標的型攻撃メール訓練での試み

GMOペパボ株式会社
セキュリティ対策室
廣川優

JPAAWG 7th General Meeting
おかわり！ Lightning Talks 2024 発表

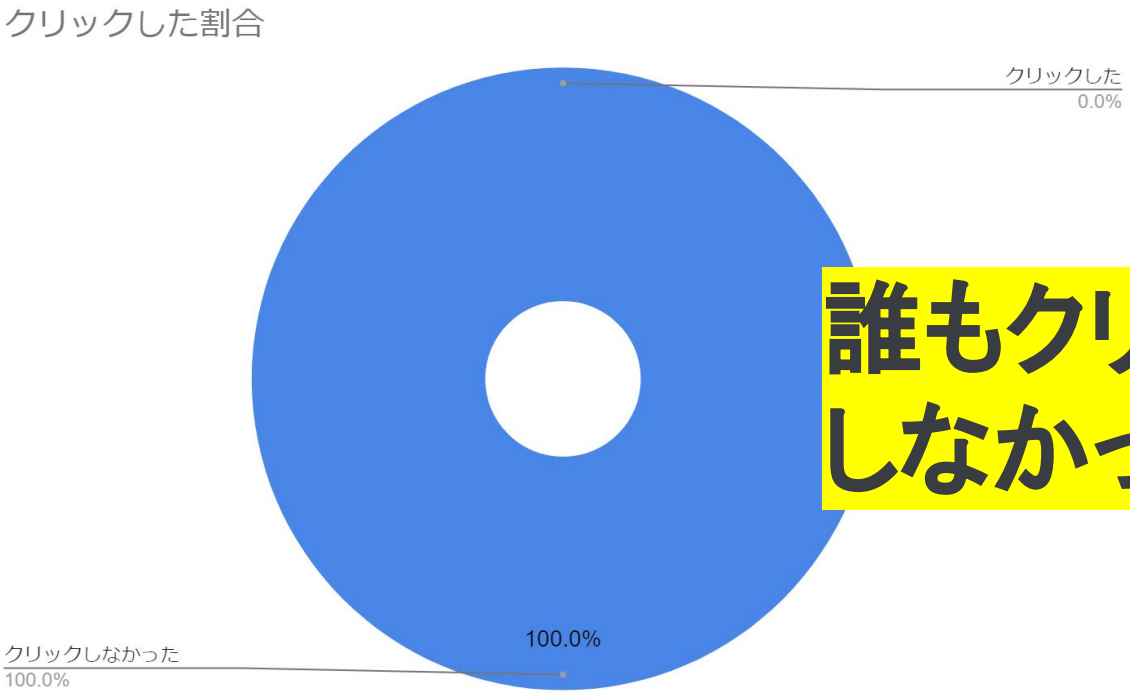
訓練やってますか？

一般的に、訓練の目的は

- 不審なメールを 見抜く目を養う
- 不審なメールを受信した場合の 対応力を身につける

などがある

前回の訓練結果レポート



誰もクリックしなかった!!

※開封通知はありませんでした

これは、、、、皆、

「自分は騙されない、大丈夫！」

と思っているのでは？

と思いました。私。

みんなこう思ってるに違いない

今回の訓練の目的を

標的型攻撃を『自分ごと』として認識してもらう。

と定めました。

目的: 標的型攻撃を『自分ごと』として認識してもらうことで、意識の向上を図る。

訓練の目的

目的: 標的型攻撃を『自分ごと』として
認識してもらうことで、意識の向上を図る。

全員が開くような攻撃メールを送るぞ !!

GMOペパボ

目的: 標的型攻撃を『自分ごと』として
認識してもらうことで、意識の向上を図る。

~~**全員が開くような攻撃メールを送るぞ!!**~~

設計

目的を決めたのでどんなメールを送るのか考える

標的型攻撃を『自分ごと』として
認識してもらうため、ほとんどの参加者が
うっかり開いてしまうようなメールを
送りたい。

人間が適切な判断を出来なくなるのは
どんなときか？

人間が適切な判断を出来なくなるのは

- 怒りを感じたとき
- 時間に追われている時
- 前に叱られたのと同じ状況になった時

など

普段から、指示が出たらすぐに対応するよう
言われているようなもの（時間・過去の叱責）

今よりネガティブに感じる労働環境の話

こういうネタを入れると良さそう

会社のポータルサイトに情報が掲載されると
同時に送信されてくるお知らせメール。

時々重要なことが書かれていて、
見落としていると叱られちゃう。

ここに、

「リモートワーク終了のお知らせ」

を組み合わせたら ....

