

ネットショッピングや
ネットバンキングを
ご利用の皆さまへ

大切な情報を

盗み取られないために。



インターネット・オークション詐欺

次のような被害が発生しています。ご注意ください！

- オークションで落札し、代金を振り込んだが、商品が送られてこない。
- オークションで落札できなかったが、メールで直接取引を持ちかけられ、これに応じ代金を振り込んだところ、商品が送られてこない。
- オークションで落札したものの送られてきた商品が壊れていた、粗悪品であった。

※取引時のホームページやメールを印刷しておくようにしましょう。

利用する際の注意点

- エスクローサービスや代金着払いなど安全な方法で取引する。
- オークション外での直接取引には応じない。
- パスワードは簡単なものを設定しない。
- 相手の銀行口座の控え、振込の控え等を保管しておく。

スパイウェア

もっとも要注意！ 個人情報盗み取る悪質ソフト

スパイウェアは、コンピュータウィルスのようにコンピュータに入り込み、打鍵（タイピング）、画面表示、ハードディスク等から個人情報を取得して、悪意のある者に送付します。

こうして盗まれた個人情報が悪用されて、銀行口座からお金を引き出されたり、クレジットカード決済で買い物やされたりする被害が発生しています。

スパイウェアは不審なソフトウェアをインストールしたり、あやしいサイトやメールの添付ファイルなどから侵入することが多いので注意が必要です。

事例

ネットバンキング会社を装ってスパイウェアを送りつけ、利用者のID・パスワードを盗み出し、利用者の口座から自分の口座へ送金した。（平成17年10月）



対策

- 不審なCD-ROMやソフトウェアは使わない。
- 使っているOSのアップデートをきちんと行う。
- スパイウェア駆除ソフトや駆除機能付きのウィルス対策ソフトを常に最新の状態で使う。

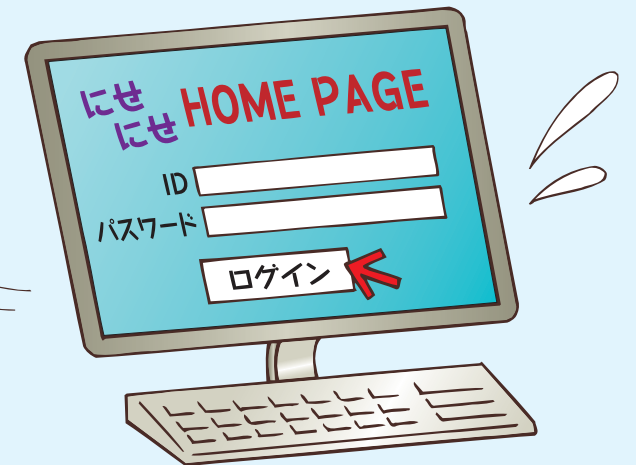
フィッシング

アクセスしたホームページがもし偽物だったら

フィッシング(phishing)は釣り(fishing)のことではありません。実在する金融機関や企業からのメールを装って「セキュリティを強化する。」などの口実をつけて言葉巧みに偽のホームページに誘導し、暗証番号、カード番号、ID、パスワードなどを入力させるといった詐欺の手口のことです。そうして得た情報をもとに偽造カードを作ったりネット決済に悪用して、現金を引き出されたり商品を購入されたりといった被害に遭います。巧妙に造られた偽のホームページにだまされないように注意してください。

対策

- メールやホームページで個人情報を聞かれても安易に答えない。
- 不審に思ったら、104（電話番号案内）等で確認した電話番号に電話するなど、その金融機関等に直接問い合わせる。
- メール本文のURLをクリックしない。
- メールやホームページで個人情報を聞かれても安易に答えない。
- 偽りのホームページを見つけたら、フィッシング110番（サイバー犯罪相談窓口）へ通報する。



インターネットカフェ

消したつもりでもデータは残る

不特定多数の人が利用するインターネットカフェ等のパソコンには、利用者の個人情報を盗むような不正なソフトがインストールされている危険性があります。実際にこの手口で個人情報を盗まれて悪用される事件が発生しています。

対策

- ID・パスワード、金融情報等の個人情報は入力しない。
- ネットバンキングなどのインターネット取引には利用しない。

無線LAN

使用するときにはセキュリティ設定を忘れずに

好きな場所からワイヤレスでネットワークに接続できる無線LANは、使い勝手の良さから利用者が増加しています。無線LANを利用する場合には、セキュリティを適切に設定し盗聴や不正利用の被害に遭わないよう注意してください。

対策

- セキュリティ設定（暗号等）を必ず行う。
- 使わないときはパソコンや無線LANルータの電源をOFFにする。