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。

● Microsoft、Outlook.com等メールサービスにて「大量送信者向け要件」適用…2024年のGMail等に続く

https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlook-s-new-requirements-for-high-volume-senders/4399730
https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about
https://powerdmarc.com/ja/dmarc-outlook-email-authentication/

このニュースをザックリ言うと・・・

- 4月2日(現地時間)、マイクロソフト(以下・MS)より、同社運営のメールサービス(Outlook.com・hotmail.com・live.com)へのメール送信者に対する「メール送信者要件」を5月5日以降に適用することが発表されました。

- 具体的には、当該メールサービスへ1日に5,000通以上のメールを送信するドメイン名に対し、SPF(メール送信に使用するサーバー・IPアドレスの申告)・DKIM(送信元メールサーバーによる署名)・DMARC(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)の設定を必須化するというものです。

- 5月5日以降、要件に準拠しないメールは迷惑メールフォルダーに隔離されるとしており、今後時期は未定ですが、メール自体の受信も拒否されるようになるとのことです。

AUS便りからの所感等

- 同様のガイドラインは2023年10月にGMailや米国のYahooが発表、2024年2月にGMailが適用を開始しており、この時点で多くの組織がSPF・DKIM・DMARCに対応しています。

- Microsoft365との契約等により、MSのメールサービスを利用している企業・組織も多く、GMail同様に顧客ユーザーは確実に利用しているものと考え、一通りの対応は全ての組織においてますます必須となるといえます。

- 現時点でDMARCのポリシー(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)は最低でもp=none(特に指定しない)となっていますが、フィッシングメール等のFrom: でドメイン名の悪用が多く報告されている場合は、p=quarantine(迷惑メールフォルダー等への隔離)ないしp=reject(受信拒否)の設定を早々に検討すべきです。

Microsoft

MICROSOFT DEFENDER FOR OFFICE 365 BLOG　5 MIN READ

Strengthening Email Ecosystem: Outlook's New Requirements for High-Volume Senders

Puneeth MICROSOFT
Apr 03, 2025

This applies to Outlook.com - our consumer service, which is supporting hotmail.com live.com and outlook.com consumer domain addresses.

Introduction

In an era where email remains one of the most widely used tools for personal and business communications, Outlook is stepping up its commitment to protect inboxes and preserve trust in the digital ecosystem. Today, we're announcing new requirements and best practices designed to strengthen email authentication for domains sending more than 5,000 emails per day.

●偽の自動音声「ボイスフィッシング」による不正入金、複数地銀等で被害

https://www.itmedia.co.jp/news/articles/2504/03/news151.html
https://www.musashinobank.co.jp/irinfo/news/pdf/2024/huseisoukinn20250331.pdf
https://www.sankei.com/article/20250406-UZ3MAQYR4JJ7NLUQZ57O2O23BA/

このニュースをザックリ言うと･･･

- 3月31日(日本時間)、埼玉県の地方銀行・武蔵野銀行より、同行を騙る自動音声の偽電話による不正送金(いわゆる「ボイスフィッシング詐欺」)の事案が確認されたとして注意喚起が出されています。

- 同行のインターネットヘルプデスクを名乗り、「口座情報の更新がされていないため、口座を凍結しました」等として、ネットバンキングの契約者情報更新のため暗証番号・パスワードを聞き出した上で、不正送金を行う例が挙げられています。

- 同行では、自動音声による案内や、電話・電子メール・SNS等で契約情報を訊ねることはないとしており、同行を騙る自動音声の電話には決して対応しないよう呼び掛けています。

- 4月6日には産経新聞より、ボイスフィッシング詐欺の事例が昨年秋以降全国で相次ぎ、3月以降も地銀5行(武蔵野銀行含む)・信金1行で判明していると報じられています。

AUS便りからの所感

- 事例が確認された各行では、ネットバンキングでの同行ないし他行への即時振込を一時停止する等の事態となっています。

- 前後して大手ネット証券各社でも、異なる手口でのアカウント情報奪取によるとみられる、株等の不正取引事案が発生しています(AUS便り2025/03/28号参照)。

