2022 年 4 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

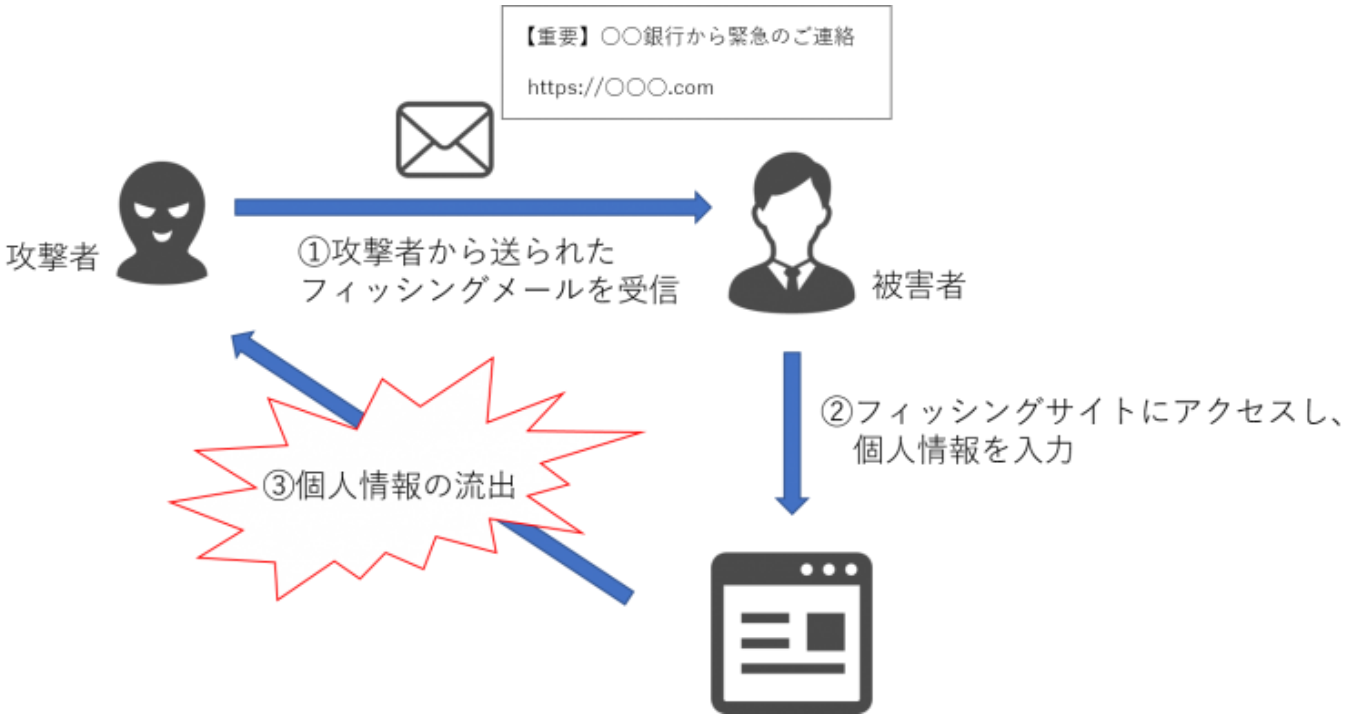
注意喚起：自動退会処理を騙るフィッシングとその対策について

1. 概要

2022 年 3 月、フィッシング対策協議会から自動退会処理を騙るフィッシングが増加しているとして、注意が呼びかけられました。今回はこの自動退会処理を騙るフィッシングの手口と、被害に遭わないための対策についてご紹介いたします。

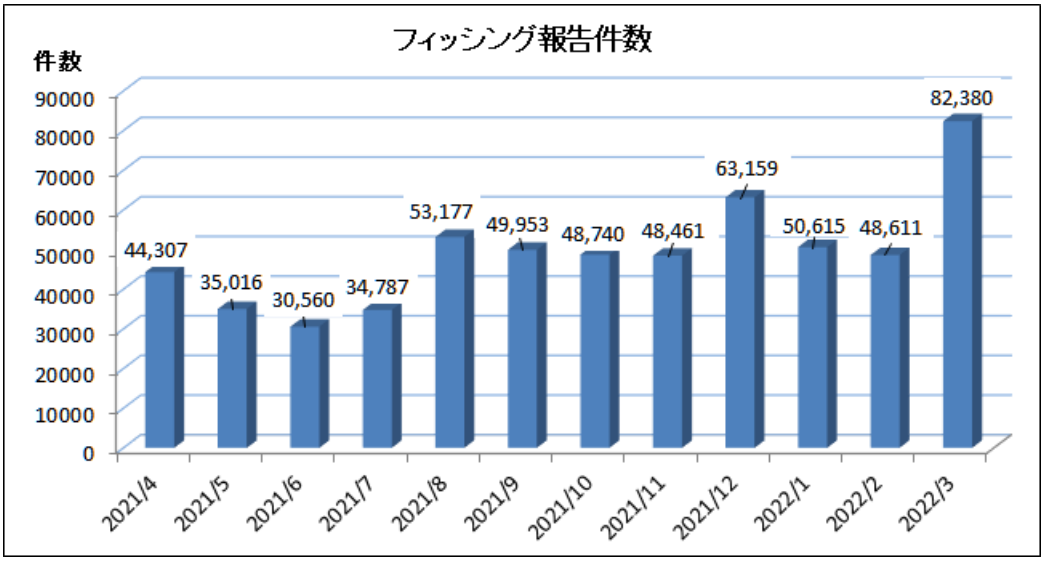
2. フィッシングとは

フィッシングとは、金融機関や有名企業を騙ったメール（フィッシングメール）などから、攻撃者が用意した本物そっくりの WEB サイト（フィッシングサイト）へと誘導し、そこでクレジット番号やパスワードを入力させ、個人情報を奪うことを目的とした詐欺行為です。



