インターネットの防犯対策「サイバーセキュリティ」　～お金と情報を犯罪者から守る～

インターネットはとても便利です。
仕事で使うだけでなく、プライベートで友人と連絡を取り合ったり、ネット通販で買い物をしたりする方も多いでしょう。
多くの人が利用しているインターネットですが、中には、これを利用して、悪いことをしようとしている人たちがいます。
あなたの情報を盗んで、お金を引き出したり、あなたになりすまして詐欺をしたりするのです。
「サイバーセキュリティ」とは、そういう人たちから、身を守ることをいいます。

大丈夫？あなたのパスワード

まずはここから確認しましょう

通販サイトや、スマートフォンアプリを使う際には、多くの場合、「ID」と「パスワード」が必要です。

IDとは「そのサービスを利用しようとするのが誰なのかを識別するためのもの」で、パスワードは「そのサービスを不正利用されないために設定する暗証番号のようなもの」です。パスワードは自宅の鍵と同じ役割を果たします。

この二つはとても大切。この組合せを他人に知られてしまうと、悪用されるおそれがあります。あなたになりすまして預金口座からお金を引き出したり、勝手に買い物をすることもできてしまいます。

これが大切

- **IDとパスワードは、誰にも知られないように、しっかり管理すること。**
- **簡単なパスワードにしないこと。**
  1234、誕生日、電話番号など、推測されやすいパスワードはやめましょう。
  英字(大文字・小文字)、数字を組み合わせ、長く、複雑なものにしてください。
- **同じパスワードを複数のサービスで使い回さないこと。**
  1つのサービスで情報が漏れた場合、被害が拡大することがあります。

フィッシング詐欺にご注意ください

そのメール、大丈夫？

厳重に管理しているはずのパスワードでも、犯人に盗まれてしまうことがあります。

その多くが「フィッシング詐欺」と呼ばれる手口によるもので、近年、被害が増加しています。

あなたのスマートフォンに、こんなメールやSMS(ショートメッセージサービス)※が届いたことはないでしょうか?

〇〇配送です。
あなた宛ての荷物をお届けにあがりましたが、
不在のため持ち帰りました。
再配達の手続きはこちらから
http://www.〇〇haiso/saihaitatsu/

〇〇銀行をご利用のお客様
あなたのキャッシュカードが不正利用されました。
カード停止の手続きはこちらから
http://www.〇〇bank/teishi/

これは、詐欺の可能性があります

犯人が、実在の企業になりすましてメールを送り、偽サイトに誘導することがあります。これに騙されて、犯人の指示に従って手続きをしてしまうと、あなたの情報を盗まれてしまいます。

※SMSとは、携帯電話の番号を宛先にして送るメールのこと。

フィッシング詐欺の流れ

❶犯人から、銀行や宅配業者のふりをしたメッセージが届く
〇〇銀行をご利用のお客様
セキュリティ強化のため、
以下のURLから本人確認をお願いします。
http://www.〇〇bank/security/

❷手続きをしようと、書いてあるURLをクリックしてしまう

❸偽物のサイトへ誘導
本人確認としてIDとパスワード、住所等の個人情報の入力を求める

❹指示にしたがって入力してしまう

あなたの情報が盗まれてしまい、
お金を引き出されたり、なりすましの被害にあったりします

こんなメールが送られてきたらどうすればいいの？

- **身に覚えのないメールには反応しない。**
- **メール内に書いてある連絡先に電話をかけない、URL(ウェブサイトのアドレス)をクリックしない。**
- **銀行やクレジット会社のサイトには、公式サイトや公式アプリからアクセスしましょう。よく利用するサイトは、ブックマーク機能(お気に入り機能)を使って登録しておくのもおすすめです。**

困ったとき、不安なときは お近くの警察署にご相談ください。

特設サイト「ムービーで学ぶ　小島よしおのサイバーセキュリティ教室」では、
今回ご紹介したフィッシング詐欺の手口や、対策について動画で解説しています。
ぜひ、ご覧ください。https://cyber-school.jp/　※令和2年12月末までの期間限定ですのでご注意ください。