― AUS（アルテミス・ユーザ・サポート）便り 2020/10/19号 ―

https://www.artemis-jp.com

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。

●「二回目特別定額給付金の特設サイトを開設しました。」…総務省を騙るフィッシングに注意喚起

https://www.antiphishing.jp/news/alert/kyufukin_20201015.html
https://www.soumu.go.jp/menu_kyotsu/important/kinkyu02_000438.html

このニュースをザックリ言うと･･･

- 10月15日(日本時間)、総務省やフィッシング対策協議会より、同省を騙るフィッシングメールが確認されたとして相次いで注意喚起が出されています。

- 同協議会が挙げているフィッシングメールは、件名が「二回目特別定額給付金の特設サイトを開設しました。」で、「マイナポータル」の「ぴったりサービス」を騙り、各種個人情報・銀行口座および運転免許証などの画像を詐取しようとする偽サイトにリンクされているとのことです。

- また総務省では、フィッシングメールの発信元メールアドレスに「soumu.go.jp(実際の総務省のもの)」が用いられているものの、このようなメール・サイトについて、総務省も含めた行政機関によるものではないとし、決してリンクにアクセスせず、メールを削除するよう呼び掛けています。

AUS便りからの所感等

- 偽サイトは「kyufukin.●●●●.online」「kyufukin.●●●●.best」「kyufukio-soumu-go-jp.●●●●」等のドメイン名が用いられているとのことで、さらに他のドメイン名が用いられる可能性も示唆されています。

- 特別定額給付金は10月19日時点で2回目の給付が決定しておらず、かつ総務省でも「特別定額給付金について、政府からメールなどでお知らせをすることはありません」としていますので、そもそも自身のメールアドレスを提示したわけでもないのに政府機関からメールが来ることについて十分に疑念を持ち、慎重に行動して頂ければ幸いです。

- マルウェア添付メールやフィッシングメールの多くはアンチウイルスやメーラー・ブラウザーのアンチフィッシング機能およびUTMによる受信の遮断等が期待できますが、SMSで送られてくるものを遮断するのは困難とみられ、そういったときにも万が一に騙されてリンクや添付ファイルを開くことのないよう、ネット上で報告がないか調査する習慣をつけることが肝要です。

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

特別定額給付金に関する通知を装うフィッシング (2020/10/15)

概要

特別定額給付金に関する通知を装うフィッシングの報告を受けています。

メールの件名

二回目特別定額給付金の特設サイトを開設しました。

詳細内容

特別定額給付金に関する通知を装うフィッシングの報告を受けています。

1. 2020/10/15 10:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。 類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。

2. このようなフィッシングサイトにて、氏名 (漢字、フリガナ)、国籍、生年月日、性別、郵便番号、住所、運転免許証/保険番号/パスポート番号、職業、 入金カード、有効期限、認証コード、入金カード種別、申請者電話番号、FAX 番号、メールアドレス、運転免許証/保険番号/パスポート/入金カードの確認書類、 通帳やキャッシュカード、インターネットバンキングの画面の写しや画像等を入力、アップロードしないよう、ご注意ください。

3. 日頃からこのようなメールを受信した際は、メールや SMS 内のリンクからはアクセスしないよう、心がけてください。

4. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

二回目特別定額給付金(新型コロナウイルス感染症緊急経済対策関連)

二回目特別定額給付金の特設サイトを開設しました。(令和2年10月14日)
特別定額給付金ポータルサイト(サイトへリンク) <https://kyufukin.●●●●.online/>
最新の情報についてはこちらをご覧ください。

特別定額給付金の概要

令和2年10月14日、「新型コロナウイルス感染症緊急経済対策」が閣議決定され、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行うため、二回目特別定額給付金事業が実施されることになり、総務省に特別定額給付金実施本部を設置いたしました。

施策の目的

「新型コロナウイルス感染症緊急経済対策」(令和2年4月20日閣議決定)において、「新型インフルエンザ等対策特別措置法の緊急事態宣言の下、生活の維持に必要な場合を除き、外出を自粛し、人と人との接触を最大限削減する必要がある。医療現場をはじめとして全国各地のあらゆる現場で取り組んでおられる方々への敬意と感謝の気持ちを持ち、人々が連帯して一致団結し、見えざる敵との闘いという国難を克服しなければならない」と示され、このため、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行う。

