

サイバーセキュリティ関連情報（4月号）

鳥取県警察本部サイバー犯罪対策課

○ 不正広告で誘導する日本郵便を偽装した当選詐欺サイトを確認

トレンドマイクロは、4月2日前後から日本郵便を偽装する不審サイトを確認したと報じた。この不審サイトは、いわゆる「当選詐欺」サイトであり、最新スマートフォンの当選を理由に最終的に個人情報からクレジットカード情報までを入力させ、詐取することが目的と考えられ、調査の結果、この当選詐欺サイトへの主な誘導経路は不正広告であることも確認したと伝えている。

犯罪者はインターネット利用者の金銭や個人情報を狙い、次々と新しい手口を繰り出しています。これに対し、利用者は今回のようなネット詐欺の最新手口を知り、だまされないようにすることが重要です。



図：今回確認された当選詐欺サイトの表示例（Android からアクセス）

正規サイトと誤解させるよう「post」という単語を入れたり、「.co.jp」と誤解させるよう「.co/jp」という文字列を URL に入れている

出典元URL <http://blog.trendmicro.co.jp/archives/17205>

○ 不正プログラム感染を確認するためのウェブサイトを公開

JC3（日本サイバー犯罪対策センター）では、不正送金やクレジットカードの不正使用等の犯罪被害につながるインターネットバンキングマルウェアによる感染拡大及びこれによる被害の防止のため、DreamBot又はGozi又はRamnitへの感染状況を確認するためのウェブサイトをホームページ上で公開し、試験運用している。

インターネット利用者は、不正プログラムに感染していないかどうか本チェックサイトで確認するなどにより、犯罪被害の防止を図ってください。



出典元URL <https://www.jc3.or.jp/info/dgcheck.html>