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。

●日本クレジットカード協会・フィッシング対策協議会等11団体「フィッシング啓発キャンペーン」

https://internet.watch.impress.co.jp/docs/news/1640299.html
https://www.value-press.com/pressrelease/346938
https://www.jcca-office.gr.jp/feature/phishing/

このニュースをザックリ言うと･･･

- 11月18日(日本時間)、日本クレジットカード協会（JCCA）他官民11団体による「フィッシング啓発キャンペーン」が開始されました。

- 同協会の他、警察庁・消費者庁・総務省・経済産業省・国民生活センター・フィッシング対策協議会・日本サイバー犯罪対策センター・日本データ通信協会迷惑メール相談センターおよび全国大学生活協同組合連合会の参加によるもので、12月17日まで実施されます。

- キャンペーンメッセージとして「①フィッシングにご注意を」「②メールのリンク先から安易にクレジットカード番号を入力してはいけません」「③フィッシングサイトでクレジットカード番号を入力してしまったら、カード会社に連絡を」と呼び掛けています。

AUS便りからの所感等

- 2023年のクレジットカード不正利用被害額は約541億円(前年比 +104億円)で過去最悪を更新、うち約93%がカード情報の盗用による非対面取引によるものとされており、また同キャンペーンにも参加しているフィッシング対策協議会に寄せられている月々のフィッシング報告件数は、今年5月以降14万件を超える水準を維持し、特に7月度は過去最高の177,875件、8月度はこれに次ぐ166,566件を記録しています。

- キャンペーンでは、「カード利用に制限がかかった」と偽ってカード番号を詐取しようとするフィッシングの一例を挙げており、ユーザーにおいて本物のサービスからのメッセージか確認する方法としては、ここで推奨されている公式アプリの使用の他、Webサービスやカード会社のサイトへ予め登録したブックマークからアクセスすることが十分効果的です。

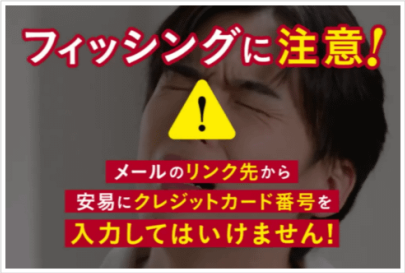
- サービス提供者側においても、通知を行う際のメールアドレスの申告(特にWebサイトや自組織と異なるドメイン名を使用する場合)や、「こういった件名でメールを送ることはない」といった情報を開示し、ユーザーがフィッシングを回避するための情報をまとめることが望まれます。

- そしてこのようなサービスを提供しない企業・組織でも、自組織からの本物のメールであることを示す機構としてのSPF・DKIM・DMARC等の導入は今や取引先等を保護する意味で必須であることに留意してください。

Impress Watch

JCCAら官民11団体がフィッシング啓発キャンペーンを開始、注意喚起の動画も公開

大東 奈央　2024年11月18日 15:10



日本クレジットカード協会（JCCA）ほか官民11団体は11月18日、消費者に対してフィッシングの注意喚起を行う「フィッシング啓発キャンペーン」を開始した。

フィッシングの手口は日々巧妙化しており、2023年のクレジットカード不正利用被害額は約541億円（前年比＋104億円）と過去最悪を更新しているという。特に、番号盗用による非対面取引での不正利用被害額は全体の約93%を占めているという。

●WordPressプラグイン「Really Simple Security」の「2要素認証」機能に重大な脆弱性、9.1.2へ更新されたか確認を

https://www.bleepingcomputer.com/news/security/security-plugin-flaw-in-millions-of-wordpress-sites-gi admin-access/
https://ja.wordpress.org/plugins/really-simple-ssl/

このニュースをザックリ言うと・・・

- 11月17日(現地時間)、米IT系メディアBleeping Computerより、WordPress向けプラグイン「Really Simple Security」に危険度の高い脆弱性「CVE-2024-10924」が存在していると発表されました。
- 脆弱性は同プラグイン(および「Really Simple Security Pro」「Really Simple Security Pro multisite」)のバージョン9.0.0～9.1.1.1に存在し、「2要素認証」機能を有効にしている場合、脆弱性の悪用により、任意のWordPressアカウントへのログインが可能とされています。
- 既に脆弱性を修正したバージョン9.1.2がリリースされており、対象バージョンに対しては自動的にアップデートを行う措置がとられたとのことです。

