンクをクリックするよう説得する代わりに、電子メール内のある種の添付ファイルを利用して、マルウェアを送信します。これらの添付ファイルの種類は、自動的に開封、実行されます。これらの添付ファイルを、メールサーバーレベルあるいはメールクライアントでブロックすることによって、ユーザーが不用意に添付ファイルを開いて、感染してしまうことがさらに難しくなります。

推奨

a. ISP とメールボックスプロバイダーは、マルウェアを送信するのに広く使用される添付ファイルの種類を無効にするべきです。例えば、Microsoft Outlook は、デフォルトで多くの添付ファイルの種類をブロックします。以下を参照してください。 http://office.microsoft.com/en-us/outlook-help/blocked-attachments-in-outlook-HA001229952.aspx.

b. これらの種類の添付ファイルを送信する必要のあるエンドユーザーは、受取人がこれらの添付ファイルを遠隔でダウンロードするように場所情報を提供するか、ファイルを圧縮（zip 圧縮）してパスワードで保護して送信することによって送信することができます。ISP やメールボックスプロバイダーによっては、この添付ファイルをブロックする場合もあります。

3. Web トラフィックフィルタリング

フィッシングメッセージは多くの場合、ユーザーの認証情報を収集するフィッシングウェブサイトへのリンクを１つ以上含んでいます。フィッシング攻撃を無効にする一つの方法は、フィッシングウェブサイトへのアクセスを遮断することです。既知のフィッシング URL へのアクセスを制限したいと考えている組織に対して、フィッシング URL の一覧を無料または有料で提供しようとする取り組みがいくつか実施されています。

最近のウェブブラウザは、訪問したウェブサイトの信頼性や詐欺行為についてユーザーを教育し、ユーザーがフィッシングメールに含まれるリンクをクリックしても、フィッシングの犠牲になることを食い止めることができます。これらのブラウザは、ウェブページの内容だけでなくリンクも検査し、訪問したウェブサイトの安全性について判定します。最近のブラウザはすべて、正規のウェブサイトを認証して、ユーザーのウェブエクスペリエンスの安全性に関してユーザーに自信を植えつけます。

推奨

1. 可能であれば、ISP やメールボックスプロバイダーは、ファイアウォールや Web フィルタリング製品を利用して確認したフィッシングサイトを一時的にブロックするべきです。

2. ISP やメールボックスプロバイダーは、最新版のウェブブラウザをダウンロードするようにユーザーを働きかけるべきです。

4. アウトバウンド保護

フィッシング詐欺師は、多くの場合、感染しているサーバーの所有者には無断でそのサーバーから、あるいは周囲のネットワークから攻撃を開始します。フィッシング詐欺師は、フィッシング詐欺師自身が利用するサーバーから感染したアカウントを経由してフィッシングメールを直接生成するか、メールサーバー、あるいはメールサーバーでないマシンを経由して生成する場合もあります。いずれにしても、無防備なキャリアは悪意のあるトラフィックを送信してしまいます。多くの場合、これらの無防備なキャリアは、ISP に接続するエンドユーザーマシンとなります。その結果、フィッシング詐欺師は多くの場合、ISP インフラを利用して、フィッシングメールを送出します。

状況によっては、フィッシング対策フィルターを利用して、ISP の機能の範囲内でアウトバウンドフィッシングの攻撃をフィルターすることができます。一部の M³AAWG メンバーは、「アウトバウンドモード」でメンバーのフィルタリングソリューションを利用して、フィッシングメッセージが ISP 網から発信されるのを食い止めるのに大きな成功を収めたと報告をしています。アウトバウンドフィルターの別の利点は、フィッシングウェブページの場所に関するレポートを ISP に提供できるかもしれないということです。フィッシングウェブページが ISP のインフラ内に設置されている場合、ISP は、ページの削除や、ページへのアクセス制限を決めることができます。

推奨

1. ISP は、自身のネットワークからフィッシングメッセージが送信されないようにするアウトバウンドコンテンツフィルターを検討するべきです。インバウンドフィルタを検討する場合、ソリューションのアウトバウンド機能を評価するべきです。

5. フィッシング関連のカスタマサポートコール

フィッシングの問題によって、サポートコールが発生するのは避けられません。効率的なカスタマーサポートのプロセスおよびツールにより、貴重な時間を節約することができます。

