こんなメールは要注意！

埼玉県教育委員会

スマートフォンなどを使っていると、さまざまなメールが送られてきますが、中には個人情報をだましとることなどを目的とした危険なメールもあります。被害にあわないために、その手口と対処法をしっかりおさえておきましょう。

危険なメールによる手口

危険なメールの手口としてよく見られるのが、**実在する企業等になりすまして不安をあおるようなメッセージを送り、偽サイトに誘導して個人情報を入力させる**というものです。

差出人：“◆◆◆◆”<××××@◆◆◆◆.com>
件名：<緊急！◆◆◆◆重要なお知らせ>

こんちには

アカウントで異常な動作が検出されたため、お客様の資産への損害を防ぐためにアカウントをロックします。ご不便をおかけして申し訳ございません。

できるだけ早くアカウントを復元するために、下のリンクをクリックして公式サイトに入り、画面の指示に従ってください。

https://××××/◆◆◆◆

「◆◆◆◆」の部分には、携帯電話事業者や宅配業者、ゲーム会社など、**実在する企業等に似せた名前**が使われています。

このURLリンクをクリックすると、**本物そっくりの偽サイトが開かれ、個人情報を入力するよう求められます。**

他にもよく見られる危険なメールの手口としては、流出した個人情報を使って**受信者の知り合いになりすまし、添付ファイルを開くよう誘導して、開いた機器をウイルス感染させる**といったものがあげられます。

被害を防ぐための対処法

危険なメールによる被害を防ぐためには、スマートフォンなどの**インターネット機器にウイルス対策ソフトやフィルタリングサービスを導入する必要があります。**

加えて、自身でも以下のような点に気をつけてください。

◆不審なメール、及びメールに添付されたファイルは開かずに削除する。
◆あやしいメールを受信した場合は、文面の一部をインターネットで検索して、被害報告がないか確認する。
◆不安をあおるようなメッセージが送られてきても決してあわてず、まずはそのサービス等を利用したことがあるか冷静に考え、利用した覚えがない場合はメールを削除する。利用した覚えがあっても、URLリンクや添付ファイルは絶対に開かず、公式サイトに問い合わせて、本物かどうか確認する。

ウイルス対策ソフトやフィルタリングサービスの導入に加えて、自身でできる対処法を実践してください。

※本資料は、埼玉県教育委員会の委託により、ポールトゥウィン株式会社が作成したものです。