2020 年 10 月 24 日

サービス＆セキュリティ株式会社 e-Gate センター

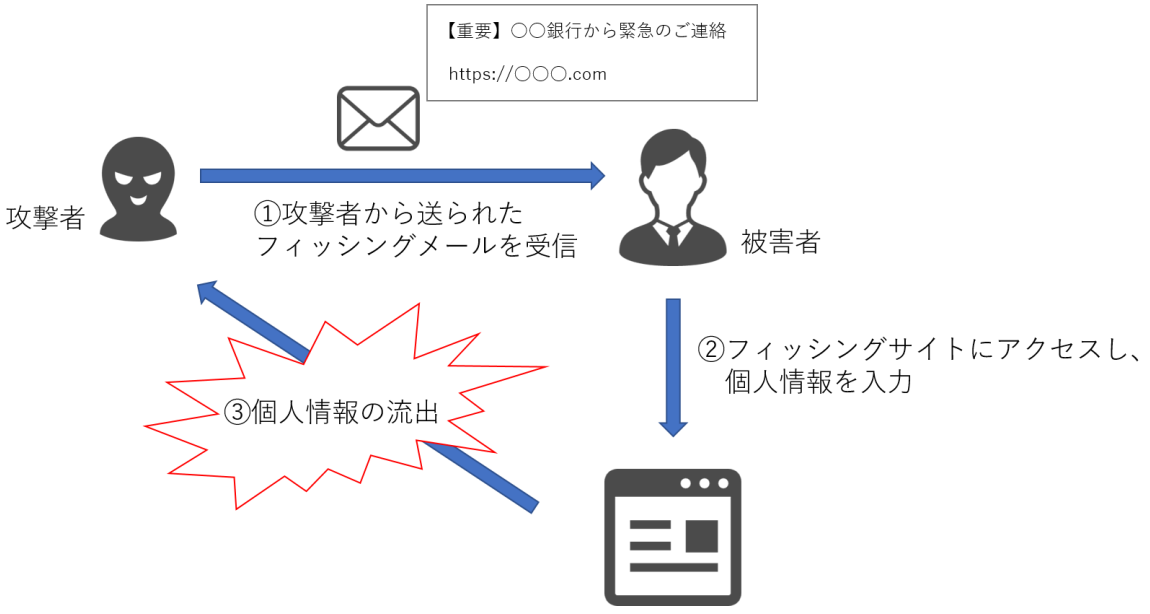
フィッシング件数の急増について

1. 概要

フィッシングは金融機関や有名企業をかたって個人情報を奪う攻撃です。フィッシングの報告件数は増加し続けています。10 月 2 日にフィッシング対策協議会から公開されたフィッシング報告状況によると、2020 年 9 月のフィッシングの報告件数は前月より増加し、28,757 件となりました。e-Gate センターでもフィッシングの検知が増加しています。今回は最近見られるフィッシングの特徴と、被害にあわないための対策をご紹介します。

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かたったメール（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攻撃です。