事業費(令和2年度補正予算(第2号)計上額)

12兆8,802億93百万円

- 給付事業費 12兆7,344億14百万円
- 事務費 1,458億79百万円

事業の実施主体と経費負担

- 実施主体は市区町村
- 実施に要する経費(給付事業費及び事務費)については、国が補助(補助率10/10)

給付対象者及び受給権者

- 給付対象者は、基準日(令和2年9月27日)において、住民基本台帳に記録されている者
- 受給権者は、その者の属する世帯の世帯主

給付額

給付対象者1人につき10万円

総務省
MIC Ministry of Internal Affairs and Communications

●岡山大に不正ログイン…フィッシングメール14,666件送信

https://www.itmedia.co.jp/news/articles/2010/08/news149.html
https://www.okayama-u.ac.jp/tp/news/news_id9690.html

このニュースをザックリ言うと・・・

- 10月8日(日本時間)、岡山大学より、同大学教員1名のメールアカウントが不正アクセスを受け、外部にフィッシングメールが送信されていたと発表されました。

- 発表によれば、不正アクセスは同大学研究室のWebサイト公開用に契約していた外部レンタルサーバーに対して行われ、安易なパスワードが設定されていたメールアカウントが不正にログインされ、7月28・29日および9月5・23・25・26日に合計14,666件のフィッシングメールが主に海外へ送信されたとのことです。

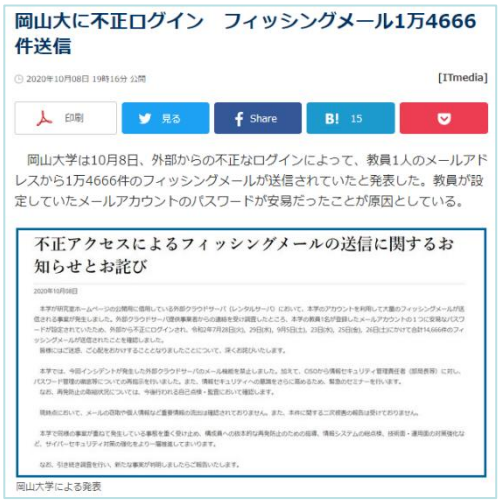
- レンタルサーバー提供事業者からの連絡を受けて発覚したもので、現在はメール機能を停止、またメールの窃取、個人情報など重要情報の流出および二次被害の報告は確認されていないとしています。

AUS便りからの所感

- 同様の事件は2月に長岡技術科学大学でも計66,482件の迷惑メール送信(AUS便り 2020/2/17号参照)が、また岡山大でも同じく2月に同様の不正アクセスで約150万件の迷惑メール送信(https://scan.netsecurity.ne.jp/article/2020/03/03/43758.html)が発生しています。

- 前述の長岡技科大の件ではメールボックスに保存されていたメールが攻撃者に閲覧された可能性も指摘されており、メールアカウントへの不正アクセスを食い止めるために十分に強力なパスワードを設定するよう全ての利用者に啓発することが最優先となるでしょう。

- 一方でサーバー側でも、不審なログイン試行を検知して遮断する設定、あるいは不正ログイン成立時にも不審な外部へのメール送信を食い止められるよう送信量の制限等を設定するといったことを、是非とも検討すべきです。


ITmedia NEWS

岡山大に不正ログイン　フィッシングメール1万4666件送信

2020年10月08日 19時16分 公開　[ITmedia]

印刷　見る　Share　B! 15

岡山大学は10月8日、外部からの不正なログインによって、教員1人のメールアドレスから1万4666件のフィッシングメールが送信されていたと発表した。教員が設定していたメールアカウントのパスワードが安易だったことが原因としている。

不正アクセスによるフィッシングメールの送信に関するお知らせとお詫び

2020年10月08日

本学が研究室ホームページの公開用に使用している外部クラウドサーバ（レンタルサーバ）において、本学のアカウントを利用して大量のフィッシングメールが送信される事案が発生しました。外部クラウドサーバ（提供事業者からの連絡を受け調査したところ、本学の教員1名が登録したメールアカウントの1つに安易なパスワードが設定されていたため、外部から不正にログインされ、令和2年7月28日(火)、29日(水)、9月5日(土)、23日(水)、25日(金)、26日(土)にかけて合計14,666件のフィッシングメールが送信されたことを確認しました。
皆様にはご迷惑、ご心配をおかけすることとなりましたことについて、深くお詫び申し上げます。

