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。

●社会実験応募者のメールアドレス流出…メール誤送信

https://mainichi.jp/articles/20191118/k00/00m/040/189000c
https://prtimes.jp/main/html/rd/p/000000004.000051036.html

このニュースをザックリ言うと・・・

- 11月18日(日本時間)、Plasma社より、同社が実施予定の社会実験「Exograph」応募者の一部メールアドレスが誤って外部に流出したと発表されました。

- 同17日の夜、書類選考での落選者約500人への通知メール送信時、アドレスをBcc: (送信されたメールには表示されない)ではなくCc: に入れて送ったことにより、同時にメールが送信された他の落選者のメールアドレスが見える状態にあったとのことです。

- 対象となった相手にはメールで謝罪の上、今後、1人当たり1万円の賠償金を支払う予定としています。

AUS便りからの所感等

- 大量のメールアドレスをBcc: ではなくCc:やTo:に入れてしまうミスでのメールアドレス流出事故は度々発生しており、例えば2018年10月には兵庫県立図書館からのお知らせメールで約3,300件のアドレス流出が発生している(AUS便り 2019/8/19号参照)他、今月にも県立広島大学にて同様の事故が発生しています(https://scan.netsecurity.ne.jp/article/2019/11/17/43242.html)。

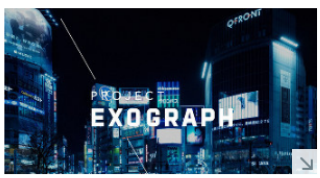
- 今回も原因となったメールの送信は社長自身が手入力で行ったとしており、このような潜在的リスクの高い単純な方法をとるのではなく、メーリングリストやメール配信サービス等、同報メール送信のためのシステムを導入すること、どうしてもメーラーで対応せざるを得ない場合はメーラー自身あるいはアドオンで提供される誤送信防止機能を有効にすることが肝要です。

毎日新聞

「私生活動画」収集計画のＩＴ会社、参加希望者のメアド流出

毎日新聞 2019年11月18日 17時38分（最終更新 11月18日 22時07分）

社会 > 速報 > 政治プレミアタイムライン >



今回の社会実験について案内するウェブページ＝Plasmaのウェブサイトから

［PR］

報酬20万円で1カ月間にわたり私生活の動画を撮影、収集する社会実験を計画しているIT会社「Plasma（プラズマ）」（東京都目黒区、遠野宏季社長）は18日、参加希望者の一部（約500人）に対し、別の参加者のメールアドレスが見られる状態でメール送信するミスがあったと発表した。【吉田卓矢/統合デジタル取材センター】

<20万円で私生活動画>1311人応募　年収200～400万円が半数

<「生活保護費と同額の代価で私生活動画」>実験を始めた社長の狙い

同社によると、ミスがあったのは17日午後11時ごろに送信したメールで、書類選考に落ちた人に落選を通知するメールだった。複数人にメールを送る際、本来「BCC」で送らなければならないところを、誤って「CC」で送り、他人のメールアドレスが見られる状態になっていた。遠野社長自身がメールを送信。直後に自分で気づき、メールで謝罪した。今後、1人当たり1万円の賠償金を支払う予定という。

PR TIMES

社会実験Exograph、一部の応募者のメールアドレスをBCCでなくCCに入れ誤送信

株式会社Plasma（東京都目黒区、代表取締役　遠野宏季）は、社会実験Exographの一部の応募者へのメールアドレスをBCCではなくCCに入れ誤送信してしまいました。

株式会社Plasma　2019年11月18日 00時53分

450 いいね！ シェア　ツイート　はてな　素材DL　その他

株式会社Plasma（東京都目黒区、代表取締役　遠野宏季）は、11月17日夜に社会実験Exographの一部の応募者のメールアドレスをBCCではなくCCに入れ誤送信してしまいました。応募者の方と関係者の方にご迷惑をお掛けし、大変申し訳ありませんでした。以後、再発防止に努めると共にプライバシーポリシーの見直しを行います。