僕だって開いちゃうかもしれない。

文面は、実際にポータルから送られている
メールのフォーマットを流用し、
内容とリンクを差し替えました。

ポータルからのメールは時期 (時代)によって、
タイトルのルールが異なるのですが
あえて少し古いメールを流用しました。

最新のルールを適用しなかった理由

1. 以前に漏洩したメールを攻撃者が流用した、
   というシナリオだと現実味がありそう
2. ポータルの事務局に叱られたから

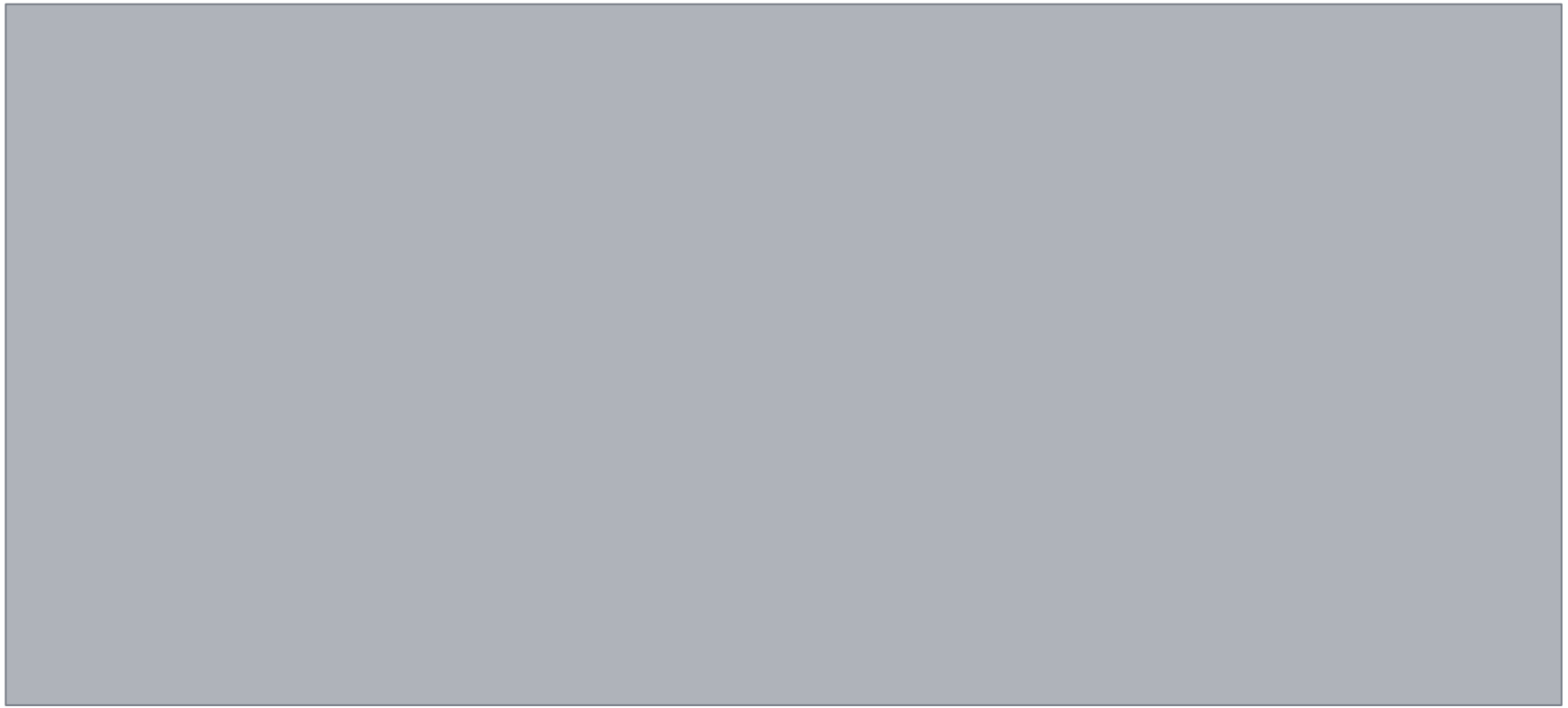
どんなメールを送るか

お疲れ様です。[redacted]になりすましたメールによるメール訓練実施に向け、関係者をご招待させていただきました。
お忙しいところ恐縮ですが、よろしくお願いいたします。

早速ですが、現在想定していますメール内容を添付にて共有いたします。[redacted]事務局として内容についてお気づきの点・気になる点などございますでしょうか？

件名と本文の頭の部分を[redacted]からの全体連絡メールと同じにはしたくないです！内容的に絶対見たくなる文面なので。本物のメールの開封率を下げたくないので、修正案を一応作ってみました。担当の部署名も、実際には存在しない部署名にした方がいいのでは？と思いました

出来た文面



1. 訓練メールの送信元を SaaSの
   セーフリストに追加
2. 情シス部門への情報連携
3. 事後アンケートの作成
4. 不審なメールを受信したときに取るべき
   行動手引きの周知

