個人情報＆プライバシー編
～防ごう！悪用・詐欺被害・特定～

良い出来事は「自分にも起こる」
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、Wi-Fi、メール、Web、SNS等には

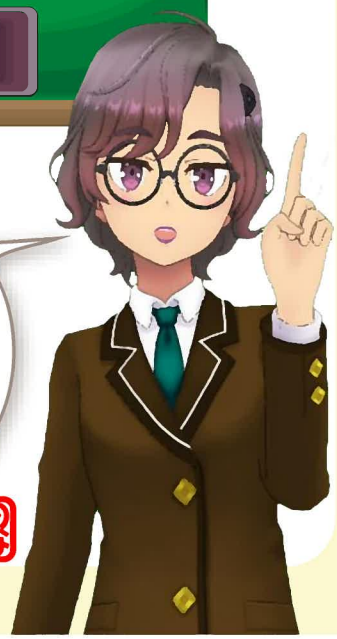
ネットのワナや人の悪意が潜んでいる

可能性があるということを忘れないで。

「自分は大丈夫」という気持ちを捨てて

万が一を想像して慎重に!!

こうした心理を『正常性バイアス』と言います。



身の回りには、個人が特定できそうな情報だらけ。
「〇〇をもらえるんだったら、登録するくらいいっか」
「招待してくるのなら、携帯番号を教えてもいっか」
「安全かわからないけど、無料だし、ま、いっか」
…なんて考えてるんだとしたら、それ、危ないよ⚠

⑨ 悪意で設置されたWi-Fiスポットを使用し情報が流出

パスワード不要の無料Wi-Fiを使ったら

Lくんは、近所に**パスワードがなくても無料でWi-Fiに接続できる場所**を発見。安定していて使いやすかったので、ちょくちょくそこでネットを使っていました。

通信内容が盗みとられてしまった

L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

でもそれは、**他人の情報を盗む目的で設置されたWi-Fi**でした。Lくんは通信内容をのぞかれ、大切な個人情報を盗まれてしまったのです。

考えてみよう！

▶学べる！プチ動画⑨

Wi-Fi接続できる場所（スポット）が増えていますが、フリーWi-Fiに自動接続して使う人を狙った悪質なWi-Fiもあります。安全に使うには、何に気をつければよいでしょう？

A.悪意で設置されたWi-Fi

名称を似せたなりすましや悪意の仕掛けなどの危険なWi-Fiは、セキュリティ設定のないものがほとんど。自動接続をオフにして、ネットワークリストで名称・鍵マーク🔒を確認するクセをつけましょう。

B. 個人の情報を守るために

フリーWi-Fi接続中には、個人情報の入力を控えるのが基本。入力しなければならないときは、通信内容を盗まれないように鍵マーク🔒やURLが「https」かなどを事前に必ずチェック！

C.いざ！というときのために※1

緊急災害時は、携帯電話会社の電波が使えなくなることも。自宅・通学路・よく行く場所の近くで信頼できるWi-Fiスポットをいくつか見つけて登録しておけば、慌てずにすみます。

※1：災害時にWi-Fiを無料開放する『00000JAPAN（ファイブゼロジャパン）』が実施されています。利用の注意点もあるので調べてみましょう。

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（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のアクセスポイントは誰にでも設置できます。ネットワーク名称、鍵マーク🔒やWi-Fiステッカー※2等でどのような接続先なのかをしっかり確認しましょう。

出先でパスワード不要のWi-Fiを探す人がいますが、**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の設定が自動接続だと悪意のWi-Fiにつなげてしまう危険が、スマホのデバイス名が本名だと接続時にフルネーム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

フリーWi-Fiの中には、悪質なものや安全性の低いものがあることも。外出先では自動接続せず、名称やセキュリティなどを必ずチェック！

※2：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。

⑩ 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**M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

その後、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⑩

運営会社をかたって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

セキュリティ上の警鐘を鳴らし、対策アプリ提供サイトのURLを示して不正アプリを導入させる手口も多発！遠隔操作アプリを導入してしまって、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

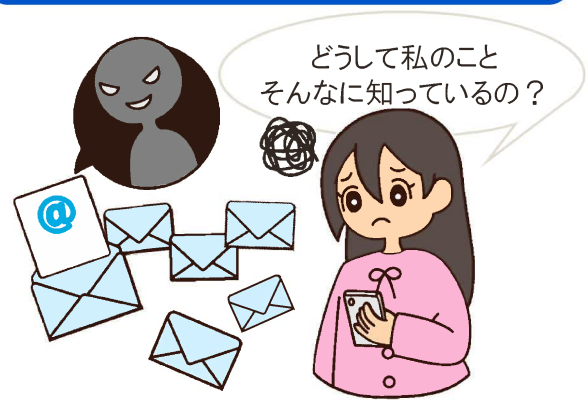
セキュリティ対策を行うと共に、日ごろから“用心”と“こまめな更新”を心がければ、突然の警告を不審に感じて、冷静な対応ができます。

11 入力した個人情報が目的外で利用?!