- 特にネットバンキング・ネット証券のユーザーにおいては、このような実際に用いられている詐欺の手口を常に情報収集して慎重に行動するとともに、ID・パスワードのみでログインないし不正な取引が実行されないよう、パスキー等の追加認証機構の設定も検討してください。

「口座を凍結した」自動音声の偽電話で不正送金させる「ボイスフィッシング」被害

2025年04月03日 13時21分 公開 [ITmedia]

武蔵野銀行は、同行をかたる自動音声の偽電話などでネットバンキングのパスワードなどを聞き出し、不正送金させられる「ボイスフィッシング」の被害を、法人向けネットバンキングで確認したと発表した。

このため3月31日から、インターネットバンキングによる他行あて即時振込を停止。当日振込が必要な場合は店頭窓口で受け付けるという。

●Microsoft・Adobe・Zoom等月例のセキュリティアップデートリリース

https://forest.watch.impress.co.jp/docs/news/2005212.html
https://msrc.microsoft.com/blog/2025/04/202504-security-update/
https://forest.watch.impress.co.jp/docs/news/2005223.html
https://forest.watch.impress.co.jp/docs/news/2005405.html

このニュースをザックリ言うと･･･

- 4月9日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5055518(ビルド 19045.5737)、11 23H2 KB5055528(ビルド 22631.5189)および11 24H2 KB5055523(ビルド 26100.3775)等となります。

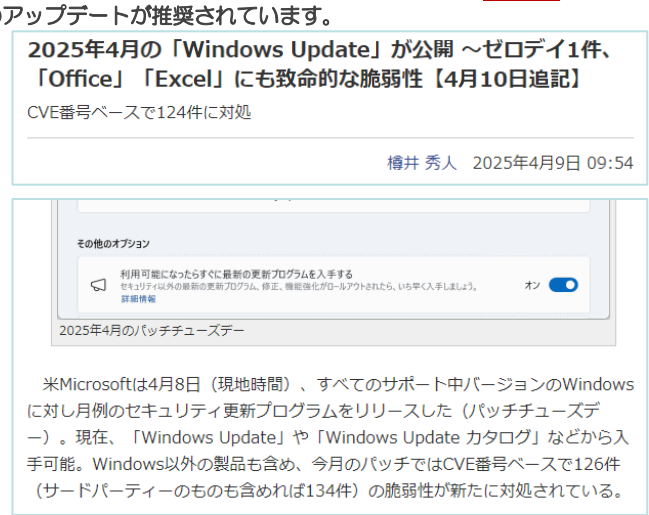
- 同日にはAdobe社より「Photoshop」等12製品について脆弱性とセキュリティアップデートがリリース、またZoom社からも「Zoom Workplace」で2件の脆弱性が報告されており、4月1日リリースの6.4.3へのアップデートが推奨されています。

AUS便りからの所感

- MSの月例アップデートでは1件の脆弱性が既に悪用を確認、またOffice・リモートデスクトップサービス等11件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。

- Zoom Workplace自体のアップデートは不定期にリリースされ、自動更新を有効に設定していても起動していない間にはアップデートが適用されず、特に使用頻度が少ない場合等に「会議の直前でアップデートが発生する」というトラブルも散見され、可能な限りトラブルを回避するよう随時クライアントを起動し、明示的に「アップデートを確認」を開くことを心掛ける必要があるでしょう。

- 今回の「パッチチューズデー(米国時間での第2火曜日にあたる)」の他、Oracle社からは4月16日にJava等に対する四半期に一度のセキュリティアップデートがリリースされる等、各種ソフトウェアベンダーが定期的に行うアップデートについて、特にシステム管理者においては忘れず意識し、OS・機器のファームウェアから各種アプリケーションに至るまで計画的に更新、加えてアンチウイルス・UTM等による多重防御策により、常に脆弱性への攻撃に備えるよう心掛けてください。



2025年4月の「Windows Update」が公開 ～ゼロデイ1件、「Office」「Excel」にも致命的な脆弱性【4月10日追記】

CVE番号ベースで124件に対処

樽井 秀人　2025年4月9日 09:54

2025年4月のパッチチューズデー

米Microsoftは4月8日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで126件（サードパーティーのものも含めれば134件）の脆弱性が新たに対処されている。