ポイント 2

プライバシーを守ることは生命の安全に直結する！

セキュリティ設定である程度スマホに守ってもらった上で、自分も気をつけて使う

個人が特定できる情報

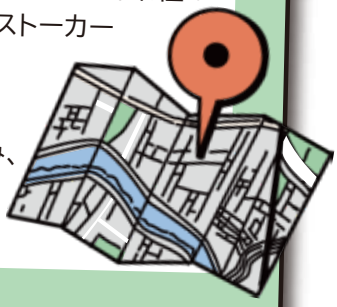
「その入力、ちょっと立ち止まって考えて⚠」
無料の占いサイトや無料ゲームなどを装い、犯罪に悪用する目的で情報を搾取するサイトやアプリも身近にあります。要注意！

ワンポイント

個人情報の安易な入力をやめると共に、SNSなどで他人に伝わらないように工夫しましょう。

位置情報は諸刃の剣

位置情報は場所探しなどにとても便利。
でも、居場所を公開してしまう危険も！
特に気をつけたいのは『位置情報共有アプリ』。素性が明らかでない人を友達登録すると、ストーカーなどの被害にあう可能性もあります。



ワンポイント

アクセス許可はアプリの使用中のみ、公開するのはリアルな友人知人だけ、など設定の工夫を！

無料(フリー)Wi-Fiにはワナも

無料Wi-Fiの中には、情報を盗むために悪意で設置したものもあるため、自動接続する設定でWi-Fiを利用するのはとても危険です。

ワンポイント

自動接続ではなく、都度確認！
正規の接続かどうかはWi-Fiのステッカーなどを確認してから接続しましょう。

セキュリティ設定を活用

ウイルス侵入防止や、フィッシングサイト等へのうっかりアクセスを防ぐために、セキュリティソフトを導入し、OSと共に常に最新の状態にしておくことが大切です。
もちろん、画面ロックの設定は最低限のお約束です。

ワンポイント

『ID=メールアドレス』、『パスワード=生年月日』は危険！使いまわしをやめ、想像が難しい文字の組み合わせを考えましょう。

一緒に考える！

いっぱい

『コミュニケーション』のリスク

ネット上でも会って話しているような感覚の中高生。緊張感や警戒心の少なさが、危険を招く要因となっています。

▸ 読む人の気持ちや表情を思い浮かべる

表情や声が届かないメッセージのやり取りは、ささいなことで誤解が生じいじめなどに発展するケースも。送るときも読むときも、相手のことを考えることで、もめ事のリスクは軽減されます。

▸ 素性やメッセージを偽って近づいてくる人も

架空の人物になりすまし、時間をかけて信頼させ、脅迫・誘拐・ストーカー行為などに及ぶといったケースが後を絶ちません。特に、DM※などで直接連絡を取ろうとしてくる相手は要注意。うまく断るメッセージを用意しておくのも賢いやり方です。

※DM:ダイレクトメッセージ(当人同士以外の目に触れない直接のやり取り)

『売買・契約』のリスク

ネットショッピングやフリマアプリは手軽で便利ですが、買物や取引は「売買契約」であることを忘れてはいけません。

▸ 見た目は良さそうでも偽通販サイトかも

代金を支払ったのに商品が届かない、激安サイトがメーカーを装った偽サイトだった等、さまざまなトラブルが起きています。値段や在庫状況など、どこかに違和感があれば購入STOP！

▸ “欲しい気持ち”や“価格の安さ”よりも信頼性

人気のフリマは、ほとんどが個人間取引。掲載情報をうのみにせず、商品の状態や評価などの確認は不可欠です。また、保護者のクレジットカードの使用や、法律で禁止されている物の取引などをしないよう徹底しましょう。