占いサービスで趣味嗜好を入力したら

よく読む情報サイトにあった無料占いの広告が気になったNさん。**名前・誕生日・趣味嗜好などを答え、結果の返信先としてメールアドレスを登録**しました。

大量の広告メールが届くようになった



その後、Nさんのスマホには占い結果以外にも**大量の広告メールが届くようになりました**。その内容は、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11

消費者教育

占いに限らず、アンケートに答えるとポイントなどがもらえるキャンペーンもあります。“個人情報やプライベートな情報”の入力を求められた際に意識しておきたいことは？

A.収集した情報で稼ぐ会社も

好みの情報なら誰でも興味を示すため、個人の趣味嗜好は貴重な情報。集めた情報を元に商品やサービスの広告メールを送る、配信業者に提供する等が収入源の会社もあります。

B.情報提供先の記述に注意

中には、わかりにくいところに「この情報は関連会社と共有する」等と記し、第三者提供する悪質な業者も。サービスを利用するのなら、同意ボタンを押す前に規約や条件に目を通して！

C.大切な情報を提供する前に

メールアドレスを変えれば大量のメール受信は止まりますが、本名・生年月日・住所・学校名などは悪用されても変更は無理。入力した情報がどう使われるか、送信前に再確認を。

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

新たなアプリやサービスを利用する際は、評価を読む、友人に聞く、保護者や信頼できる人に見てもらうなど、複数の方法で安全性を確認しましょう。アプリの場合、公式ストアを利用し、**ダウンロード時に表示される「アクセス許可するもの」をチェック**。アプリとは関係ない情報を求めている等の不安があれば中止するのが賢明です。

また、利用登録時には個人に関する情報を入力しますが、**氏名、住所、年齢、性別、メールアドレスなどが無断で、別の目的に使われたり悪質な業者に第三者提供されたりするリスク**もないとは言いきれません。登録情報の利用目的についても、しっかり読んで確認しておくことが大切です。

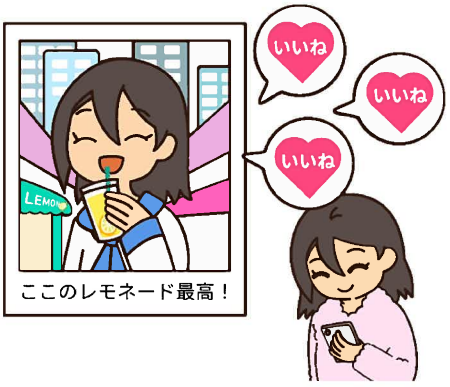
ワンポイントアドバイス

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。

㊟本事例集では、青少年のインターネット利用の現状を鑑み、「個人に関する情報」も含めて「個人情報」として取り扱っております。

⑫ 投稿から個人が特定されたことによる被害

おいしい情報をシェアするつもりが



よく行くショッピングタウンでお気に入りのお店を見つけたOさん。親しい人たちに教えてあげようと、**位置情報オフで撮影した写真を投稿**しました。

知らない人に付きまとわれるようになった

その後、誰かに後をつけられていることに気づきました。引き金は、Oさんが投稿した**写真の背景。場所がわかり生活範囲が特定**されてしまいました。

考えてみよう！

▶学べる！プチ動画⑫

ネットにアップした写真や動画で、撮影場所や生活範囲が知られてしまうケースが。事件やトラブルに巻き込まれないために、投稿の際に注意しなければならないことは？

A.高性能・高画質への注意

カメラの性能が高まり、ピースサインで指紋が判別されることもあるとか。電柱・看板の文字が読めたり、瞳に映ったものが見えたり‥‥撮影・投稿にはより一層の注意が必要です。

B.閲覧者を限定した投稿が○

一番の安全策は、プライベートな情報をネットに載せないこと。でも、情報のシェア自体が悪いわけではありません。投稿前によく見直し、非公開設定にして特定の人とだけ共有する等の危機管理を！

C.もしも不安を感じたら

自分のサイトに気になる投稿があった、知らない人に突然名前で呼び止められたなど、不安を感じたときは必ず大人に相談すること。できるだけ、誰かと一緒に行動しましょう。

解説 “こっそり”だけじゃない！時間をかけて徐々に近づくケースも急増

SNSが当たり前の環境で育った子供・若者は、ネットで個人情報を扱う際、慎重さに欠ける傾向があります。そもそも、誰でも見ることができるのがSNSの基本。写真に映りこんだものから、訪れた店や地域など生活範囲が推測できるため注意が必要です。また、事例❷(P8)にもあるように、長期間やりとりを続ければ初期の警戒心は段々薄れ、信頼感が生まれ、プライベートなことまで話すようになるのを見込んで近づいてくる人もいます。投稿・やりとりの先にある、脅迫・ストーカー・誘い出し・投資詐欺などの被害の可能性を忘れてはいけません。

「個人が特定できるもの・コトを公開しない」「非公開や短時間で消える場合でも投稿前にチェック」と共に、**「ネットだけの友達には警戒を緩めず個人的な話は控え、少しでも気になったら距離を置く」**ことを心に留めて。

ワンポイントアドバイス

コミュニケーション系アプリの多くは、閲覧できる人の設定が可能。公開範囲を絞り、悪意で近づいてくる人に個人情報が伝わらない工夫を。

※ネット上にアップした・された情報で困ったことが起きたら『違法・有害情報相談センター』もご利用ください。➡ https://www.ihaho.jp/