警視庁からのタイセツな、お知らせ

タ　ダウンロードは慎重に

パソコンやスマートフォンは、悪意あるソフトやアプリからウイルスに感染する危険性があります。どんなに便利そう、面白そうでも、信頼できないアプリなどのダウンロードはやめましょう。

イ　いますぐアップデート

ソフトやアプリの弱点を突いた攻撃が原因となって、サイバー犯罪の被害に遭う場合があります。弱点をなくすために、アップデートが公開されたら後回しにせず、速やかに行いましょう。

セ　セキュリティソフトを導入しよう

どれだけ注意しても、ウイルスは感染の機会を狙っています。パソコンやスマートフォン内に記録された大事なデータをウイルスから守るため、セキュリティソフトを導入しましょう。

ツ　使いわけようパスワード

IDとパスワードを使い回して、ひとつでも漏れてしまうと次々に悪用されるかもしれません。複数のパスワードを使い分け、管理しましょう。

迷ったら タップしない！ 入力しない！ 疑ってみる！

≒JOY 江角怜音　　≒JOY 市原愛弓

インターネット空間の危険から身を守ろう！

警視庁では、サイバー犯罪やサイバーセキュリティに関する情報発信を行っています。

サイバーセキュリティインフォメーション　検索
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/index.html

YouTube 警視庁公式チャンネル

X公式アカウント警視庁サイバー @MPD_cybersec

警視庁サイバーセキュリティ対策本部
街とともに。人とともに。FOR MORE COMMUNICATION けいしちょう

迷ったら タップしない！ 入力しない！ 疑ってみる！

SNS型投資詐欺

SNSの広告で投資を勧誘し、グループチャットなどで信用させて、お金をだまし取る

正しい対処法

1. 取引業者が金融商品取引業者等に登録されているかを確認する!
2. DMやグループチャットでの儲け話に注意!
3. 「個人名義の口座」には振り込まない!

フィッシング

実在する有名企業や官公庁を装ったメールやSMSを送り、本物にそっくりのサイトへ誘導してログインIDやパスワード、クレジットカード情報などの個人情報を盗み取る

正しい対処法

1. メールやSMSのリンク先からは個人情報を入力しない!
2. 不安を煽るような内容のメール・SMSは疑う!
3. 被害に遭ったらすぐ警察に相談!

闇バイト

高収入・ホワイト案件等と、甘い言葉で普通の求人を装いながら、犯罪に加担させる

正しい対処法

1. まず疑う。楽してお金を稼げるアルバイトは存在しない!
2. 少しでも怪しいと思ったら色々調べてみる!
3. 一人で決めない。悩んだら専用窓口に相談!

偽サイト

メールやSMSから偽サイトに誘導し、ログインIDやパスワードなどを入力させ盗み取り、不正に悪用する

正しい対処法

1. メールやSMSに記載されたURLは開かない!
2. メールやSMSのリンク先からは個人情報を入力しない!
3. サービスの公式アプリや公式サイトからアクセスして内容を確認する!