平成２９年８月２日

不正プログラム関連情報
～フィッシング詐欺を見抜くためのポイント～

※　先日の鳥取県サイバーセキュリティ対策ネットワークの合同専門分科会で「不正アクセス等を防ぐ方法は、気付く方法は・・・・」旨の御質問があり、同分科会参加の皆様から参考意見等を賜ったところですが、見出しのニュースがインターネット内に掲示されていましたので、参考として送付させていただくものです。

鳥取県警察本部サイバー犯罪対策室

○　トレンドマイクロ社が新着記事として、2017 年 7 月 27 日に記事公開

- 掲載アドレス～https://www.is702.jp/news/2183/partner/101_g/
- 題名「すぐに役立つ！フィッシング詐欺を見抜くためのポイントとは？」

○　記事内容の概要（上記アドレスの記事を引用）

・　「フィッシング詐欺」は、一見本物に見える電子メール（フィッシングメール）により、不正サイト（フィッシングサイト）へ誘導し、利用者自身に氏名や住所、アカウントやパスワードを入力させ、情報を詐取する詐欺です。

　古典的な手口ですが、現在も深刻な問題となっており、むしろその被害は拡大の一途をたどっています。

・　銀行やクレジットカード等の金融機関の情報以外にも、Amazon・Ｐaypal のようなネットショッピングや決済に関わるサービス、Facebook・Twitter 等のようなソーシャルメディア、Apple ID・Google アカウントのようなマルチサービスアカウント、クラウドサービス、Web メールのアカウント等、幅広い情報が近年はターゲットになっています。

・　典型的なフィッシング詐欺は､まずフィッシングメールを受け取るところからスタートします。知人や実在企業からの連絡を装い、リンクをクリックさせ、外部サイトにアクセスさせ、そこで情報を詐取しようとします。ただし、的確なセキュリティ対策を導入し、注意深く観察すれば、真贋を判別することはある程度可能でしょう。

・　フィッシング詐欺に対する「注意点」「違和感」としては、以下があげられます。日頃からこれらのポイントを確認する習慣を付けてください。

<u>【見抜くためのポイント】</u>

①　「個人情報や認証情報を安易に要求してくる」メールに用心する。

②　リンクをクリックする前に､ＵＲＬの上にマウスカーソルをかざして表示される「参

照先」を確認する。

③ 「心当たりがないタイミング」で、勝手に送られてくるメールは非常に疑わしい。

④ 「登録したものと異なるアドレスに届いたメール」は、一斉配信されたスパムの可能性が大。

⑤ 「期限を区切って早急な対応を求める」「威圧的・脅迫的な内容」のメールも危険。

⑥ 「普段と異なるドメイン」から送信されたメッセージは危険信号。Ｗｅｂ検索で確かめるのもよい。

⑦ 「あいさつ文がない、個人名を書いていない等、普段と異なる書式」のメッセージは危険信号。

⑧ 「画像を読み込まない」「表示がくずれている」メッセージは危険信号。

⑨ 文法間違いやスペルミス等、「不自然な文章」のメッセージは危険信号。

⑩ 「無意味な文字列」のメールタイトルは、通常ありえない。

⑪ 自身が使用しているメールクライアントの機能を再確認し、不審メールはブロックする。

⑫ 日本の銀行、クレジットカード会社等の金融機関は、基本的にメールによる口座番号や暗証番号、本人確認は行っていない。

⑬ 会員番号を使用しないサービスから会員番号を含むメールが送られてきた際には注意が必要。

⑭ 個人情報を扱う正規サイトでは、通常「ＨＴＴＰＳ」通信が使用され、ブラウザに錠前マークが表示

○　その他

本件マイクロトレンドの記事については、「フィッシング対策協議会」のホームページにも本年７月 31 日に紹介されています。