

不正アプリについて

スマートフォンでは、アプリをインストールすることで、利用可能な機能を増やすことができます。しかしアプリの中には、機器に入り込んで不正な行為をする不正アプリも存在しており、不正アプリをインストールしたことにより被害を受けてしまった人も出ています。

不正アプリをインストールさせようとする手口

インターネット上にいる犯罪者はあの手この手を使って、スマートフォンの利用者に不正アプリをインストールさせようとしています。その代表的な手口としては、以下のようなものがあげられます。

- ・偽の警告画面からの誘導
「ウイルスが検出されました」といった偽の警告メッセージを表示し、ウイルスを除去するアプリと称して不正アプリをインストールさせようとする
- ・メールやショートメッセージを使って誘導
宅配業者などの実在する企業や個人を装ってメールやショートメッセージを送り、そこに記載したリンクから不正なサイトへと誘導して、不正アプリをインストールさせようとする
- ・人気のアプリを装う
人気のアプリに似せた名前やアイコンを使って、不正アプリをインストールさせようとする

○○○○でウイルスが検出されました

お使いの○○○○のウイルス感染が検出されました。対応策をとらないと、SIMカード、写真、および連絡先がまもなく破損します。

ウイルスを今すぐ除去

お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。下記よりご確認ください。

<http://○○○○○○○○○○>



○○Music

インストール

こうした手口に引っかかって不正アプリをインストールすると、電話帳に登録している連絡先や、保存している画像や動画、SNSのパスワードなどを抜き取られるといった被害にあう可能性があります。

不正アプリの被害にあわないために

不正アプリの被害にあう危険性を減らすためには、以下のような対策が有効です。

- ・スマートフォンにセキュリティソフトを導入する
- ・アプリのインストールは公式ストアからだけにする
- ・提供元が不明なアプリはインストールしない
- ・インストールする前にそのアプリをインターネット上で検索し、不正アプリとしての報告がないか確認する
- ・アプリの内容から考えると不必要な情報へのアクセス許可を求められたときは、インストールを中止する
(ゲームアプリなのに電話帳や現在地へのアクセス許可を求められた、など)



不正アプリをインストールさせるための手口にはどのようなものがあるのか、不正アプリの被害にあわないようにするためにはどのような対策が有効なのかを、子どもたちにきちんと理解させておくことが大切です。