サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和2年
5月14日
Vol.44

自治体等の正規サイトを装った偽サイトに注意！

実在する自治体や企業を装った、正規サイトにそっくりな偽サイトの存在が全国的に確認されています。

サイト上でメールアドレス、ID・パスワード等の個人情報を入力すると、その情報が窃取される可能性があります。

偽サイトの特徴

・内容はそっくり！

偽サイトは正規サイトと同じ内容で、見分けが付かない。

・ドメインが違う！

URLのドメインの最後の「.jp」が「.tk」や「.gq」等の見慣れない表記になっている。

【例】http://www.〇〇.××.▲▲/

この「▲▲」の部分に

「tk」「ml」「ga」「cf」「gq」等

が使用されている。

対策

・まず、URLを確認

正規サイトのURLと異なる点がないか、よく確認する。

ログインや申請等で情報を入力する時は、再度確認する。

・次にドメインを確認

日本の自治体が使用する「.jp」ではなく「.tk」等ではないか、「.jp」でも、その前の部分に異なる所がないか、よく確認する。

・基本は「ブックマークから」

利用しているサービスは、ブックマークに登録しておく。

今後、自治体や企業を装って送信された偽のメールやショートメッセージ(SMS)に記載のリンクをクリックすることにより、偽サイトに誘導され、ＩＤ・パスワード等の個人情報が窃取される可能生があります。

そんな時のために、日頃から・・・

1　**不審なメールは無視！**
身に覚えのないメールは無視し、不安をあおるメールに惑わされない。

2　**リンクはクリックしない！**
リンクの表記は偽装できます。クリックしないことが一番の対策。

3　**添付ファイルは開かない！**
添付ファイルにはウイルス感染の危険性があります。送信元に確認を。

4　**ブックマークから！**
メールの内容について確認したい時は、ブックマーク等から正規サイトにアクセス。

相談窓口

愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110㈹