サイバーだより

令和元年６月２５日

長野県警察本部
サイバー犯罪対策室

情報流出を防止するために
～身近に潜むウイルス感染について～

スマートフォン、タブレット型端末の普及により、これらの情報通信機器は、小学生から高齢者まで幅広い年齢層が利用しています。
しかし、情報通信機器のセキュリティ対策については、あまり意識せず利用されている方が多いのではないでしょうか。
今回は、身近に潜む情報流出のおそれがある経路について、ご紹介します。

流　出　経　路　と　対　策

USB充電ポートは安全？

USB充電ポートが設置されている施設がありますが、誰もが利用できるUSB充電ポートの中には接続された端末から情報を盗み取るためマルウェア（悪意のあるウィルス）が仕込まれる可能性があります。

対　策

信頼できるUSB充電ポート以外では、モバイル端末を接続しない。

モバイルバッテリーを利用して端末を充電する。

フィッシングメール等に注意

昨年来、大手宅配業者をかたるフィッシングメールが送りつけられ、不正アプリのダウンロードや偽サイトへ誘導し、ID・パスワードを盗み取られる被害が多く発生。
手口の多くは、実在する企業をかたり、不在通知を送りつけてきたり、アカウント情報の変更を求めてきます。

対　策

不審なメールに記載されているURLにアクセスしない。

迷惑メール対策ソフト等を活用する。

ワンポイントアドバイス
不在通知メール（フィッシングメール）の見分け方
1　メール本文に入力項目があるときは要注意
宅配業者から送信されるメールの本文中にID・パスワードの入力箇所がある時は、要注意。
また、メールのドメインを確認して、末尾がtop、clubとなっていれば要注意。
2　サイトで確認
大手宅配業者では、なりすましメール対策の一環としてホームページ上で例示を掲出して注意喚起を行っています。
なお、登録しない限り不在通知がメールで届くことはありません。