AUS便りからの所感

- 「Really Simple Security」は、元々はWordPressサイト全体をHTTPS化する「Really Simple SSL」だったもので、9月の9.0.0リリースより現在の名前になるとともに、2要素認証をはじめいくつかのセキュリティ機能を提供するようになりました。
- WordPressには、自動更新を無効にしているプラグインについても、緊急のセキュリティアップデートについて強制的に適用させる機能があり、過去にもいくつかのプラグインで実行されています。
- WordPressでは本体・各種プラグインとも頻繁にセキュリティアップデートのリリースがあるため、使用しているプラグインについてセキュリティ情報を収集、特に意図的に自動更新していないものがあれば定期的に管理画面で各種アップデートの有無を確認すること、また今回のような強制アップデートがあった場合についても確実に安全なバージョンとなっているか確認することが重要です。
- またセキュリティ機能を提供するプラグインも今回問題となったReally Simple Securityを含め多く提供されており、厳正な選定の上でいずれかを導入することを推奨致します。


BLEEPINGCOMPUTER

Security plugin flaw in millions of WordPress sites gives admin access

By Bill Toulas — November 17, 2024 10:19 AM

A critical authentication bypass vulnerability has been discovered impacting the WordPress plugin 'Really Simple Security' (formerly 'Really Simple SSL'), including both free and Pro versions.

Really Simple Security is a security plugin for the WordPress platform, offering SSL configuration, login protection, a two-factor authentication layer, and real-time vulnerability detection. Its free version alone is used in over four million websites.

●「たよれーる Microsoft 365」で管理者アカウントへの不正ログイン発生、多要素認証の設定呼び掛け

https://www.itmedia.co.jp/news/articles/2411/19/news125.html
https://mypage.otsuka-shokai.co.jp/news/detail?urlparam1=yrGys1alLsgWJKexRUWirg%3D%3D

このニュースをザックリ言うと・・・

- 11月15日(日本時間)、大塚商会より、同社が運営する「たよれーる Microsoft 365」において管理者アカウントに対するセキュリティ侵害が発生しているとして注意喚起が出されています。
- Microsoft 365内のデータ削除や漏洩、テナント内のアカウント削除、および迷惑メール送信等サイバー攻撃の踏み台にされる恐れがあるとしています。
- 本件は同社におけるセキュリティインシデントではなく、海外IPアドレスからの不正ログインによるものとされ、同社では管理者権限アカウントにおける多要素認証の設定を呼び掛けています。

AUS便りからの所感

- 十分に強力でないパスワードを設定していた管理者アカウントが不正ログインの被害を受けたとみられ、「アカウント侵害の方法によっては、強固なパスワードへの再設定だけでは対策不十分の可能性」があるとのことです。
- 特に組織内の多数のユーザーを管理するようなサービスの管理アカウントへのログインにおいて、近年多要素認証の設定を必須とするケースが増えています。
- 管理者のみならず個々のアカウントへの不正ログインでも、組織内外に与える悪影響は多々ありますので、推測されにくい固有のパスワードを設定するとともに、提供されているアカウント保護機構、不正ログインを阻止する機構を有効にすることを心掛けましょう。


ITmedia NEWS

「たよれーる Microsoft 365」一部の管理者アカウントが侵害　データ削除など被害のおそれ

2024年11月19日 12時33分 公開 [ITmedia]

大塚商会は、同社のサポートとMicrosoft 365を組み合わせた「たよれーる Microsoft 365」の一部のユーザーで、複数の海外アドレスから不正アクセスを受けて管理者アカウントが侵害される事象が発生しているとし、ユーザーに注意を呼び掛けている。

「強固なパスワードへの再設定だけでは対策不十分の可能性がある」とめ、管理者権限アカウントの多要素認証を設定するよう求めている。またこの問題は、同社のセキュリティインシデントではないとしている。