12

スマートフォンのアプリで、架空請求メールが届く

最近はやりのスマートフォンですが、パソコンに比べると、技術的にも利用者の意識的にも安全対策が甘い点を突かれて、架空請求や情報の盗難・漏洩などのトラブルが起こっています。

たとえば、アンドロイドOSのスマートフォンでは、一般のサイトで配布している「動画の再生」のアプリをインストールしたら、サイト利用料金を請求する画面が出て、後日、メールなどでも請求が届くようになった事例があります。**このアプリには、架空請求の画面を表示したり、電話番号やメールアドレスなどの個人情報を収集して外部に送信する機能が組み込まれていました。**架空請求を狙った悪者がつくったのは間違いないでしょう。

似たような事例として、**スマートフォンのメールアドレスを誰にも教えていないのに、アプリをインストールしたら広告メールが届いたり、アドレス帳に登録している全員に同じ広告メールが届いた**という話もあります。

スマートフォンのアプリを配布する公式のサイトの場合には、事前に内容の審査をするので、こうした不正な機能が組み込まれたものが公開されることはめったにありません。

しかし、それ以外のものは、どのような機能が組み込まれているかは利用する人それぞれが判断して自己責任で使うことになります。そのことを知らないでいると、悪者に騙される危険性があります。

昔はパソコンでも同じような不正行為がありましたが、セキュリティソフトがチェックしてインストールや動作ができないようにしたり、検索エンジンがチェックして警告の表示を出すなどの仕組みが整うにつれて被害が出なくなりました。

スマートフォンでも同じような取り組みは始まっていますが、まだ成果を上げるほどには機能していません。そもそも**スマートフォンに、セキュリティソフトを組み込んでいない人も多い**のが問題です。

もう一つ、悪者がスマートフォンを狙う理由があります。個人持ちのスマートフォンを仕事でも使うことを認める企業が増えているので、「**スマートフォンから企業の重要な情報を盗み出しやすい**」と悪者が考えているのです。会社のパソコンでは、個人が自由にアプリをインストールすることを禁止したり、個人的な用途でパソコンを使うことを制限する企業が増えています。ところがスマートフォンでは、利用者が気楽にアプリをインストールして試すのが主流になっています。インストールしては試して、満足で

分かったら、すぐに消す人も多いでしょう。一カ月も前に試したアプリが何だったか、覚えていないかもしれません。

こんなやり方で試したアプリの一つが、スマートフォンの内部の情報をこっそりと外部に送信する不正アプリだったとすると、情報を盗まれたことに気がつかないうえに、「**どのアプリで盗まれたかを調べることもできない**」という状態になってしまいます。

スマートフォンのアプリの新作情報を見ても、**すぐに飛び付いてダウンロードするのはやめましょう**。最初に提供者（作者や企業）、機能や使い勝手などの評判を確認し、評判情報が少ない場合には警戒したほうがいいでしょう。

また、アプリを利用するなら、ダウンロードした場所（ＵＲＬ）、インストール・アンインストールした日付などを記録しておくといいでしょう。

ここがPOINT!

用心もせずにスマートフォンでアプリを試しまくると、架空請求や個人情報盗難、重要情報の漏洩などのトラブルに巻き込まれます。