リニューアル版
ラップニュース

VOL.229
2022.4.1
発行：ラップ東京株式会社
https://www.raptokyo.co.jp/

◎ラップ東京では、皆様のお役に立てるような様々な内容のコラムを発信しています。　バックナンバーは www.raptokyo.co.jp から

「再・注意喚起」

「最近、変なメールが届く」とあるお客様から問合せがありました。よく聞いてみると、いわゆる迷惑メールで、私自身も最近、「迷惑メール（スパムメール）」がとても多くなっていると感じます。私のメールアドレスが様々なところに公開されていることもあり、日々数十通は届きます。多くはセキュリティソフトが「迷惑メール判定」をしてくれるのですが、送信者も送信元サーバを常に変更して送ってくるので、セキュリティソフトとスパムメールのイタチごっこのような状況です。

その中でも、「アマゾン」、各クレジットカード会社、ETC カードなどが多いように思います。カードのご利用状況の確認をお願いします、とか、個人情報の確認をお願いします、といった文面です。アマゾンを語るメールでは、「あなたのカードで買い物をされましたので、下記アドレスから確認をお願いします」と記載されているので、少々、焦ってしまいました。文面内には購入者の氏名、住所、電話番号などが記載されていて、一見、本物みたいです。メールに記載してあるリンクからではなく、ブラウザからアマゾンにログインして確認したところ、購入などされておりませんでした。（※メールに記載されているアドレスをクリックしてログインすると、IDやパスワードを盗まれてしまいますので注意してください。）

仕事柄、私は調べ方が少しわかるので、どこから迷惑メールが送信されているのかを確認してみると、世界中から発信されているのがわかります。

まずは、差出人のメールアドレスをよく確認してみてください。本物のアドレスに非常に似ているものもあります。少しでも怪しいと思ったら、削除してください。

また、メールアカウントを奪取される被害もあります。その場合、そのサーバから数万通のメールを勝手に送信されてしまい、多くは未達のメールとなって自分自身に戻ってきます。結果、そのメールを送信したサーバは迷惑メールの送信者として「登録」され、しばらくの間メールを送信できない事態になります。メールアカウントを奪取されないようにするためには、まず、パスワードを複雑なものにしてください。

先月のラップニュースでお知らせしたウイルス「エモテット」は、まだまだ猛威を振るっています。先月だけで、当社の取引先４社ほどが感染しています。身近にこれだけ感染してしまった会社がいるので、全体で考えると物凄い数だと思います。「エモテット」に関しては、ラップニュース２２８号に記載してありますので、参考にしてください。

当社もウイルスチェックはしっかり行っているつもりですが、それでも感染してしまうことがあります。（感染してしまうことが悪いことではなく、そのようなウイルスをまき散らす人たちが悪いのです！）明日は我が身です。より一層の危機意識をもってメール確認をしていきましょう。

ご案内

エモテットの確認方法は

「警視庁　エモテット」で検索

Emotet（エモテット）感染を疑ったらというページに感染の有無を調べる方法が掲載されています。

他、詳しい情報はこちらもご覧ください。

一般社団法人
JPCERT コーディネーションセンター
https://www.jpcert.or.jp/