【図 1 】フィッシングの流れ

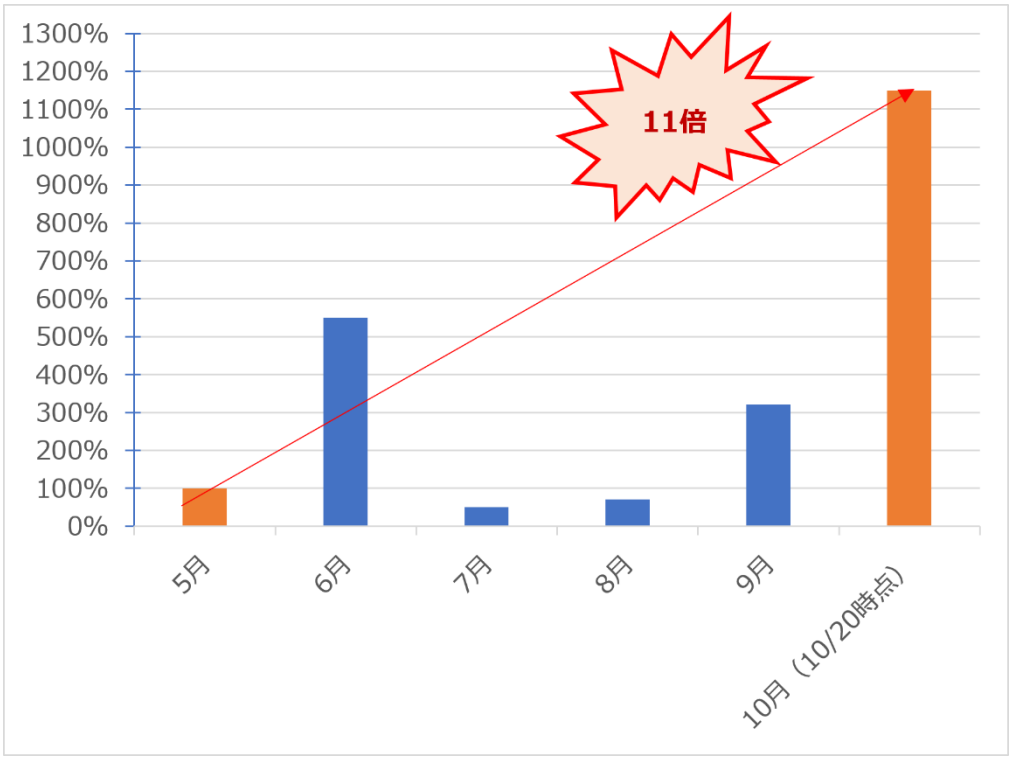
フィッシングの詳細は以下の記事をご参照ください。

『フィッシングの最新情報および対策方法』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9834

3. e-Gate センターで検知したフィッシングメール

e-Gate センターでもフィッシングメールの受信を検知しています。今年 6 月に検知数が急増し、その後は一度減少しました。しかし 9 月には再び急増し、5 月と比べて 3 倍以上となりました。10 月に入ってからもフィッシングメールの検知数は増加しており、10 月 20 日までで 5 月全体の 11 倍を超えています。



【図 2】e-Gate センターでのフィッシングメール検知件数

これらのフィッシングメールには、大手ショッピングサイトや国内大手のカード会社を装ったフィッシングサイトへのリンクが貼られています。本物のサイトへのリンクのように見せかけるために、リンクの URL にはそれらの有名サイトやカード会社名の単語が含まれています。

4. フィッシングの発生状況

国内のフィッシング件数は増加傾向にあります。フィッシング対策協議会の「2020/09 フィッシング報告状況」の情報によると、9 月のフィッシング報告件数は前月より 7,761 件増加し、28,575 件となりました。Amazon、楽天、三井住友カード、LINE をかたるフィッシングメールが全体の約 93.2%を占めました。

トレンドマイクロの「2020 年上半期セキュリティラウンドアップ」の情報によると、フィッシングサイトに誘導された人は 1 月～6 月で約 297 万人となり過去最大でした。偽装するサービスとして楽天市場、Amazon プライム、ヨドバシ・ドット・コムといった EC サイトが顕著に見られます。

フィッシング件数が増加した背景として、新型コロナウイルス感染症拡大による新しい生活様式が普及し、PC やスマートフォンを利用する場面が増えたことが考えられます。

新型コロナウイルスに便乗したフィッシングの詳細は、以下の記事をご参照ください。
『新型コロナウイルスに便乗したフィッシング』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10717

5. 対策

フィッシングには以下の対策が有効です。
・メールから直接 WEB サイトにアクセスしないようにする
・「重要」「緊急」などの急かす文言に焦らない
・電子署名の確認
・セキュリティソフトの有効化、最新版への継続的なアップデート
・同じパスワードを別のサービスで使い回さない
・セキュリティ機器の導入、監視

ネットワークセキュリティ機器導入後は、それらの機器の適切な運用が不可欠です。サイバー攻撃は 24 時間 365 日いつでも行われる可能性があることからリアルタイム監視が欠かせません。さらに、ネットワークセキュリティ機器が出力するログを分析し、危険性を判断する必要があります。

しかし、社内だけでこれらの運用を行うには多くのコストがかかってしまいます。そこで、外部の SOC（セキュリティオペレーションセンター）にネットワーク機器の運用をアウトソーシングするという手段がございます。

6. 参考情報

フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202009.html
トレンドマイクロ
https://www.fnn.jp/articles/-/86261

7. e-Gate のセキュリティ運用監視サービスについて

e-Gate のセキュリティ運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ運用監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、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。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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/

«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