❖テーマ３❖

個人情報について気をつけたいこと

良い出来事は「自分に起こる」
悪い出来事は「自分には起こらない、大丈夫」

人は楽観的で⇧こんな風に思い込みがち。
でも、ネットや受信メール等に

悪意の仕掛けが潜んでいる可能性

があることを忘れないで。

「自分は大丈夫」という気持ちを捨て

万が一を想像して慎重に!!

最近、個人情報の扱いが軽くなっている気がするの。
「〇〇もらえるなら登録くらいしてもいっか」
「招待してくれるなら携帯の番号を教えてもいっか」
「無料だし安全じゃなくても、ま、いっか」etc...
なんて考えてない？　それ、危ないよ❗

⑥ 入力した個人情報の意図しない二次利用

占いアプリで趣味嗜好を入力し

いつも読んでいる情報サイトに掲載されていた無料の占いにアクセスしてみたGさん。**生年月日や趣味嗜好を答えると、占いの結果が表示**されました。

大量の迷惑メールが届くようになった

その後、Gさんのスマホには**続々と広告のメールが届くようになりました**。その内容は、Gさんが占いの時に入力した好みに合ったものばかりでした。

考えてみよう！

▶学べる！プチ動画⑥ 事例⑥

消費者教育

占いの他、ポイントが獲得できるアンケートなどもありますが入力した情報が使われた例を知っていますか？

A.興味を示す広告を送る

好みの情報が送られてくれば誰でも興味を示します。購入・利用をしてもらえそうな商品や有料サービスの広告メールを送るために、個人の趣味嗜好を集める会社もあるのです。

B.悪用・流用されることも

わかりにくいところに「この情報は〇〇社と共有する」と記して、気づかないうちに個人情報が二次利用されていたりする可能性もあるため、細心の注意を！

掲載したメルマガや情報サイトの運営会社が信頼できても、広告の内容が信頼できるとは限らない！

解説 個人に関する情報へのアクセス許可や入力欄には要注意

アプリやサービスを利用登録をするときなどに、個人に関する情報を求められることもありますが、中には必要ない情報を入力させる悪質なものもあるので要注意。**氏名や住所、年齢、性別、メールアドレスなどが無断で二次使用されたり、業者に売られたりするリスクもあります。**新しいアプリやサービスを利用する際は、評価を確認する、友人に聞く、保護者に見てもらうなど、複数の方法で安全性を確認し、公式ストアを利用しましょう。

また、**ダウンロード時に表示される「このアプリにアクセス許可するもの」を確認し**、そのアプリに不要な情報へのアクセス許可を求めているなど、少しでも不安があるときはダウンロードを中止するのが賢明です。

ワンポイントアドバイス

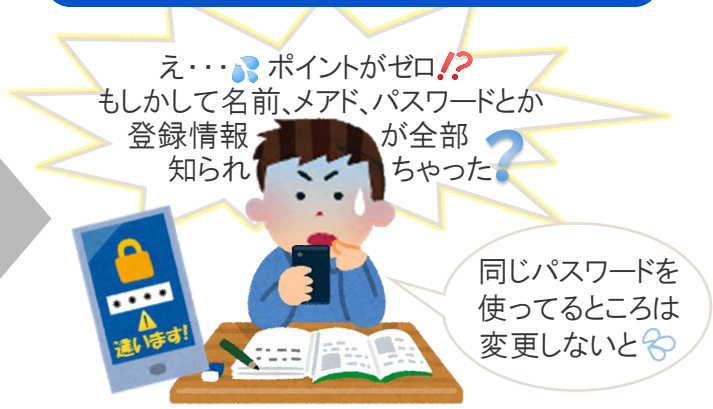
無料のアプリやサービスは、安全なものばかりではありません。個人に関する情報を求められたときは、しっかり確認するよう心がけましょう。

7 メールからの誘導によるフィッシング詐欺被害

IDがロックされたというメールが届き

「アカウント情報確認と再設定のお願い」メールが届いたHくん。よく使うIDなのでロックされたら困ると、慌ててメールにあったリンク先で手続きをしました。

ポイントと個人情報を盗まれてしまった



夕食後、アイコンからそのサービスを使おうとしたらアクセス不可。パスワードを再設定してログインすると、**貯まっていたポイントが全て使われていました。**

考えてみよう！

▶学べる！プチ動画7

運営会社をかたり安全確認やセキュリティ問題解消を促すメールは増える一方です。ウソを見抜き被害を避けるには、何に気をつけ、どんなことを心がければよいでしょう？

A.疑わしいメールやメッセージ

携帯会社、OS事業者、銀行、ショッピングサイト等の名で届く確認メールは、本物そっくりの入力画面へ誘導し個人情報を盗むことも。慌ててアクセスせず、公式サイトで必ず確認！

