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から「パスワードリセットのお知らせ」メール、本物でも身に覚えなければ触らないで

https://www.itmedia.co.jp/news/articles/2509/25/news123.html
https://x.com/PayPaysupport/status/1971048047279997301
https://paypay.ne.jp/help/c0016/

このニュースをザックリ言うと･･･

- 9月25日(日本時間)、PayPayより、「第三者のパスワード再発行操作により、身に覚えのないパスワードリセット通知が届く事象を検知」しているとして、X(旧Twitter)上で注意喚起が出されています。

- Xを含めたネット上では「notice＠paypay-corp.co.jp」から件名「[PayPay]パスワードリセットのお知らせ」のメールが届いたとの報告が多数寄せられていますが、paypay-corp.co.jpはPayPayの正規のドメイン名で、通知メールもフィッシング等ではなくPayPayから送信されたメールとみられています。

- 注意喚起では、心当たりがない場合、通知メールを削除すればパスワードリセットは行われないとしており、不安な場合は手元のアプリからのパスワード再設定を行うよう呼び掛けています。

AUS便りからの所感等

- 攻撃者が別途入手したり推測したりしたメールアドレスに対し、無差別にパスワードリセットを行うよう仕掛けた可能性があり、ネット上の反応から、少なくともユーザーを不安がらせる愉快犯的行為の役割は果たせたものと思われます。

- 今回の手口で通知メールを受信したユーザーがリンクを辿り、パスワードの変更等何らかのアクションをとったとしても、それだけでは攻撃者が即座にアカウントの乗っ取りが行えるわけではなく、改めて新しいパスワードでログインしようとするユーザーを偽のログイン画面へ誘導する等も十分に考えられ、SNS等ネット上で同様の報告がないか、およびサービス公式の発表やヘルプ情報を調査し、慎重に行動するよう心掛けることが肝要です。

PayPay、「身に覚えのないパスワードリセット通知」に注意喚起　「受け取っても操作不要」

2025年09月25日 16時13分 公開　[ITmedia]

PayPayは9月25日、「第三者のパスワード再発行操作により、身に覚えのないパスワードリセット通知が届く事象を検知している」として、サポート用のXアカウントで注意を呼び掛けた。

心当たりがない場合は通知は削除し、操作は不要と案内している。操作しなければパスワードがリセットされることもない。

PayPay公式サポート @PayPaysupport · 4時間
⚠注意
第三者のパスワード再発行操作により、身に覚えのないパスワードリセット通知が届く事象を検知しています。
お心当たりない場合、通知は削除し操作は不要です リセットもされません。
ご不安な場合は、通知上のURLではなく必ずお手元のアプリからパスワード再設定を

ログインできない場合のパスワード再設定/パスワードを忘れた場合 - PayPay へ...
paypay.ne.jpから
6　173　102　3万

不安な場合は、通知上のURLではなく、手元のアプリからパスワードを再設定してほしいと案内している。

●大学の教員用メールサーバに不正ログイン、メール差出人情報読み取られた可能性

https://scan.netsecurity.ne.jp/article/2025/10/01/53715.html
https://www.chuo-u.ac.jp/aboutus/informational/itcenter/news/2025/09/81980/

このニュースをザックリ言うと･･･

- 9月19日(日本時間)、中央大学より、同大学の教員用メールサーバーが不正アクセスを受け、教員2名のメールアカウントにログインされた可能性があると発表されました。

- 不正ログインにより、メールインデックス情報が読み取られ、7月23日までに当該アカウントにメールを送信した差出人のべ1082名分のメールアドレス・氏名が流出した可能性があるとしています。

- 同大学では対象者に個別に連絡を行うとともに、メールの差出人情報が標的型攻撃メールに利用される恐れがあるとして注意喚起を行っています。

AUS便りからの所感

- メールの本文までの読み取り、およびアカウントを踏み台にしてのスパムメール送信は行われていない模様ですが、仮に元のユーザー・組織になりすましてのメール送信が行われた場合、SPF・DKIM・DMARCといった各種フィッシング対策機構による確認が通用しなくなる恐れがあります。

- 不正ログインに至った原因の詳細は不明ですが、過去の同様の事案では、簡単なパスワードが設定されていたり、いわゆる「リスト型攻撃」で不正ログインに至ったケースもあり、他と使い回していない十分に複雑なパスワードを設定すること、およびPCがマルウェアに感染しての不正ログインを避けられるようアンチウイルス・UTM等による防衛が重要です(多要素認証が設定可能なメールサービスであれば、是非とも設定を行うべきです)。

● Steam配信ゲームでマルウェア入りアップデート、暗号資産奪取の被害

https://automaton-media.com/articles/newsjp/blockblasters-20250923-358730/
https://www.theverge.com/news/782993/steam-blockblasters-crypto-scam-malware
https://www.bleepingcomputer.com/news/security/verified-steam-game-steals-streamers-cancer-treatment-donations/

このニュースをザックリ言うと･･･

- 9月22日(現地時間)、米IT系メディアBleeping Computer等より、ゲームプラットフォーム「Steam」で配信されていたゲームで悪意のあるアップデートが行われていたと報じられています。

- 7月30日にリリースされた2Dアクションゲーム「BlockBlasters」において、8月30日のアップデートでマルウェアが仕込まれ、インストールしたPCから暗号資産を奪取する挙動を示していたとされています。

- 9月21日に当該ゲームはSteamから削除されましたが、261ユーザーがマルウェアの被害を受け、被害総額は15万ドル(約2,200万円)に上るとされており、Bleeping ComputerではBlockBlastersをインストールしたことがある場合、Steamのパスワードをすぐにリセットし、暗号資産を新しいウォレットに移動するよう注意喚起しています。

AUS便りからの所感

- ゲームプラットフォームでマルウェア入りゲームが配信された事案として、今年2月に同じくSteamにおいて配信されていた「PirateFi」(AUS便り 2025/02/27号)等が挙げられます。

- Bleeping Computerでは、一般にダウンロード数やレビュー数が少ないゲームや、開発段階が「ベータ」のタイトルにはマルウェアが含まれている可能性があるため、注意するよう呼び掛けている一方、今回のBlockBlastersは最初のリリース後にレビューで高評価を得ていたとされ、また段階的に悪意のあるコードを追加したり(あらゆるマルウェアでみられる手口ですが)、標的型攻撃だったとみられたりと、巧妙な攻撃が行われた様子が窺え、Androidアプリストア等と同様にプラットフォーム側でマルウェアの配信の阻止を効果的に行えるか、またマルウェアがSteamアプリケーション等の枠外を出てPCに入り込んだりするのを阻止できるようになるか等が注目されるところです。