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。

●PayPayへのクレカ不正登録被害…登録チェック機構に問題

https://www.nikkei.com/article/DGXMZO39061320X11C18A2X30000/
https://www.nikkei.com/article/DGXMZO39071890181220I8CC1000/
http://www.itmedia.co.jp/mobile/articles/1812/17/news090.html
http://www.itmedia.co.jp/news/articles/1812/19/news145.html

このニュースをザックリ言うと･･･

- 12月中旬、スマートフォンから利用できる電子決済サービス「PayPay」において、サービスを利用していない第三者のクレジットカードが登録され、不正に利用される被害が相次いで発覚しています。

- 同14日以降、運営元のPayPay社より注意喚起等の対応が行われており、同社では「(出資元である)ヤフーやソフトバンクのサービスからカード情報が流出した事例はない」としています。

- PayPayに登録可能なVISA、MasterCardおよびYahoo!カードについて、理論上は任意のカードが不正登録される可能性があったとみられ、同社からも心当たりがないカードの利用についてはカード会社に連絡するよう呼びかけられています。

AUS便りからの所感等

- PayPayアカウントが乗っ取られたわけではなく、悪意のあるPayPayユーザが外部で入手した他人のカード情報を登録したものとされており、12月初頭にPayPayが行ったキャンペーンにあわせてか、ダークウェブ（闇サイト）上では以前流出したカード情報が大量に売買されたとの情報があり、これをもとに不正登録が行われた模様です。

- PayPayアプリにおいては、カード番号・有効期限・セキュリティコード(CVV)の入力で登録できる仕組みになっていて、複数回入力失敗した場合に登録をロックする機能や「3Dセキュア」による本人認証を行っていなかったことが指摘されており（その後、複数回の入力失敗時にはロックするよう対応された模様です）、少なくとも3Dセキュアに対応していれば、不正登録が行われる可能性は大幅に抑えられたものと思われます。

- 利便性を優先して十分なセキュリティを確保しなかったことにより、今回はこれまでのような「サービスに登録されたアカウントや機密情報が奪取された」ケースとは異なる「第三者の情報が本人のあずかり知らないところで登録、利用される」事態が発生することになりました。

- 十分な本人確認を行うことや、カード情報の管理を含めた決済業務を「PCI DSS」に準拠する決済代行業者に委託すること等、決済が発生するサービスの立ち上げや運用にあたっては、是非とも今回の一件とそれに対する指摘を念頭に置くべきでしょう。

日本經濟新聞


スマホ決済「ペイペイ」、不正利用相次ぐ
ネット・IT　社会
2018/12/17 21:22
保存　共有　印刷　その他
ヤフーとソフトバンクが出資するスマートフォン（スマホ）決済会社のPayPay（ペイペイ、東京・千代田）は17日、スマホの決済サービスで、不正な利用があったことを明らかにした。同社はセキュリティー対策を強化し、被害の拡大を防ぐとしている。
【関連記事】スマホ決済、競争過熱　普及には使い勝手が課題

画像の拡大
ペイペイを利用したことのない人に請求が届くなど、現時点で被害は数十件に上るとみられる（ペイペイのホームページ）


ペイペイ不正利用「ダークウェブ」でカード情報入手か
ネット・IT　社会
2018/12/18 11:47
保存　共有　印刷　その他
スマートフォン（スマホ）を使った決済サービス「ペイペイ」で、クレジットカードが不正に利用される被害が相次いで発覚した。セキュリティーの専門家によると、匿名性の高い闇サイト群「ダークウェブ」上では日本人のカード情報が大量に流出、流通しており、今回の不正利用との関連が疑われている。アプリにカード情報を登録する際の仕組みも悪用されており、不正対策の強化が求められている。
ペイペイを巡るカード不正利用の構図

画像の拡大

ITmedia Mobile


PayPayの「クレジットカード不正利用」はなぜ起きたのか？
2018年12月17日 15時09分 公開
印刷　1838　1063
PayPayが、コード決済サービス「PayPay」から…対応について、注意喚起を行っている。
PayPayは、身に覚えのないPayPayからの請求が…履歴であるレシートを確認するよう呼びかけている…あった場合、自分の携帯番号とクレジットカード情…だし、支払いのキャンセルをするには店舗での手続…るよう求めている。
レシートに身に覚えのない履歴がない、またはPa…ユーザーの携帯電話やクレジットカードを知りえる…確認するよう呼びかけている。それでも心当たりが…利用されている可能性があるので、カード会社に連…

ITmedia NEWS


PayPayが謝罪、クレカ不正利用などの問題で　「再発防止徹底する」
2018年12月19日 20時43分 公開
[ITmedia]
印刷　114　30　B!　9
モバイル決済サービス「PayPay」でクレジットカードの不正利用や二重決済などの問題が起きたことを受け、PayPay社は12月19日、公式サイトで謝罪した。利用者の意見を真摯（しんし）に受け止め、順次改善施策を講ずるという。