株式会社Plasma（東京都目黒区、代表取締役　遠野宏季）は、11月1日からプライベート情報を全て収集・マネタイズするExographの第一回社会実験を行っています。
https://exograph.plasma.inc/

その応募者へのメール連絡業務の中で、11/17夜に一部の応募者のメールアドレスをBCCではなくCCに入れ誤送信してしまいました。

応募者の皆様と関係者の方々に大変なご迷惑をお掛けし、大変申し訳ありませんでした。

●「officeアカウント情報を完善してPinコードを設定。」Microsoftを騙るフィッシングに注意喚起

https://www.jc3.or.jp/topics/v_log/201911.html#d20191118
https://internet.watch.impress.co.jp/docs/news/1208223.html

このニュースをザックリ言うと・・・

- 11月18日(日本時間)、日本サイバー犯罪対策センター(JC3)より、Microsoftを騙るフィッシングメールに対し注意喚起が出されています。

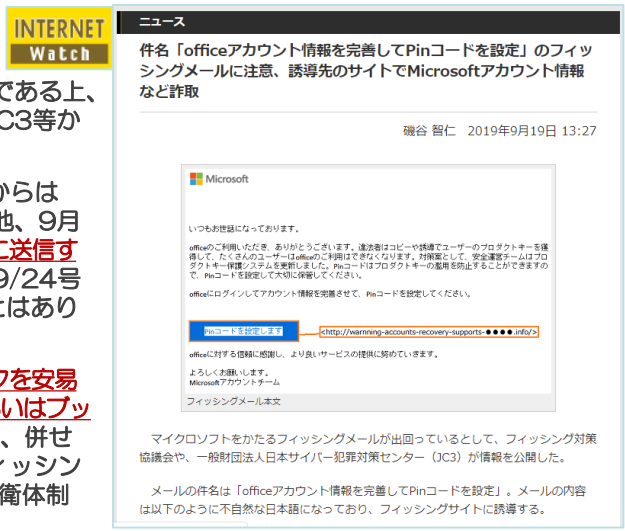
- メールは件名が「officeアカウント情報を完善してPinコードを設定。」で、本文は「officeにログインしてアカウント情報を完善させて、Pinコードを設定してください。」等と書かれ、リンクをクリックすると「OFFICEのプロダクトキーが不正コピーされています」と表示してMicrosoftアカウントおよびクレジットカード情報を詐取しようとする偽サイトにアクセスする模様です。

AUS便りからの所感

- 「アカウント情報を完善」等不自然な日本語からなるフィッシングである上、また9月19日には全く同じ内容のフィッシングメールが確認され、JC3等から注意喚起が出されていました。

- また、フィッシング対策協議会(https://www.antiphishing.jp/)からは11月に入り三井住友銀行やJCBを騙るフィッシングも出されている他、9月には「フィッシングメールの件名や文面、URLを少しずつ変えて小規模に送信するケースが増えている」等の傾向も報告されており(AUS便り 2019/9/24号参照)、巧妙に行われるフィッシングに対し常に警戒するに越したことはありません。

- とにかくフィッシングに騙されないようにするには「メールのリンクを安易にクリックしない」「正規のサイトのURL(ドメイン名)を記憶する、あるいはブックマークし、そこからアクセスする」といった回避策がまず重要であり、併せてメーラー・ブラウザー・セキュリティソフト・UTM等のアンチフィッシング機能を有効にすることにより、フィッシングに対するより強固な防衛体制をとることを推奨致します。


INTERNET Watch

ニュース

件名「officeアカウント情報を完善してPinコードを設定」のフィッシングメールに注意、誘導先のサイトでMicrosoftアカウント情報など詐取

磯谷 智仁　2019年9月19日 13:27

Microsoft

いつもお世話になっております。

officeのご利用いただき、ありがとうございます。違法者はコピーや誘導でユーザーのプロダクトキーを獲得して、たくさんのユーザーはofficeのご利用はできなくなります。対策として、安全運営チームはプロダクトキー保護システムを更新しました。Pinコードはプロダクトキーの盗用を防止することができますので、Pinコードを設定して大切に保管してください。

