

パソコンいわくら教室新聞

年末に向けて段々と慌ただしくなるこの時期。通年そうなのですが、やはり気をつけたいのは、迷惑メールや詐欺メールです。その時、どう対処すればよいのでしょうか。

なぜ届く？

身に覚えのない「迷惑メール」や「詐欺メール」が、メールアドレスや電話番号を教えたわけでもないのに、なぜメールやSMS（電話番号宛のショートメール）で届くのでしょうか。

メールアドレスや電話番号を指定して届くわけですから、何らかの方法で知られてしまっているわけです。では、どうやって…。それは、

- ①名簿が出回っている
- ②パソコンがウイルスなどに感染した
- ③自らネット上に情報を表示している
- ④誘導されるままに安易に入力してしまった
- ⑤知られたわけではなく、適当に送られたメールがたまたま自分のアドレスだった
- ⑥登録している企業などがサイバー攻撃されたり情報漏えいが起こった

などが考えられます。

この中の①⑤⑥はこちらからは防ぎようがありますが、それ以外は注意すればある程度防ぐことができます。②はOSのアップデートを怠らないこととウィルス対策ソフトの導入です。③はSNSなどで安易に個人情報を表示するよう

なことはしない。④はメールで届いた案内に従つてしまい、情報を入力してしまう「不注意」が招くことですので、安易にメールを信用しないことです。メールで「アカウントの情報を確認したい」などの内容で入力ページに誘導し入力をさせる常套手段です。必ず送信先のメールアドレスを確認することと、正式の手続きではこのようなことは行われないので、誘いに乗らないことです。必ず正規のページを確認してください。

このように、悪者はあの手この手で個人情報を盗もうとしますので、注意しましょう。



届いてしまつたら？

詐欺メールと思われるメールが届いてしまつたりどうするべきでしょか。「無視し削除」です。が、そのメールが詐欺なのか？をある程度判断する方策も覚えておくと良いでしょか。

送信元のアドレス、宛先、本文の内容、それに注意が必要です。

①差出人のアドレスを確認する。全く関係のないアドレスが表示されているなら詐欺メール。

②アドレスが1文字違うなど、アドレスをよく確認します。

③宛先に自分以外のアドレスが表示されている。正しいメールなら、この手のメールを複数人宛に送付されることがあります。

④本文の文章に不審な言い回しがないか、またリンクも正しいものかを確認します。リンクをポイント（クリックせずにマウスポイントを合わせること）するとリンク先のアドレスが表示されますので、正しいものかを確認します。

では、詐欺メールとわかるとやつてはいけないことは、

- ①絶対返信しない、問い合わせしない。
- ②添付ファイルは絶対開かない。
- ③メール本文中にある「ト」をクリック」などのリンクは開かない。

少し注意してみましょう。

アドレス漏れてない？

メールアドレスが漏洩していないか？を調べることができます。（100%ではありませんが）調査できるサイトにアドレスを入力するだけです。もし漏洩してたら、そのアドレスは使わないようにするか、パスワードを変更したり、認証方法を見直したり、対策を考えましょう。

<https://monitor.firefox.com>

Firefox Monitor ホーム データ侵害 セキュリティの状態 ログイン

オンラインのデータ侵害に含まれていないか確認します。

ハッカーが既にあなたについて知っていることを調査しましょう。一歩先に行方を探してみます。

メールアドレスを入力してください
データ侵害を確認する

についての結果 kishi.toshiyuki@gmail.com
このメールアドレスは 3 個の既知のデータ侵害があります。

新しい侵害があった場合に通知する。

Adobe レポート提出された日: 2019年12月4日
提出者: ハッカ
IP アドレス、端末名
この侵害について詳しく見る

Last.fm レポート提出された日: 2016年9月20日
提出者: ハッカ
IP アドレス、メールアドレス
この侵害について詳しく見る

