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。

●3月度フィッシング報告件数は43,423件、急増した1月度と同水準に…対策協議会発表

https://www.antiphishing.jp/report/monthly/202103.html

このニュースをザックリ言うと･･･

- 4月2日(日本時間)、フィッシング対策協議会より、3月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 3月度の報告件数は43,423件で、2月度(https://www.antiphishing.jp/report/monthly/202102.html)の30,949件から12,474件の増加となり、1月度(https://www.antiphishing.jp/report/monthly/202101.html)に記録した43,972件に近い水準となっています。

- フィッシングメールに悪用されたブランドについて、報告全体に対するAmazonの割合が51.9%、楽天・MyJCB・三井住友カード・エポスカードを合わせた5ブランドで約81.7%とそれぞれ2月度より減少し、一方でISP・ホスティング業者を騙ったメールアカウント・管理アカウントの詐取が目的とみられるフィッシングの報告についても言及されています。

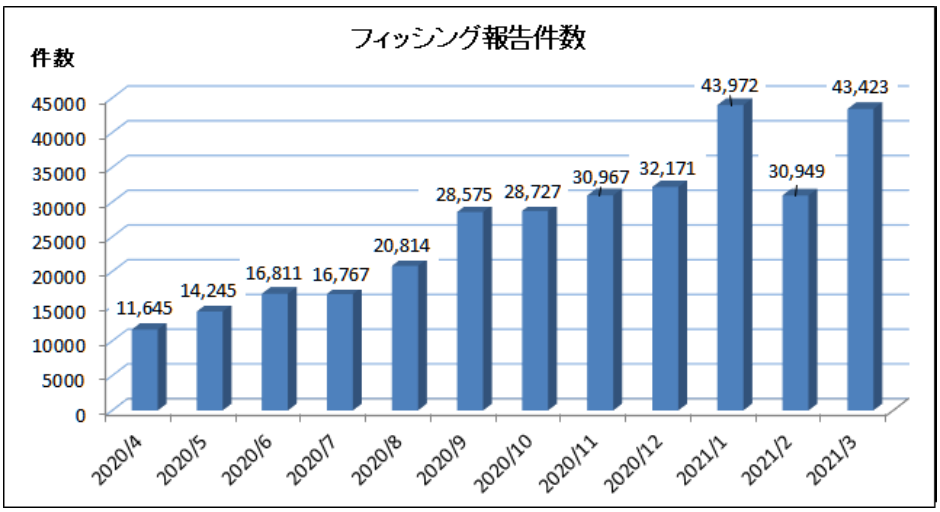
AUS便りからの所感等

- 月間の報告件数は2019年以降右肩上がりの傾向を持続しており、今年に入ってからは急増とそれまでの水準との間で乱高下しているものの、やがては4万件台を維持、さらには今年中に5万件台に乗るものと予想されます。

- SMSによるフィッシングについて、送信元の電話番号は、同様のSMSから不正なアプリのインストールへ誘導された被害者のものである可能性が高いとしており、PC等でのマルウェア感染と同じく、感染者がさらなる加害行為に加担させられている恐れもあることに改めて留意すべきでしょう。

- また厳密なフィッシングとは異なるものの、ユーザーのプライバシーを盗み見ていると偽って仮想通貨を要求する脅迫メール(セクストーション)についても注意喚起を出し、過去に漏洩した情報をもとにメールが送られているケースも確認されているとしており、同協議会を含め様々なセキュリティ関連団体等が行っている啓発、自分たちが利用しているサービス等からの公式発表あるいはソーシャルネットワーク上での情報をもとに、サービスの公式サイトにはあらかじめブックマークからアクセスする等、適切な防御策と慎重な行動でフィッシングをはじめとする各種攻撃に対応できるようにすることが肝要です。

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



●「gmail.com」入力ミスで…大学入学予定者135人の個人情報流出か

https://www.itmedia.co.jp/news/articles/2104/01/news095.html
https://www.kcua.ac.jp/20210331_mail/