いざ実食実送

カタカタカタカタカタカタ
カタカタカタ

ポチッ

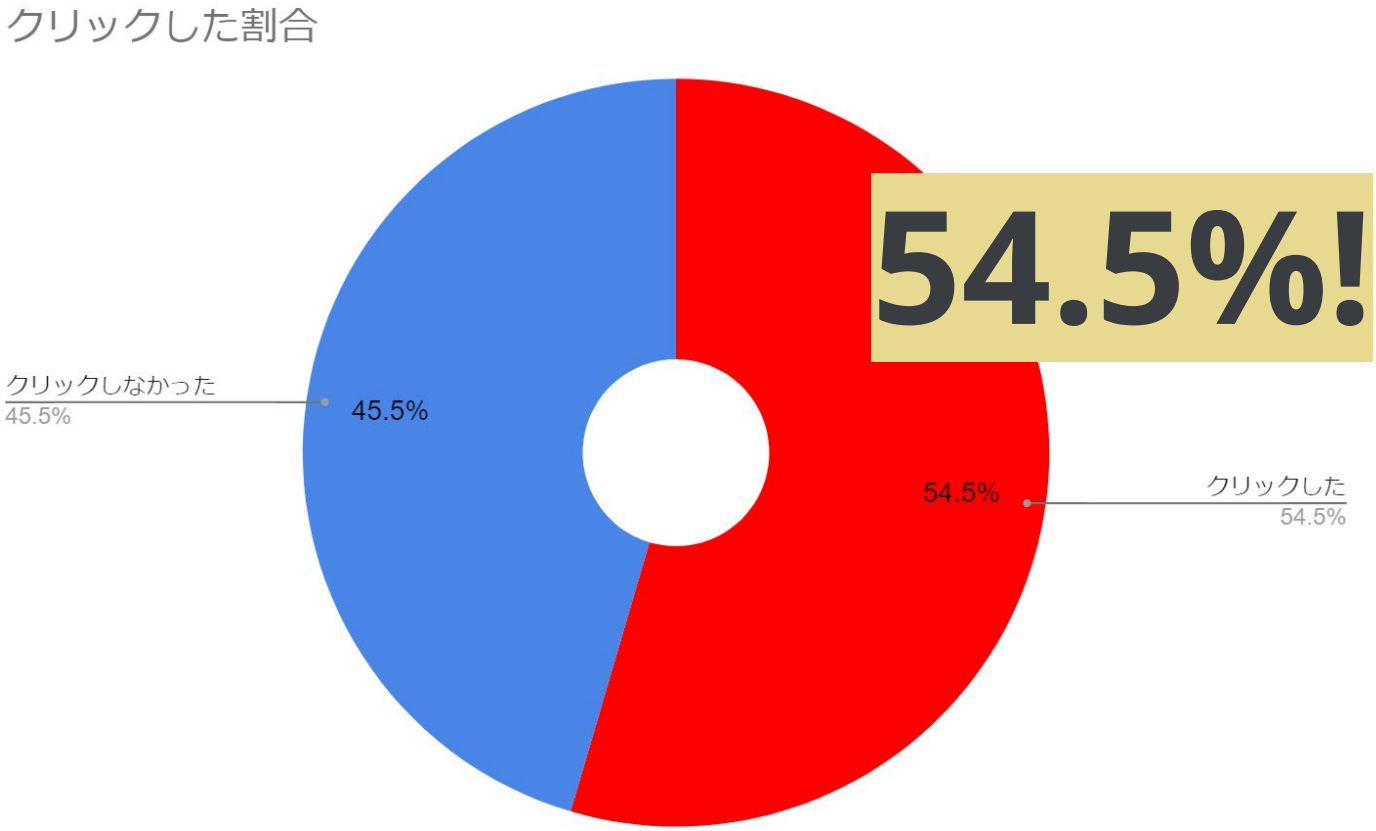
お問い合わせとか来るかなぁ

ポータルの事務局も対応の体制を
敷いてくれているけど
大丈夫かなぁ(不安)

訓練対象者からの問い合わせ
→ なし

事務局への問い合わせ
→ なし

訓練結果



事後アンケート

[redacted] メール訓練アンケート [redacted]

You created this channel today. This is the very beginning of the # [redacted] メール訓練アンケート [redacted] channel. 標的型攻撃メール対応訓練の事後アンケート回答チャンネルです。 [redacted]
[redacted] (Edit description)

Add coworkers | Send emails to channel

Today

[redacted] 11:55 AM

@channel お疲れ様です。標的型攻撃メール対応訓練Weekを終えての事後アンケートにご回答ください。
アンケートの回答を以て訓練の完了となります。アンケートはDescription か Bookmarks からアクセスしてください。
回答期限を [redacted] としておりますのでご回答よろしくお願いします。
不明な点はこのチャンネルにて(このポストへの**リプライではなく**新規の発言にて)お尋ねください。

回答後はleaveしていただいて構いません。

1 | 済 1

攻撃メールに気付いた方へお尋ねします

メールをどのように扱いましたか？ *

開いたがリンクのクリックはしなかった

どのような特徴から攻撃メールだと気付きましたか？ *

担当部署を聞いたことが無い。**リンクのURLが本文に記述されているものと異なる。**

どのような特徴から攻撃メールだと気付きましたか？ *

最後まで気づきませんでした…

全く気が付かなかった

開いたので気付いた・・・

普通に内容を確認しようと思ってみたかんじでした。

まとめ

- 標的型攻撃を『自分ごと』として認識してもらうことが出来た
- 具体的な部署名・個人名などなくても人はついメールを開きクリックする
- 関係部署との連携は大事

ご清聴ありがとうございました