【図 1】フィッシングの流れ

フィッシングの報告件数は増加傾向にあり、中でも 2022 年 3 月の報告件数は顕著に多くなっています。フィッシングは今後さらに拡大し、気を付けるべきセキュリティインシデントの 1 つであると言えるでしょう。



【図 2】フィッシングの報告件数

（出典：フィッシング対策協議会 HP「2022/03 フィッシング報告状況」）

3. 自動退会処理を騙るフィッシング手口とその巧妙化の特徴

2022 年 3 月から増加傾向にある自動退会処理を騙るフィッシングでは、フィッシングメールに「【重要】サービスの自動退会処理について」のような件名が記載されており、メール本文では「ログインが確認できない場合は自動的に退会処理を実行する」というような内容とともにフィッシングサイトへのリンクが記載されています。退会を望んでいない利用者にとっては、放置しておくと強制的に退会処理が実行されてしまうため、メールに記載された手続きを緊急で対応する必要があるように感じられます。

このような手口は、従来よりもさらに緊急性を強調することで利用者を焦らせて冷静に思考する時間を奪い、直ちにフィッシングサイトへ誘導するように巧妙化したものだと言えます。

4. 対策

自動退会処理を騙るフィッシングにおいても、従来の対策と同様、以下が有効です。

・不審な SMS やメールは開封しない

・メッセージの内容や送信元をよく確認し、メッセージに記載されている URL に安易にアクセスしない

・正しい Web サイトの URL をブックマーク登録しておき、ブックマークからアクセスするようにする

・表示された Web サイトが正しいかどうか、必ずアドレスバーの URL を確認する

・普段と異なるタイミングで二要素認証や決済情報、ログイン情報の入力を求められた場合、その Web サイトの URL を再確認する

・アンチウイルスソフトを使用し、パターンファイルを最新にする

また、自動退会機能があるサイトでは、焦らずに一旦無視してしまうことも有効な対策となります。自動退会によるデメリットは「もう一度登録する手間」だけである場合が多いためです。

5. 参考

フィッシング対策協議会

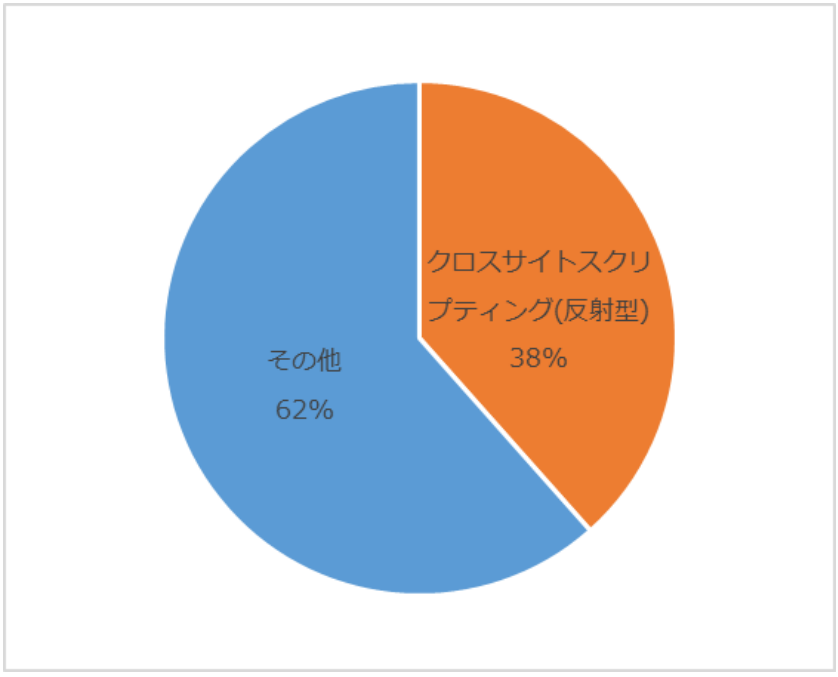
https://www.antiphishing.jp/report/monthly/202203.html

6. e-Gate の脆弱性診断サービスについて

今回ご紹介した自動退会処理を騙るフィッシングは、利用者を焦らせて偽サイトへ誘導するものでしたが、利用者がアクセスしたサイトが正しいサイトだったとしても、そのサイトに以下のような脆弱性がある場合、フィッシングの被害が発生する可能性があります。

・クロスサイトスクリプティング(反射型)
・クロスサイトスクリプティング(格納型)
・クロスサイトスクリプティング(DOM 型)
・オープンリダイレクト

上記のうち、クロスサイトスクリプティング(反射型)は、当社診断案件の 38%で検出されています。



【図 3】2018 年 3 月～2022 年 3 月に実施した Web アプリケーション診断全案件のうち
クロスサイトスクリプティング(反射型)が検出された案件の割合

上記検出割合から推測すると、正規サイトがフィッシングの共犯となってしまう可能性は少なくないと当社では考えます。

e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp