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。

● 稚拙な内容の一通目で注意力を逸らす→本命の二通目で騙す…「二段階式フィッシングメール」警視庁が注意喚起

https://internet.watch.impress.co.jp/docs/news/2116742.html
https://x.com/MPD_cybersec/status/2064986229846987253

このニュースをザックリ言うと･･･

－6月11日(日本時間)、警視庁より、「二段階式フィッシングメール」として、2通のメール等を時間差で送りつけるフィッシングの手口について注意喚起が出されています。

－具体的な例として、1通目に組織の会計係を騙る内容のフィッシングメール等を送信した後、今度は2通目で同じ組織のシステム担当者を騙り「社員に不審なメールが送信されています」と注意を促すと同時に「不審なメール受信状況を調査する」として悪意のあるサイトに誘導するものが挙げられています。

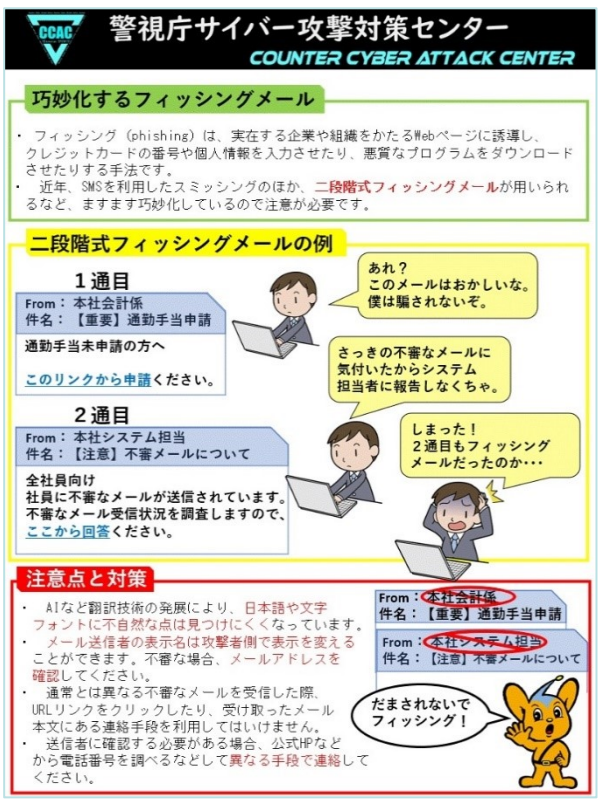
－二段階式フィッシングメールでは、このように1通目であえて稚拙な内容で送って受信者に見破らせることにより、本命となる2通目のメールに対する注意力を逸らさせる目的があるとされています。

AUS便りからの所感等

－注意喚起では最近のフィッシング全般も含めたいくつかの注意点・対策も取り上げていますが、AI等翻訳技術の発展により、日本語や文字フォントに不自然な点は見つけにくくなっている等としています。

－またメール送信者(From:)の名義は送信する側で任意の名前を設定できるため、不審な場合はメールアドレスを確認するよう推奨しています(ここで自組織のドメイン名を悪用している場合はSPF・DKIM・DMARCによる遮断が期待できる一方、全く無関係なドメイン名でSPF等を設定しているケースも多々あることに注意が必要です)。

－信頼できる送信元であることを確認できない限り、メールに記載されたリンクやボタンを決してクリックしないことが最も確実性の高い回避策の一つであり、他にもメールとは別の、通常使用している電話・Slack等の連絡手段を用いる(メールに記載されている連絡先が普段と異なる場合にも警戒すべきです)等、慎重な行動を常時とることが重要です。



● 5月度フィッシング報告件数は126,061件…下旬に報告等急減

https://www.antiphishing.jp/report/monthly/202605.html

このニュースをザックリ言うと・・・

- 6月18日(日本時間)、フィッシング対策協議会より、5月に寄せられたフィッシング報告状況が発表されました。

- 5月度の報告件数は126,061件で、4月度(https://www.antiphishing.jp/report/monthly/202604.html)の151,112件から25,051件減少しています。

- フィッシングサイトのURL件数は40,912件で4月度(66,574件)から25,662件減少、使用されるTLD(トップレベルドメイン名)の割合は .com(約47.3%)、 .jp(約35.4%)、 .cn(約10.1%)で全体の約92.8%、次いで.so(約1.9%)、 .shop(約1.0%)、.cfd(約0.9%)、 .pl(約0.8%)、 .net(約0.8%)、 .gd(約0.6%)、 .co(約0.4%)と併せて、全体の約99.1%を占めたとしています。

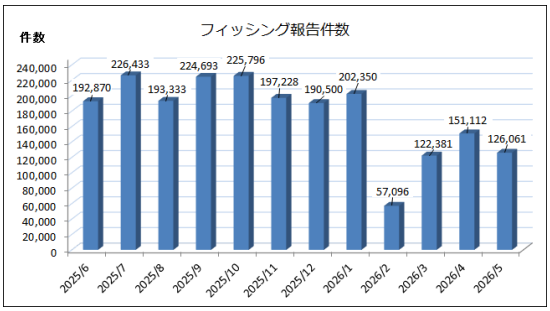
- 悪用されたブランド件数も112件で4月度(117件)から5件減少、最も報告が多かったブランドは楽天カードが約18.5%、次いでPayPayカード(約17.1%)、Amazon、Apple、日本年金機構と合わせて約60.4%、さらに1,000件以上報告された23ブランドまで含めると約89.3%となっています。

AUS便りからの所感

- 同協議会への報告件数や、調査用メールアドレス宛に届いたフィッシングメールの件数の日毎の推移について、5/23-25にそれぞれ急減をみせたことにより、月間での件数についても再減少が発生していますが、手元では6月上旬にある程度の増加、中旬にはまた減少といった印象があり、6月においても概ね3月以降の水準以内で推移するとみられます。

- 調査用メールアドレス宛に届いたメールの約98.0%がPTRレコード(IPアドレスからの逆引き)非設定とされ、逆引き、さらにはFCrDNS(逆引きで得たホスト名をさらに正引きして検証)によるチェックを行うことがフィッシング・スパムメールの大幅な遮断に繋がる可能性があるとみられますが、PTRレコードが設定されているGoogle Cloud等からの発信も多く存在する上、万が一実際の取引相手でDNS設定が正しくない送信元のメールを遮断しないよう、設定には細心の注意を払うことが重要です。

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



● WordPressのフォーム作成プラグイン「Everest Forms Pro」に致命的脆弱点、4月以降攻撃を確認

https://cybersecuritynews.com/wordpress-plugin-vulnerability-exploit/
https://www.wordfence.com/blog/2026/06/attackers-actively-exploiting-critical-vulnerability-in-everest-forms-pro-plugin/
https://innovatopia.jp/cyber-security/cyber-security-news/107998/

このニュースをザックリ言うと・・・

- 6月3日(米国時間)、WordPress向けセキュリティプラグイン「Wordfence」を提供するDefiant社より、WordPress用フォーム作成・設置プラグイン「Everest Forms Pro」の脆弱点を悪用する攻撃が4月以降発生していたと発表されています。

- 脆弱点(CVE-2026-3300)は3月30日に発表されていたもので、公開されているフォームへの不正な入力により、Webサーバー上で任意のPHPコードを実行され、サーバーの乗っ取りに繋がり得る恐れがあったとされ、同18日リリースの1.9.13で修正されていました。

- Defiant社によれば、4月13日以降に脆弱点を狙った攻撃を確認、ピークとなる5月16日には17,900件以上の攻撃が発生したとしており、Wordfenceによって29,300件以上の攻撃を遮断したとしています。

AUS便りからの所感

Cyber Security News

- Everest Forms Proは、Defiant社の推定では世界で4,000件近くインストールされているとのことです。

- Defiant社が確認した攻撃は、管理者アカウント「diksimarina」を作成するという特徴があったとし、当該プラグインをインストールしている場合には1.9.13以降にアップデートされていることの確認の他、不審な管理者アカウントの確認と削除を行うことも強く推奨されています。

- 有償版の同プラグインの他に無償版の「Everest Forms」も提供されていますが、こちらにも同様に危険度の高い脆弱点(CVE-2026-3296)が報告され、3月24日リリースの3.4.4で修正されています。

- WordPressでは、本体からサードパーティー製のプラグインに至るまで日々何らかの脆弱性が報告されており、インストールしているプラグイン全てについて随時セキュリティ情報を確認しつつ、最新バージョンに保つよう留意すること、またWordfence等セキュリティ機能を提供するプラグインについても、数多く提供されているものから選択の上、必ず導入することが重要です。