



ウイルスメール「エモテット」に注意!

「Emotet (エモテット)」と呼ばれるコンピュータウイルスを使ったメール攻撃が再び発生しています。

感染すると、パソコンを乗っ取られるだけでなく、メール情報が流出して、関係先にウイルスメールがばらまかれてしまいます。

【ウイルスメールの例】

送信者名は、取引先等になっているが、送信者メールアドレスが異なる

よく使われる件名、返信を装う

ワードまたはエクセルが添付されている!

よく使われる文面

差出人: 株式会社●●商事 <marumaru@xxxx.or.jp>
 送信日時: 2020年9月1日 17:35
 件名: Re:第●回定期会合の開催について
 添付ファイル: 20200901_第●回定期会合次第.doc

関係会社各位
お世話になっております。
標記の件、例年とお開催することとなりましたので、式次第を送付します。
業務ご多忙中と存じますが、ご出席のほどよろしくお願いいたします。

株式会社●●商事
佐賀太郎

ちょっと待った!!



この表示が出たら要注意!



! セキュリティの警告 マクロが無効にされました。

コンテンツの有効化

ウイルスに感染するので絶対にクリックしないでください!

～ 被害に遭わないために気をつけること ～

- ・ウイルス対策ソフトを導入し、最新の状態に更新して使用する!
- ・返信メールに見えても安易に添付ファイルやURLをクリックしない!
- ・添付ファイルの「コンテンツの有効化」をクリックしない!

参考: 独立行政法人情報処理推進機構 (IPA)
エモテットと呼ばれるウイルス 右のQRコードをご確認ください。





サポート詐欺に騙されないで！！

サポート詐欺とは「パソコンがウイルスに感染している」など偽の警告画面を表示させてユーザーの不安をあおり、画面に表示された電話番号に電話をかけさせ、パソコンを遠隔操作するソフトをインストールするように促し、有償のサービス契約に誘導する詐欺の手口です。

ウイルス！？
電話しないと！



※※セキュリティ警告※※

エラーコード：#00XX
お使いのコンピュータはウイルスに感染しています。

サポート窓口（050-〇〇-xx）

「トロイの木馬に感染しています」などの警告表示

企業の実名とサポート問い合わせ先の電話番号を表示

ピー！
ピー！

サポート窓口で～す



～ 被害に遭わないために気をつけること ～

- 警告画面や警告音が出ても慌てず、電源を切る
- サポート窓口で電話をしない
- 電子マネーの支払いやクレジットカード情報の入力には応じない
- ソフトをインストールしてしまった場合には、アンインストール、システムの復元を検討する（メーカーへ相談をする）

参考：一般社団法人日本サイバー犯罪対策センター（JC3）
サポート詐欺の手口（動画解説）右のQRコードをご確認ください





料金確認の偽メールに注意!

【 偽メールの例 】

< 050-XXXX-XXXX

SMS/MMS
10月1日(月)12:30

〇〇〇お客様センターです。
ご利用料金のお支払い確認
が取れておりません。
ご確認が必要です。

<https://〇〇〇.net/index.html>

偽サイト

携帯電話会社を装ってメールを送り、偽サイトに誘導してID・パスワード等の情報を入力させてだまし取る手口です。

情報を入力してしまうと、利用しているサイト、サービスに不正ログインされ、ネットで高額な買い物をされるなどの被害につながります。



被害に遭わないための対策

- ・メール添付のURLをクリックしない
- ・ウイルス対策ソフトを導入する
- ・サービスごとのパスワードと多要素認証を設定する

だまされないぞ!



偽メール、偽サイトは、実在の企業名とロゴを使っており、見分けるのは困難です。全ての受信メールに注意を払い、安易にURLに接続しないようにしましょう!

参考：日本サイバー犯罪対策センター（JC3）
最新の脅威具体例 <<https://www.jc3.or.jp/threats/>>