このニュースをザックリ言うと・・・

- 3月31日(日本時間)、京都市立芸術大学より、同大学の2021年度入学予定者の個人情報が学外に流出した可能性があると発表されました。
- 該当する情報は、美術学部への入学予定者135人の志望科・氏名・ふりがな・性別・出身校名とされ、それ以外の住所・電話番号・メールアドレス等は含まれていないとのことです。
- 事務局から教員に対し、授業のクラス分けに必要な情報として当該情報を送信した際、「***@gmail.com」となっていたメールアドレスを「***@gmai.com」と誤入力して送信していたことが原因としています。

AUS便りからの所感

- 「gmail.com」のような全世界にユーザーがいるドメイン名に対し、誤送信やWebアクセス等を狙って似たようなドメイン名を取得する手口は「タイポスクワッティング」と呼ばれて長年行われており、またそれを阻止するために本来のサービス提供者が取得するケースもあります。
- メール送信時のミスによる情報流出のケースとしては、他にも「複数のユーザーにメールを送信する際、メーラーのBcc:ではなくCc:にメールアドレスを入力した」という事例が度々発生しています。
- これらのケースに対応したメールの誤送信防止機能はメーラー自身に備わっている場合があるほか、メーラーへのアドオンやメールサーバー等に対するソリューションとして提供されている場合もありますので、どういったケースの誤送信・情報流出の恐れがあるかを把握した上で、できる限り各ユーザーによるチェックだけに依存せず、防止機能・ソリューションの導入を検討することが望まれます。


京都市立芸大、誤送信で135人の入学者情報流出
「gmail」を「gmai」と入力ミス
2021年04月01日 14時40分 公開 [ITmedia]
印刷 見る Share B! 7
京都市立芸術大学は3月31日、2021年度の入学予定者135人の個人情報が学外に流出したと発表した。職員の入力ミスが原因で、「***@gmail.com」とするべきドメイン名を「***@gmai.com」と入力していた。
京都市立芸大学（出典：公式ページ）
流出したのは、美術学部に入学予定の学生の氏名、性別、出身校名、志望科。同大によると、大学の事務局職員が授業のクラス分けのためにこれらの情報をリスト化して、3月17日と24日に教員に送付したという。住所、電話番号、メールアドレスはリストに記載していなかった。

●PHP開発用サーバーに不正アクセス…ソースコード改ざん発生

https://gigazine.net/news/20210330-phps-git-server-hacked-backdoors/

このニュースをザックリ言うと・・・

- 3月28日(現地時間)、米国のPHP開発者チームより、PHP開発用サーバーが不正アクセスを受けたと発表されました。
- 不正アクセスにより、開発中のPHPのソースコードに悪意のあるコードが挿入されたことが明らかになっています。
- 開発者チームでは自前のサーバーによるソースコード管理を断念し、これまでミラーサイトとしてきたGitHubを正式に利用すること、また新しいバージョンのリリースを2週間保留するとしています。

AUS便りからの所感

- 悪意のあるコードは、特定のリクエストを受信した際、リクエストヘッダー内で指定された任意のコードをWebサーバー上で実行するものであった模様ですが、現在リリースされているPHP 8.0系・7.4系ないしそれ以前へ挿入されたものではなく、一般的なPHPの利用者への影響は免れているとみられています。
- 今回は該当しないとされるものの、攻撃者が開発者のアカウントを乗っ取ることにより、マルウェアや悪意のあるコードをソフトウェアに仕込む手口は、いわゆる「サプライチェーン攻撃」の一環として名のあるソフトウェアでも度々発生しており、ユーザー側でのアカウントの管理はもちろん、サービス側でも未使用のアカウントが悪用されないよう管理すること、サーバーへのアクセスの監視等も徹底すること、また開発者同士でもコードの修正等を必ずチェックすること等が重要です。


GIGAZINE
2021年03月30日 11時07分 ソフトウェア
ハッカーがPHPの開発者になりすましてソースコードにバックドアを仕込んでいたことが判明
オープンソースのプログラミング言語であるPHPの開発者らが使用していたGitサーバーに何者かが侵入し、PHPのソースコードにバックドアをしかけていたことが判明しました。ハッカーは悪意のあるコミットをプッシュする際、PHPの開発者であるラスマス・ラードフ氏らになりすましていました。