ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●9月のフィッシング報告件数、3万件目前に…対策協議会発表

https://www.antiphishing.jp/report/monthly/202009.html
https://www.antiphishing.jp/news/alert/japanpost_20200928.html

このニュースをザックリ言うと・・・

- 10月2日(日本時間)、フィッシング対策協議会より、9月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 9月度の報告件数は28,575件で、8月度(https://www.antiphishing.jp/report/monthly/202008.html)の20,814件より7,761件の増加、またフィッシングサイトのURL件数も6,686件で、8月度の4,953件から1,733件の増加となっています。

- Amazon・楽天・三井住友カード・LINEを騙るフィッシングメールの大量配信が報告全体の約93.2%と引き続き9割を占め、その約半数が差出人メールアドレスにおいて正規サービスのドメインを騙る「なりすまし送信」だったとのことです。

- なお同協議会では9月28日にも、日本郵便を騙り、クレジットカード情報を含む個人情報を詐取しようとするフィッシングについて注意喚起を出しています。

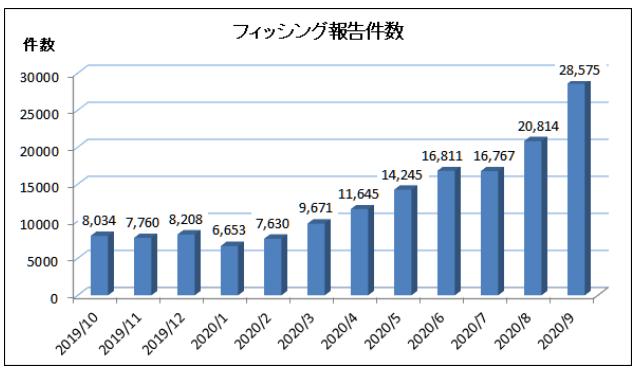
AUS便りからの所感等

- つい先月に2万件を突破したばかりの報告件数ですが増加の勢いは衰えを知らず、10月度においては4万件前後に到達することでしょう。

- 本物と完全に同一なドメイン名を送信元とする「なりすまし送信」メールに対してはSPF・DMARC等の送信ドメイン認証技術によるチェックが有効とされますが、スパムメール業者が微妙に似せたドメイン名を用い、かつSPFを正規に設定してチェックを回避しようとするケースもあり、迷惑メールの文面等のチェックによるフィルタ機能も併せての対策は不可欠です。

- 一方で、月々の報告状況からみられるフィッシングの主な手口は、「大手ネットサービス・クレジットカード・金融機関を騙る」「宅配業者の不在通知を騙るSMSの誘導で不正なアプリをインストールさせる」「スマートフォン等が当選したと誤認させて個人情報等を詐取する」あたりの傾向が数ヶ月続いており、まずはこういった手口の存在を十分に認識し、サービス各社の公式情報等も随時確認の上、確実に対処できるよう行動することが重要です。

フィッシング対策協議会
Council of Anti-Phishing Japan



●東映子会社のECサイトに不正アクセス…カード情報1万件に流出の可能性

https://www.itmedia.co.jp/business/articles/2010/01/news103.html
https://www.toei-video.co.jp/?p=38885

このニュースをザックリ言うと・・・

- 9月30日(日本時間)、東映グループ会社の東映ビデオ社より、同社ECサイト「東映ビデオオンラインショップ」が不正アクセス被害を受け、クレジットカード情報などが流出した可能性があると発表されました。

- 被害を受けたのは2019年5月27日～2020年5月11日に同サイトで決済に用いられたクレジットカード情報(名義人・番号・有効期限およびセキュリティコード(CVV))計10,395件(10,021人分)とされています。

- 5月11日に決済代行会社からカード情報流出の可能性の指摘を受けてサイトを停止しており、同社では不正アクセスを受けたシステムを破棄して新しいシステムを構築中としています。

AUS便りからの所感

- クレジットカードの業界団体である日本クレジット協会が策定した「セキュリティガイドライン(https://www.j-credit.or.jp/security/document/)」により、ECサイト上でカード情報を保持しない(非保持化)が求められるようになったことから、攻撃者の手口は、サイトの脆弱性を突いてフォームの改ざんを行うことにより、セキュリティコードを含めた入力内容を外部に送信させる等に移行しつつあります。

- 今回については「システムの一部の脆弱性をついたことによる不正アクセスを示す形跡が認められたものの、クレジットカード情報の不正取得に繋がる改ざんや不正プログラム等は発見されませんでした」と発表され、手口の詳細が明らかになっておらず、カード情報の非保持化がされていなかった可能性も、あるいは非保持化がなされていたがフォームの改ざんが行われた(その痕跡が消去されていた)可能性も考えられます。

- フォームの改ざん等を利用者側のアンチウイルス等で検知することは困難な場合も考えられるため、サービス提供者側においてはWebサイトの脆弱性を確実に塞いで攻撃者の侵入を防止することが重要ですし、加えて万が一不正プログラムの設置やフォーム改ざん等が行われた場合でも、外部への不審な通信を遮断するための出口対策を行うことが、効果的な情報の防衛となり得るでしょう。

●特に若年層が利便性を重視、パスワードの安全な文字数は「8文字」が各年代で最多…認証方法に関するアンケート

https://www.antiphishing.jp/news/info/20200909.html

このニュースをザックリ言うと・・・

- 9月9日(日本時間)、フィッシング対策協議会より、インターネットサービスへログインするための利用者認証に関するアンケート(2月28日～3月2日調査、回答者562人)の結果が発表されました。

- 年代毎の回答の傾向から、特に若年層において安全性より利便性を重視する傾向がみられたとし、例えば「ブラウザーにパスワードを記憶させられる場合に記憶させるか」という問に対し、特に18～29歳においては46.8%が「記憶させる」、また「利用するサービスによって変える」を含めると84.6%と、世代毎で最も高い割合を示しています。

- またパスワードの文字列について「安全と思う文字数」についての問では、各世代とも「8文字」が最も多く、また60代以上を除く世代で8文字以下の割合が過半数を占めていました。

AUS便りからの所感

- 8文字のパスワードで安全かどうかは、使用している(あるいは使用できる)文字種次第と言えますが、ネットサービス側でパスワードを最大8文字としている(さらには記号が使えない等の制限もある)ケースは依然多く、そういった状況に引っ張られて「8文字で安全」と回答している場合もあるものと推測します。

- また、いずれも比較的歴史の長い顔認証と指紋認証について、前者は18.9%が「嫌い」とする一方、後者では11.9%と反応が分かれている等、様々な傾向がみてとれます。

- アンケート結果では「利便性よりも安全性を求めている」とした事業者側への別のアンケートとの差を挙げ、「これらの差を埋めるためにも安全確保に工夫が必要と思われます」と締めており、調査の半年後に話題となった銀行口座からの不正出金問題(AUS便り 2020/09/28号参照)等とも鑑み、必要最小限で効果的に第三者の不正ログイン等を食い止める認証が提供され、ユーザーに受け入れられることを期待したいものです。