B.ニセの対策アプリへ誘導等

セキュリティ上の問題が生じて、対策アプリのダウンロードが必要だとURLを示し、不正アプリを導入させようとするものも！遠隔操作ウイルスにより盗撮等の被害に遭った人もいます。

C.不審なポップアップ

画面に出た「当たり」や「警告」のメッセージに不用意にアクセスすると、金銭や個人情報を騙し取られたり、ウイルス感染や機器乗っ取り等の被害に。“無視”も危機管理の1つです。

解説 安全をエサに釣る、巧妙な“フィッシングの仕掛け”に要注意

友人を装ったり興味を引くことを示して詐欺サイトへ誘導するワンクリック詐欺もありますが、**企業や行政機関等をかたり、安全性の確保を呼びかけるフィッシングの仕掛け**が増えました。「普段よく利用しているから何かあったら大変！」という人の心理を悪用し、パスワードやカード情報等を盗む手口。メールやメッセージの具体例や対策が各社の公式サイトに掲載されているので、**アクセスの前に確認するか、無視して削除**しましょう。

その他、ファイルを暗号化し解除をネタに金銭を要求する**「ランサム(＝身代金)ウェア」、盗撮や犯罪に利用するための遠隔操作ウイルス等の被害も発生しています。OSやセキュリティソフトの更新を忘れず安全な利用環境を！**

ワンポイントアドバイス

セキュリティ対策を行うと共に、日ごろから“用心”と“こまめな更新”を心がければ、突然の警告を不審に感じて、冷静な対応ができます。

⑧ 悪意あるWi-Fiスポットを利用したことによる情報流出

パスワード不要の無料Wi-Fiスポットで

Iくんは、**パスワードもいらず無料でネットに接続できる場所**を近所に発見。家の電波が不安定なので、よくその場所に行ってネットをしていました。

通信内容が盗み見られてしまった

Iくんの通信内容

・メール内容
・アクセス履歴
・書き込み内容
・ID/パスワード
ほか

そのWi-Fiスポットは、**他人の情報を盗むために悪意で設置されたもの**でした。Iくんの通信内容は、ずっと盗み見られていたのです。

考えてみよう！

学べる！プチ動画⑧

Wi-Fiが自由に使える場所が増えていますが、ネットを使いたいという人の思いを利用した悪質なWi-Fiスポットもあります。安全に使うために気をつけたいことは？

A .悪質なWi-Fiスポットも存在

悪意を持った者がWi-Fiスポットを設置することもあります。新しくWi-Fiスポットに接続するときは、誰が提供しているのか、接続先の名称や鍵マークは正しいかを確認するようにしましょう。

B. 通信内容の保護を

個人情報等を入力するときは、通信を途中で盗み見されないようにするために、ブラウザ上に鍵マークが表示されるか、URLが「https」からはじまっているかを確認しましょう。

C.いざ！というときのために

緊急災害時、携帯電話会社の電波が使えなくなることもあります。通学路や自宅近くで安全なWi-Fiを提供している場所をいくつか知っておけば、命をつなぐことに役立ちます。

解説 ラッキー！が一転、個人情報の流出や悪用の恐れもある

スマホは、携帯電話事業者の回線（3G/4G/LTE/5Gなど）だけでなく、Wi-Fiスポットを使ってネットに接続することができます。でも、自宅に無線LAN環境が作れるように、Wi-Fiスポットは誰にでも設置できます。名称、鍵マークやWi-Fiステッカー※等でどのようなWi-Fiスポットなのかを落ち着いて確認しましょう。

出先でパスワード不要の無料Wi-Fiを探す人もいますが、**通信傍受やID・パスワードなどを盗むために設置する人もいる**ことを思い出して！**Wi-Fi設定が自動接続だと悪意のWi-Fiスポットにつながる危険が、スマホのデバイス名が本名だと接続時に名前が知られてしまう危険が**あるので、設定を見直すことも大切です。

ワンポイントアドバイス

Wi-Fiスポットの中には、悪質なものや安全性の低いものがあることも。外出先で利用するなら、提供者や通信内容の保護を必ずチェック！

※公共施設や店舗等に貼ってある、Wi-Fiが使えることを示すステッカー。緊急災害時にも役立つので、身近なWi-Fiスポットを調べてみましょう。