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。

●Chrome拡張「uBlock Origin」の偽物が公式拡張ストアに…現在も削除されず

https://www.reddit.com/r/uBlockOrigin/comments/1mcqy5h/has_anyone_seen_this_version/
https://ublockorigin.com/

このニュースをザックリ言うと・・・

- 7月29日(現地時間)、掲示板サイトRedditにおいて、Chromeブラウザー向け拡張機能「uBlock Origin」の偽物が公式拡張ストアに存在するとして注意喚起が出されています。

- 本物のuBlock Origin(開発者: gorhill)は拡張機能の新しい仕様「Manifest v3」に対応していないため、公式拡張ストアで「uBlock Origin」と検索しても本物は表示されなくなっており、また8月4日現在でも偽物(開発者: bigjpgai)の方が削除されずに表示される状態となっています。

- 偽物について解析を行った者によれば、現時点で不審なコードやファイルが含まれている様子はないものの、後日のアップデートにより悪意のあるコードが追加される可能性もあると指摘されています。

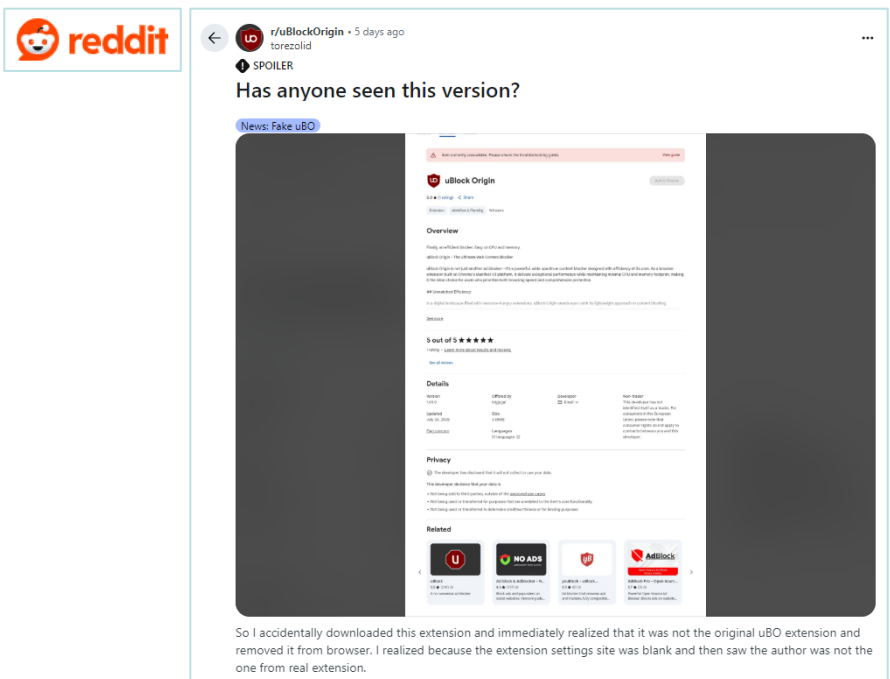
AUS便りからの所感等

- Chrome 134以降、Manifest v3に対応していない拡張は通常の手順で公式拡張ストアからのインストール・有効化ができなくなっており、引き続き同じ拡張を使いたいユーザーを騙そうと「Manifest v3対応バージョン」を騙る偽の拡張をアップロードするケースが散見されています。

- 拡張機能管理画面において「デベロッパーモード」を有効にすることにより、使用している拡張機能のIDが確認できますが、IDが「cjpalhdlnbpafiamejdnhcphjbkeiagm」でないuBlock Originは偽物のため、速やかに削除してください。

- uBlock Originと同じ開発者によってManifest v3に準拠した「uBlock Origin Lite」の開発が進んでおり(「uBlock Origin」で検索した場合にもこちらが表示されます)、現時点でChromeインストール後に広告ブロッカーを導入する場合はこれをインストールするのが無難でしょう。

- ブラウザーにインストールした拡張機能がソフトウェア上で様々な機能の使用を許可されることに留意すること、ストアで検索して出てきたものを安易にインストールせず、SNSでの報告等を十分に確認し、必要最低限の拡張機能のみインストール・有効化すること、また後からでも不要な拡張機能の棚卸し、万が一身に覚えのない拡張機能が入っていた場合のアンインストール等を行うことは、今回に限らずあらゆる拡張機能の利用時に重要です。



●証券会社からの対策喚起を騙るフィッシング…ワンタイムパスワードも奪取

https://ascii.jp/elem/000/004/306/4306805/
https://www.antiphishing.jp/news/alert/iwaicosmo_20250616.html
https://www.iwaicosmo.net/service/security/crime.html

このニュースをザックリ言うと･･･

- 7月23日(日本時間)、「ascii.jp」において、証券会社からのセキュリティに関する注意喚起を騙るフィッシングの事例が取り上げられています。

- 事例は、6月16日にフィッシング対策協議会から発表があった、岩井コスモ証券を騙るもので、「セキュリティシステム改定のお知らせ」「セキュリティアップデートのお知らせ」「セキュリティプロトコル更新のお知らせ」「システムセキュリティ強化のお知らせ」等と称して、同証券のWebサービスのアカウント情報を詐取するページへ誘導するものとされています。

- また文面においても「最近フィッシング詐欺が増加している状況を踏まえ…」等、今年春に多発したネット証券各社の不正取引事案を受けての対策実施を装う文面になっているとしています。