推奨

1. フィッシングとスパムは同義ではないことを思い出してください。サポート担当者が、この２つの違いを理解するようトレーニングしましょう。この違いには、419 詐欺（前金詐欺）や「友人が外国で困っている」（寸借詐欺）などの複数の種類の詐欺が含まれます。

2. ユーザーが個人情報を要求する不審な電子メールを報告してきた場合、ISP やメールボックスプロバイダーは、フィッシング攻撃の危険性をユーザーに通知し、オンラインで個人情報を提供しないよう警告するべきです。さらに、フィルターを更新するのに利用できるように、ISP やメールボックスプロバイダーにメールの複製を送付するようユーザーに助言するべきです。

3. ユーザーが詐欺にあったと確信している場合、米国連邦取引委員会（FTC）などの適切な詐欺対策組織に正式に苦情を訴えるようユーザーを説得するべきです。APWG は詐欺対策組織の一覧を http://docs.apwg.org/resources.html#antifraud で管理しています。

4. フィッシングの疑いのあるメールやサイトが、ISP から送信されたか、ISP でホスティングしている場合には、素早く修正するためにカスタマーサポートプロセスを確立するべきです。

5. また、カスタマーサポートは、フィッシングなどの脅威の本質やその影響の範囲を把握でき、ISP やメールボックスプロバイダーがユーザーを保護するために実施している対策について解説している消費者教育リソースにユーザーを誘導するべきです。

6. カスタマーサポートは、同じパスワードを再使用するアカウントを含め、ユーザーが漏らしたパスワードを変更するようユーザーに指示するべきです。また、詐欺課金について金融口座を確認するようにユーザーに指示するべきです。

6. ISP からフィッシング対象への通信

可能であれば、ISP やメールボックスプロバイダーは、ある機関になりすましたフィッシングメッセージを受信した場合、その標的となっている機関に対してフィッシング攻撃の情報を早く伝えるべきです。

推奨

1. ISP やメールボックスプロバイダーは、標的となっている機関に対して、www.antiphishing.org サイトの APWG や別の同様の地域団体を通じて、フィッシング攻撃の情報を伝えるべきです。

2. ISP やメールボックスプロバイダーは、メッセージが DMARC に失敗した場合、DNS レコードに指定された報告メカニズムに対して、DMARC の集約レポートおよび個別分析レポートを送信するべきです。

3. ISP やメールボックスプロバイダーは、他の ISP のユーザーが、メッセージがスパムやフィッシングであると報告してきた場合、この申し出を受け取るフィードバックループを提供し、これらのフィードバックループを利用して、悪意のあるユーザーを無効にすべきです。

7. ユーザー教育

一般ユーザーが、フィッシングメッセージを検出することは困難です。メールボックスプロバイダー、特に保護すべき価値のある情報を所有する大きな組織などは、フィッシング対策トレーニングに投資するべきです。貴殿のユーザーは、貴殿のポリシーを理解しているべきであり、そのポリシーは明確かつ簡単に見つけることができなければなりません。

推奨

1. ISP は、ユーザー向けにフィッシング対策教育を表示するウェブページを立ち上げるか、別の組織のフィッシング対策ページ[4]にリンクを張るべきです。理想を言えば、ユーザーが既知のフィッシングサイトをクリックした場合、フィッシング対策ページにリダイレクトするべきです。

2. 大きな組織は、エンドユーザーに対してフィッシング対策トレーニングを定期的に実施すべきです。トレーニングは、組織内で開発したものでも、フィッシング対策教育企業が提供するサービスでも構いません。

8. 結論

フィッシングは、対抗することが難しい問題ですが、本文書に記載した M³AAWG が推奨する実装を行うことにより、ISP や他のメールボックスプロバイダーは、ユーザーがフィッシングの犠牲になる可能性を減らすことができます。

[4] 教育ページの一覧に関しては、http://apwg.org/resources/Educate-Your-Customers/を参照してください。

この文書はインターネット協会（Internet Association Japan）によって産業界への貢献を目的として翻訳されたものです。
http://www.iajapan.org/