お客様へのお詫び
2018年12月19日　お知らせ
いつもPayPayをご利用いただき、ありがとうございます。
この度は、二重決済や身に覚えのない請求など、多大なるご迷惑とご心配をお掛けしましたことを深くお詫び申し上げます。現在、皆さまから頂戴したご意見や関係各所からのご指摘を真摯に受け止め、順次改善施策を講じております。
改善施策の詳細につきましては、更なる不正利用防止の観点から皆さまにお伝えすることができません。あらかじめご了承いただけますよう、お願い申し上げます。
また、クレジットカードを不正利用された疑いのある場合は速やかにクレジットカード会社にご連絡ください。
弊社では今回このような問題が発生したことを重く受け止め、再発防止策の徹底を図り、安全・安心なサービスの運用に向けて全力で取り組んでいきます。
PayPayが公式サイトで謝罪

●兵庫教育大から11,322人分の個人情報漏洩…メール転送先で不正アクセス

https://www.kobe-np.co.jp/news/sougou/201812/0011912582.shtml

このニュースをザックリ言うと・・・

- 12月17日（日本時間）、兵庫教育大学より、学内外の11,322人分の個人情報が漏洩した可能性があると発表されました。

- 同大学の事務職員が2017年4月1日以降大学のメールアドレス宛のメールを外部のフリーメールサービスに転送する設定を行っていたところ、今年10月26日に転送先のメールアカウントが不正ログインを受け、その間に転送されていた個人情報を含むメールを第三者に閲覧された可能性があるとしています。

- 大学側では学内メールの自動転送を禁止し、今後メールアカウントへのログイン時に2段階認証の導入も検討するとしています。

AUS便りからの所感等

- 職員が使用していたフリーメールサービスへの不正アクセスが原因で勤務先の個人情報漏洩が発覚したケースとしては、9月にも静岡県島田市で同様のケースが発生しており（AUS便り 2018/10/01号 参照）、この時と同様、職員個人が契約した「大学の管理が及ばない」メールアカウントを「安全に管理していなかった」ことが流出の元となったと考えられます。

- 組織が提供する各種サーバ・サービスの利用が単に不便なものであれば、機密情報の持ち出しや、個人所有機器の持ち込みが組織のあずかり知らないところで行われる可能性は今後も考えられますので、資産管理ソリューションやUTM等による、機器・サービスの利用およびデータの出入りの管理・監視は、ネットワーク、システムおよびそこで管理される機密情報の保護の面でも重要視されるべきでしょう。


神戸新聞NEXT

2018/12/17 17:54 神戸新聞NEXT

学生ら１万人の個人情報流出　兵教大、パスポート写しや銀行口座番号も

ツイート　おすすめ 22　シェア　印刷

謝罪する兵庫教育大の福田光宏学長（右から２人目）＝神戸市中央区、兵庫教育大神戸ハーバーランドキャンパス　拡大

兵庫教育大学（本部・兵庫県加東市）は１７日、４０代の男性事務職員が業務用メールを転送していたフリーメールに不正ログインがあり、学生を含む学内外の約１万人の個人情報が流出した可能性がある、と発表した。パスポートの写しや銀行の口座番号など、機密性の高い情報も１４０人分含まれていたという。

大学によると、男性職員は２０１６年４月１日から、業務用メールをフリーメールへ自動転送するように設定。今年１０月２６日にフリーメールへの不正ログインに気付いたという。その時点で、フリーメール上に約４万通のメールが残っており、学生や教職員、学外の講師ら１万１３２２人分の名前や住所などが書かれていた。また、金融機関の情報や学生の障害・病歴が書かれたものもあったという。

男性職員から報告を受けた大学側が調べたところ、今年５月以降、日本や中国、台湾から２７回の不正アクセスが確認された。大学側は機密性の高い情報が漏れた可能性のある１４０人に順次、謝罪しているが、現時点で被害は把握していない。また、大学のメールサーバーなどへの不正アクセスは確認されていないという。

●年末年始における情報セキュリティに関する注意喚起、JPCERT呼びかけ

https://www.jpcert.or.jp/pr/2018/pr180002.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となる年末年始を迎えるにあたり、12月18日（日本時間）にJPCERT/CC、同20日にはIPAより、情報セキュリティに関する注意喚起が出されています。

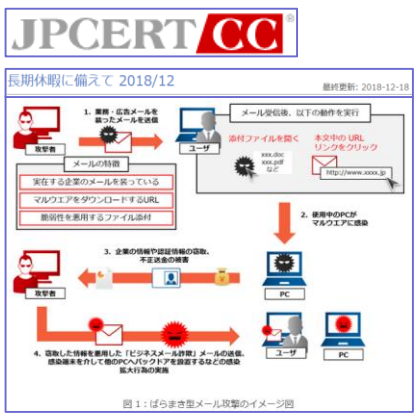
- 両組織とも、実在の企業の業務メール等をかたり、情報詐取型マルウェアをばらまく攻撃を取り上げていますが、特にJPCERT/CCでは、昨今の攻撃手法に変化がみられており、感染した端末のメールやWebサイトの情報を窃取する機能が追加され、窃取した情報をもとにさらなる攻撃を行う可能性を指摘しています。

- この他JPCERT/CCでは、昨年末から確認されたWebサーバソフトウェアの脆弱性を狙う攻撃が今も続いている例を挙げて、アプリケーションやサーバを最新に保ち、アクセスに用いるIPアドレスやポートを制限するよう呼び掛けています。

AUS便りからの所感等

- セキュリティ機関の呼びかけにおいては、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有が、そういった攻撃による被害を最小限に抑えられるために大切なことと言えます。


JPCERT CC

長期休暇に備えて 2018/12

最終更新: 2018-12-18

図１：ばらまき型メール攻撃のイメージ図