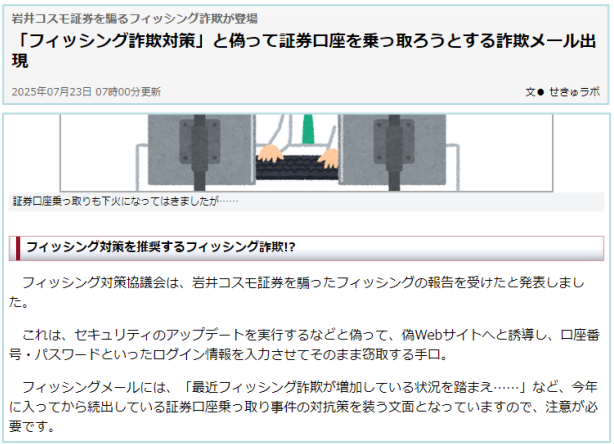
- 記事では同証券の本物のWebサイトにある注意喚起ページにもリンクしている一方、推奨されているセキュリティ対策の一つであるワンタイムパスワードもいわゆる「リアルタイムフィッシング」によって破られる可能性があり、万能ではないとしています。

AUS便りからの所感

- リアルタイムフィッシングは、フィッシングサイトでアカウント情報のみならずワンタイムパスワードも要求し、入力されたそれぞれの情報を即座に本物のログインページに中継する手口をとることにより、不正ログインを成立させるもので、今年春の不正取引事案でも多用されたとみられます。

- 記事では、既に日本証券業協会において「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正が進められていることを取り上げており、7月15日にはフィッシングに耐性のあるパスキー等による多要素認証を必須とする改正案が発表されています(https://xtech.nikkei.com/atcl/nxt/column/18/00001/10906/)。

- ネット証券各社で5月頃に実施された対策について、今後上記ガイドラインに基づいた変更等、数ヶ月での変動が発生する可能性があり、各社からの正規の情報に注視する意味でも、予め登録したブックマークや公式アプリから本物のサイトにアクセスすることでフィッシングを回避することを心掛けましょう。


岩井コスモ証券を騙るフィッシング詐欺が登場
「フィッシング詐欺対策」と偽って証券口座を乗っ取ろうとする詐欺メール出現
2025年07月23日 07時00分更新
文● せきゅラボ
証券口座乗っ取りも下火になってはきましたが……
フィッシング対策を推奨するフィッシング詐欺!?
フィッシング対策協議会は、岩井コスモ証券を騙ったフィッシングの報告を受けたと発表しました。
これは、セキュリティのアップデートを実行するなどと偽って、偽Webサイトへと誘導し、口座番号・パスワードといったログイン情報を入力させてそのまま窃取する手口。
フィッシングメールには、「最近フィッシング詐欺が増加している状況を踏まえ……」など、今年に入ってから続出している証券口座乗っ取り事件の対抗策を装う文面となっていますので、注意が必要です。

●夏季休暇における情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20250801.html
https://www.ipa.go.jp/security/anshin/measures/vacation.html
https://www.ipa.go.jp/security/anshin/measures/everyday.html

このニュースをザックリ言うと･･･

- 企業・組織によっては長期休暇となるお盆の時期を迎えるにあたり、8月1日(日本時間)、IPAより、「夏休みにおける情報セキュリティに関する注意喚起」が発表されました。

- 長期休暇の時期は、システム管理者が長期間不在になる等「いつもとは違う状況」になりがちであり、ウイルス感染・不正アクセス等セキュリティインシデント発生時の対処が遅れたり、思わぬ被害が発生したりして、休暇明けにおける業務継続にも影響が及ぶ可能性があるとしています。

- IPAでは「長期休暇における情報セキュリティ対策」と題した、「企業・組織システムの管理者」「システムの利用者」それぞれを対象とした「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得、また「(SNS等を利用する)個人」としての立場での注意事項についてまとめています。

AUS便りからの所感

- IPAが長期休暇の時期(年末年始・ゴールデンウィーク・夏季休暇等)に発表する内容は、近年は発表毎に新しい内容が追加されることは少なくなっていますが、一方でインターネット境界に接続装置の脆弱性を悪用する「ネットワーク貫通型攻撃」については毎回多数の被害が報告されているとみられ、長めの文面をとって注意喚起が出されています。

- この他、ゴールデンウィークの際(https://www.ipa.go.jp/security/anshin/heads-up/alert20250421.html)は「サポート詐欺」についても注意喚起が出されていました。

- 休暇までに日にちがなく十分な対応が間に合わなかったとしても、お盆明け以降に点検すべきことは多く存在しますし、以後も年末年始・ゴールデンウィーク等に備えて対応しておくべき事柄も変わらず、また長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策」として別途まとまっており、それぞれにおいて準備・点検を行うよう意識していくことが肝要です。


IPA 独立行政法人 情報処理推進機構
2025年度 夏休みにおける情報セキュリティに関する注意喚起
公開日：2025年8月1日
独立行政法人情報処理推進機構
セキュリティセンター
多くの人が夏休みの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。
長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生し、長期休暇後の業務継続に影響が及ぶ可能性があります。
このような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、それぞれの対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。
長期休暇における情報セキュリティ対策
日常における情報セキュリティ対策
注釈：上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。
1. 個人の利用者：個人向けの対策（3）
2. 企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策（2-2.／3.）
3. 企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策（2-1.／2-2.／3.）