本学では、今回インシデントが発生した外部クラウドサーバのメール機能を停止しました。加えて、CSIRTから情報セキュリティ管理責任者（部局長等）に対し、パスワード管理の徹底等についての再指示を行いました。また、情報セキュリティへの意識をさらに高めるため、緊急のセミナーを行います。
なお、再発防止の現時点については、今後行われる自己点検・監査において確認します。

現時点において、メールの窃取や個人情報など重要情報の流出は確認されておりません。また、本件に関するご苦情等の報告は受けておりません。

本学で同様の事案が重なって発生している事態を重く受け止め、構成員への啓発の徹底、情報システムの総点検、技術面・運用面の対策強化など、サイバーセキュリティ対策の強化をより一層推進してまいります。

なお、引き続き調査を行い、新たな事実が判明しましたらご報告いたします。

岡山大学による発表

●Flash Playerに緊急の脆弱性…最新バージョン32.0.0.445へアップデートを

https://news.mynavi.jp/article/20201015-1415234/

このニュースをザックリ言うと・・・

- 10月14日(現地時間)、米US-CERTより、「Flash Player」に脆弱性が確認されたとして注意喚起が出されています。

- 脆弱性はChrome・Firefox・Edge・IE等あらゆるブラウザー向けのFlash Playerに存在し、不正なFlashコンテンツの閲覧により、PCを乗っ取られる恐れがあるとされています。

- Adobe社より脆弱性を修正したFlash Playerの最新バージョン32.0.0.445がリリースされており、必要に応じアップデートを行うよう推奨されています。

AUS便りからの所感

- 2020年一杯を以てFlash Playerは配布・アップデートが終了が発表されており(https://www.adobe.com/jp/products/flashplayer/end-of-life.html)、また今年に入ってからのFlash Playerのアップデートは2月・6月以来3度目と、かつてに比べ頻度が低くなっており、サポート終了までに全ての脆弱性が解消することは期待できないと思われます。

- 既に現時点でブラウザー上でFlashコンテンツの再生には明示的に許可するよう選択する必要がありますが、依然Flashコンテンツを用いているサイトの利用者を騙して不正なFlashコンテンツを再生させようと誘導する攻撃の可能性は十分考えられますので、どんなサイトであっても安易に許可を選択しないよう注意してください(Flash Playerのバージョンを確認するサイト https://get.adobe.com/jp/flashplayer/about/ へのアクセス時も慎重に行いましょう)。

- そして、Flash Playerのアップデートが完了するまでの隙に不正なFlashコンテンツを読み込んでしまう等の可能性を抑止するため、アンチウイルス等による防御を必ず固めておくようにしてください。


マイナビニュース

Adobe Flash Playerに緊急の脆弱性、すぐにアップデートを

2020/10/15 15:06　著者：後藤大地

United States Computer Emergency Readiness Team (US-CERT)は10月14日(米国時間)、「Adobe Releases Security Updates for Flash Player | CISA」において、Adobe Flash Playerに脆弱性が存在すると伝えた。この脆弱性を悪用されると、攻撃者によって影響を受けたシステムの制御権が乗っ取られる危険性がある。

脆弱性が存在するとされるプロダクトおよびバージョンは次のとおり。

- Adobe Flash Player Desktop Runtime 32.0.0.433およびこれよりも前のバージョン（Windows、macOS、Linux）
- Adobe Flash Player for Google Chrome 32.0.0.433およびこれよりも前のバージョン（Windows、macOS、Linux、Chrome OS）
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.387およびこれよりも前のバージョン）

脆弱性が修正されたプロダクトおよびバージョンは次のとおり。

- Adobe Flash Player Desktop Runtime 32.0.0.445（Windows、macOS）
- Adobe Flash Player for Google Chrome 32.0.0.445（Windows、macOS、Linux、Chrome OS）
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.445（Windows 10、Windows 8.1）
- Adobe Flash Player Desktop Runtime 32.0.0.445 Linux