串木野中学校教頭通信

Kyo to correspondence

～当たり前のことを当たり前に～

号外⑤
令和６年　２月１６日（金）

いちき串木野市立串木野中学校教頭
文責　長岡

あなたのアカウントは大丈夫？

中学生で SNS を利用している人は多いと思います。では，**『SNS アカウントの乗っ取り』**について知っている人はどれくらいいるでしょうか？

SNS やWeb サービスのアカウントを乗っ取られてしまうと**「個人情報の漏えい」「金銭的な被害」「信頼関係が損なわれる」**といった大きな影響をもたらしかねません。

アカウントの乗っ取りとは

パソコンやスマートフォン（以下，スマホ）を用いて，SNS や Web サービス，アプリなどを新たに使用する際，新規アカウントの作成が求められます。アカウント作成に伴い「メールアドレス」「氏名」「住所」「趣味嗜好」「利用用途」といった情報を登録し，アカウントへのログインのための「ID」「パスワード」を設定することになります。ユーザーがこうして設定したアカウントを，第三者が詐取するなどして**「なりすます」**のがアカウントの乗っ取りです。

アカウントを乗っ取られると，その**アカウントを不正に利用されてしまいます**。まずは**基本的な情報がすべて漏洩**することになり，**掲載した写真等も併せて悪用**されるかもしれません。また，知人などつながりがあるユーザーに対して**「不正なメッセージを送り付ける」「虚偽の宣伝を行う」「偏った主張を行う」「他者への誹謗中傷を行う」**ということがあり，ユーザー本人になりすまして**「他者への詐欺を試みる」**場合もあります。

SNS の乗っ取りからアカウントを守る予防策

- 普段からできるだけ二段階認証（SMS 認証など）を設定する
- パスワードを推測しにくいものにして，決して外部に漏らさない。10 桁以上にして，文字種（大文字・小文字，数字，記号）を多く使う
- ほかのサイトのパスワードと同じパスワードは使わない
- ログイン通知機能などの通知機能を有効にし，通知内容の確認を行う
- 興味のあるサイトであっても，アプリ連携に注意する
- どんなに親しい人の投稿からの誘導先であっても，誘導されるリンク先については十分注意をする（特に短縮 URL）
- フォローしている人のタイムラインに URL が含まれる連続投稿があった場合は，十分注意する
- 不審な投稿にある URL にアクセスしない
- 身に覚えのないアプリや連携させ続けておく必要のないアプリは連携を解除しておく

SNS のアカウント乗っ取りは年々，巧妙化しているようです。乗っ取りを防ぐだけでなく，偽の投稿内容を見て騙されないようにするなど，リテラシーを高めていくことが大切です。普段から予防策を実践し，万が一，乗っ取りの被害にあった場合は，保護者に伝えて警察に相談するなど慌てずに対処してください。保護者の方々もスマホ等の利用に関しては，しっかりと見守りのほうをお願いします。