個人情報の漏洩にご注意を！

令和３年１月　社会福祉士Ａ

最近、パソコンやスマホに個人情報を盗もうとする不審メールがよく届きます。
パソコンやスマホを良く知らないまま使っている我々世代には、特に注意して盗まれないようにしなければならないですね。
氏名や生年月日、電話番号、メールアドレス、クレジットカード番号、銀行口座情報、各種インターネットサービスの認証情報といった個人に紐づく情報が漏えいし犯罪者の手に渡ってしまうと詐欺や金銭被害などにつながる恐れがあります。
また、流出した個人情報は悪用されるだけでなく、ネット上で取引されたり、暴露されたりすることもありますので十二分の注意が求められます。
その経路と対策について下記にまとめてみましたので、ご参考にして頂ければ幸いです。

《情報漏洩の経路》

① ネット利用時におけるフィッシングサイト。

サイバー犯罪者は実在するショッピングサイトや銀行、クレジットカード会社などの正規ログインページを装う偽サイトにネット利用者を誘導し、そこで入力させた情報を盗み取ります。（つい最近では、楽天やアマゾンの通販サイト名でメールを送られてくるのが多いですね）

② マルウェア感染も情報漏えいのきっかけになります。

たとえば、マルウェアの一種であるスパイウェアに感染した場合、パソコン内の情報やキーボードから入力した情報を外部に送信されてしまいます。
不正アプリをインストールしてしまった場合でも端末内の情報を奪われる危険性があります。

《その対策》

① メールやSMS、SNSのURLリンク、ネット広告を安易に開かない。

・実在する企業や組織、友人が差出人でも、何らかの理由をつけてURLリンクを開かせようとするメッセージに注意すること。

・検索結果に表示される広告の中にも、偽サイトに誘導する広告が紛れ込んでいる場合がありますので、その企業のホームページに掲載される注意喚起情報をチェックしたり、友人に電話や他のチャットなどで直接連絡したりして事実確認を行う事。
・なお、総務省や行政機関から特別定額給付金申請についての案内が直接メールで届くことはありません。

一見怪しくないメッセージが届いた場合でも、金銭や情報の入力を求める内容には十分注意して下さい。

② ネットでの情報入力やアプリのインストールは慎重に行う。

SNS やショッピングサイトなどのアカウントへのログインやアプリのインストロールは必ずブックマークに登録した正規サイトや、公式アプリから行うこと。
ネット上で何らかの情報入力を求められた際は必ず一度立ち止まり、正規サイトかどうか改めて確認する必要があります。

③ セキュリティソフトを最新の状態で利用する。

セキュリティソフトを常に最新の状態で利用し、不正サイトにアクセスしたり、マルウェアに感染したりするリスクを減らしましょう。
また、機器やソフト、アプリの脆弱性を悪用されないためにも、OS やソフト、アプリの開発元からセキュリティに関する更新プログラムが提供された場合は速やかに適用しましょう。

以　上