officeにログインしてアカウント情報を完善させて、Pinコードを設定してください。

Pinコードを設定します　<http://warnning-accounts-recovery-supports-●●●●.info/>

officeに対する信頼に感謝し、より良いサービスの提供に努めていきます。

よろしくお願いします。
Microsoftアカウントチーム

フィッシングメール本文

マイクロソフトをかたるフィッシングメールが出回っているとして、フィッシング対策協議会や、一般財団法人日本サイバー犯罪対策センター（JC3）が情報を公開した。

メールの件名は「officeアカウント情報を完善してPinコードを設定」。メールの内容は以下のように不自然な日本語になっており、フィッシングサイトに誘導する。

●公立高校の校内サーバがランサムウェアに感染

https://scan.netsecurity.ne.jp/article/2019/11/11/43203.html

このニュースをザックリ言うと・・・

- 11月1日(日本時間)、神奈川県川崎市より、同市立橘高等学校の校内ネットワーク上のサーバーがランサムウェアに感染したと発表されました。

- 10月28日に、Wordファイルが暗号化され、画面上に英文の脅迫文が表示されたことから感染が発覚したとされ、授業や学習活動で生徒が作成した成果物などのデータ・ファイルが使用できない状況となっているとのことです。

- サーバーには他にも教員が作成した進路指導および授業用の資料等に関するデータも一部保存されていたものの、外部への流出は確認されていないとしています。

AUS便りからの所感等

- 感染が発生したネットワークは校内でのみ構成されており、他の市立学校の教育用・校務用ネットワークおよび市行政情報システムへの影響は現在のところ確認されていないとのことです。

- ランサムウェアについては一時期に比べ頻繁に取り上げられなくなったものの、昨年10月に国内病院の電子カルテシステムに「GandCrab」が感染したケース(AUS便り 2018/10/29号参照)があったり、そのGandCrabも開発終了が宣言される一方でまた異なるランサムウェアが活動したりと、収束する気配はありません。

- ランサムウェアに限らない「マルウェアへ感染しないための対策」として、単にアンチウイルス等を用いるのみならず、PCのOSやソフトウェアを最新のバージョンに保ち全てのセキュリティパッチを適用すること、「万が一の感染時の影響を最小限に食い止めるための対策」として、UTM等を用いたネットワーク構成の適宜分割や外部への不審な通信の遮断等、そして「ランサムウェア感染への対策」として、データの随時バックアップ(オフラインストレージへの保存)等、とるべき対策を可能な限り実施することが重要です。


ScanNetSecurity

インシデント・事故 ／ インシデント・情報漏えい

2019年11月11日（月） 08時00分

市立高校の校内サーバがランサムウェアに感染（川崎市）

神奈川県川崎市は11月1日、市立橘高等学校全日制及び定時制課程にて、生徒の学習等で使用するコンピュータ端末用に構成している校内ネットワーク・サーバがウイルス感染したことが判明したと発表した。

神奈川県川崎市は11月1日、市立橘高等学校全日制及び定時制課程にて、生徒の学習等で使用するコンピュータ端末用に構成している校内ネットワーク・サーバがウイルス感染したことが判明したと発表した。

これは10月28日午前に、同校の職員が端末から校内ネットワーク・サーバにアクセスした際、MS Wordドキュメントが暗号化されており、画面上でランサムウェア型ウイルスの感染を示唆する英文の脅迫ドキュメントを確認したというもの。

ランサムウェアに感染した当該サーバには、生徒が作成した学習成果物のデータや教員が作成した進路指導や授業の資料に関するデータも一部保存されていたが、現時点で外部への流出は確認されていない。また当該ネットワークは校内のみで構成されており、他の市立学校の教育用ネットワークや校務用ネットワーク、市行政情報システムへの影響は現在のところ確認されていない。

トップページ

リリース（川崎市立高等学校におけるコンピュータ・ウイルス感染について）

シェア　ツイート

もっと「お詫び」のニュース

出願用の調査書を誤記帳、大学から連絡があり発覚…

会員向けメールを誤送信、167件のアドレスが流出…

社内パソコンのウイルス感染、複数顧客から不審メ…

編集部にメッセージを送る