サイバーセキュリティ通信【第27号】

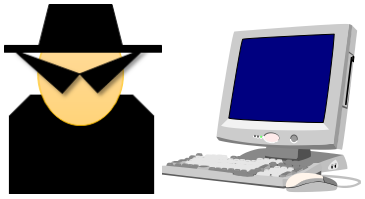
令和2年12月
大分県警察本部生活安全部
サイバー犯罪対策課

フィッシングによる重要情報の窃取に注意！！！

「フィッシング」により、ネットバンキングのＩＤ・パスワードや、クレジットカード情報等の個人情報が盗まれ、不正に利用される被害が後を絶ちません。
「フィッシング」とは、銀行やクレジットカード会社の正規ホームページサイトに似せて作られた偽物のサイトに、重要情報等（ＩＤ・パスワード・クレジットカード情報・銀行口座情報など）を入力させ、盗み取る手口です。
メールやＳＭＳ（ショートメッセージサービス）に添付されたＵＲＬにアクセスすると重要情報等を盗み取る偽物のサイトに誘導されることから、安易にアクセスして被害に遭わないように注意してください。

フィッシング詐欺の流れ

① 実在する金融機関等を装ったメールを送付する

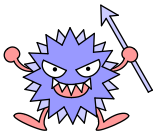


② メールに添付したＵＲＬにアクセスさせる

＜重要＞●▲銀行からのお知らせ
異なる端末からのアクセスを確認しました。
ご利用環境の本人確認のため下記URLから
手続きをしてください。
https://●▲■.xyz.com

④ 口座番号・パスワード等を盗み悪用する

③ 本物とそっくりな偽サイトに誘導し口座番号・パスワード等を入力させる



偽物

●▲銀行オンライン窓口
口座番号
パスワード
ログイン

本物

●▲銀行オンライン窓口
口座番号
パスワード
ログイン

防犯のポイント

→ 重要情報は入力する前に必ず正規サイトで確認しましょう
→ メールやSMSに添付されたURLに安易にアクセスしないようにしましょう
→ このようなメールが来た場合は１人で判断せず警察に相談しましょう

あなたの会社や団体で研修の一環として、サイバーセキュリティセミナーを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。
大分県警察本部生活安全部サイバー犯罪対策課
企画・指導・サイバーセキュリティ係　Tel:097－536－2131