サイバーだより

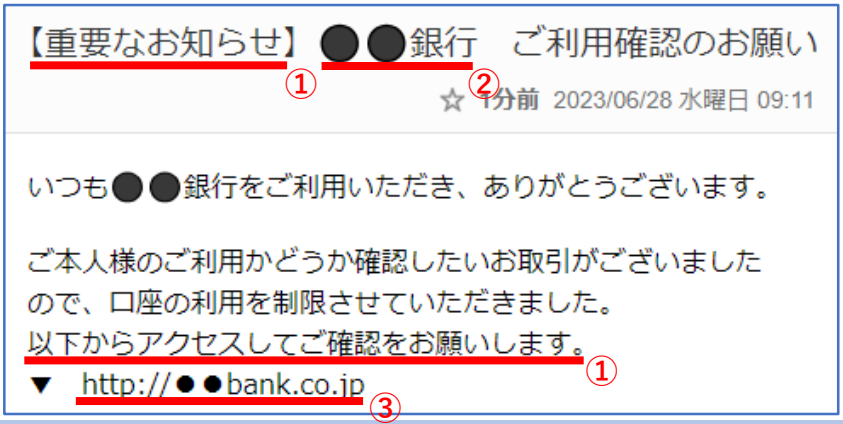
栃木県警察本部
サイバー犯罪対策課
令和５年７月

フィッシング詐欺に注意！！

フィッシングとは、実在する組織を騙って、個人情報を盗むことです。
メール（SMS等）のリンクから正規サイトに似せた偽のサイト（フィッシングサイト）に誘導し、個人情報を入力させて情報を盗みます。
盗まれた情報は不正に使用され、多くの場合金銭的な被害が発生します。

フィッシングメール（SMS等）に注意！！

・フィッシングメール（例）



フィッシングメールの特徴

①「重要なお知らせ」や「至急」等と件名に入れて不安にさせ、リンク先へ誘導する

②銀行・クレジットカード会社・通信販売会社等、様々な企業や団体等の名前が使われる

③フィッシングサイトのリンクが貼られている（見た目だけで正しいと判断できない）

フィッシングサイトは正規サイトにとても似ています

・フィッシングサイト（例）

フィッシングサイトの特徴

①URLが正式なサイトと異なる

②ロゴは正式なもの使い、表記や項目も酷似していて正規サイトと見分けづらい

③口座番号・クレジットカード番号・ID・パスワード等個人情報に関する入力フォームがある

被害に遭わないためには

○　メールのリンク（URL）からウェブサイトにアクセスしない
○　条件反射でID、クレジットカード情報、パスワード等を入力しない
○　普段使用しているアプリやブックマークからサイトにアクセスする

栃木県警察
Tochigi Police