安心安全ネット社会推進事業

考えよう！情報安全・情報モラル

その３：個人情報の利用について（第２部）

個人情報の利用について、第２部では調査結果などをもとに実際にどのような書き込みがあるのか、携帯電話やスマホなどからどのようにして流出するのか、どのようなトラブルに巻き込まれる可能性があるのかについて考えてみましょう。

個人情報の公開

熊本県では、児童生徒が危険やトラブルに巻き込まれるのを防ぐ目的で、平成２１年度より学校非公式サイトに書き込まれた内容の調査・報告を行っています。今回は、投稿された内容の一部を確認し、問題点を考えてみましょう。

◆ＳＮＳ、コミュニティサイト、ブログ、掲示板への書き込み
- プロフィールに「氏名」「学校名」「学年・クラス」「出席番号」「写真」を掲載
- 自分や友達の写真、体育祭などで撮った集合写真などを投稿
- 無料通話アプリのIDを投稿（QRコードの画像）
- 同級生や自分の名前を投稿、他の学校の友達の名前を投稿
- 教室で撮った先生の写真、名前を投稿
- 友達や自分が映った動画を投稿
- 個人情報が書かれている投稿を自分のサイトに再投稿

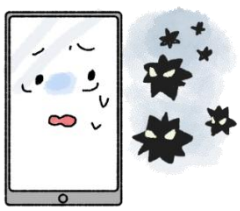
インターネットへの不要な掲載は、個人情報を悪用されてしまう可能性があり、詐欺やストーカー犯罪に巻き込まれたり、なりすましに利用される危険性があります。自分の投稿に個人情報や、個人情報になり得る情報を含んでいる場合は、すぐにでも削除してください。

携帯電話・スマホからの個人情報流出

インターネットに公開する以外にも、携帯電話やスマホから個人情報が流出してしまう可能性があります。細心の注意を払って利用するようにしましょう。

◆　電話帳やGPS機能に不必要にアクセスするアプリなどは、情報を外に漏らす目的のアプリかもしれません。インストール前に確かめてから使いましょう。

◆　ウイルスに感染することで電話帳データ、メールの内容、パスワードなどの情報を盗まれる危険性があります。ウイルス対策ソフトは必ず入れるようにしましょう。



◆　落としたり置き忘れた携帯電話・スマホを悪意のある人が見つけた場合、電話帳やメール内容を見られることで流出する場合もあります。画面ロック、パスワードロックなどで他人に中身を見られないようにしましょう。

熊本県教育委員会　　作成：合同会社ＮＥＷＦＥＥＬ

流出したことで起こるトラブル

■電話番号、メールアドレスが悪用された場合
　出会い系サイトに電話番号やメールアドレスが掲載された。

どうなるか
　出会い系サイトを見たという人から電話がかかってきたり、架空請求のメールや嫌がらせのメールがくるかもしれません。大きなトラブルにならないために携帯番号を変更することも必要になるかもしれません。

■無料通話アプリのIDを悪用された場合
　IDからパスワードを解析され乗っ取られた。IDを掲示板などに流布された。

どうなるか
　悪意を持った人が他人のIDを使ってなりすまし、詐欺や嫌がらせに利用する可能性があります。また、犯罪やトラブルなどに巻き込まれる可能性もあり、そのままにしておくと大変危険です。IDの削除、再取得を検討する必要もあります。

　流出した情報は完全には削除することはできません。簡単に変更できない個人情報は将来的にも悪用される可能性があります。管理には十分注意してください。

考えてみましょう

■何がいけないのか、みなさんで考えてみてください。

①無名のオークションサイトが激安だったので登録して購入した。

②ＳＮＳに無料通話アプリのＱＲコード画像を投稿した。

④スマホの画面ロックが面倒だったので解除した。

⑤友達の個人情報が書かれた投稿を自分のＳＮＳに再投稿した。