テレワークのセキュリティ ここにも気をつけよう!

電子メールからのウイルス感染に注意!

メールに添付されているWordファイル等のマクロ機能を起動したり、メール本文やPDF等の添付ファイルに記載してあるURLにアクセスしたりするとウイルスに感染する恐れがあるので、安易にクリックしないようにしましょう。

カフェなどのWi-Fiスポットの安全性に注意!

Wi-Fiスポットは、セキュリティが十分でない場合があるので、重要な情報のやり取りは行わず、ファイル共有機能をオフにしましょう。

テレワーク後の機器は、社内に戻す前に安全確認!

テレワークで使用した機器は、ウイルスに感染している恐れがあるので、会社のシステムに接続する前に、最新のウイルス定義のウイルス対策ソフトで、ウイルスチェックしましょう。

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。

情報セキュリティ広場 検索
https://www.keishicho.metro.Tokyo.lg.jp/kurashi/cyber/index.html

@MPD_cybersec

YouTube

警視庁サイバーセキュリティ対策本部

ストップ!! それ、信用できません!

情報セキュリティ広場 検索
https://www.keishicho.metro.Tokyo.lg.jp/kurashi/cyber/index.html

街とともに。人とともに。
FOR MORE COMMUNICATION
けいしちょう

@MPD_cybersec

こんな時、ちょっと待って!

SMSを悪用した偽サイト詐欺(フィッシング)

例えば スマホのSMS(ショートメッセージ)に宅配便の不在通知が届いたのでSMS記載のURLにアクセスすると宅配業者に偽装したサイトに誘導され個人情報を盗まれた。

- 宅配業者や金融機関からSMSでログイン情報の入力を求められてもURLをクリックしないようにしましょう。
- ウェブサイトにアクセスするときは、あらかじめ登録したお気に入りや公式アプリから行いましょう。

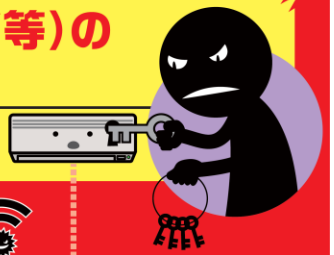
[偽警告]によるインターネット詐欺

例えば インターネットを見ていたら「ウイルスが検出されました」というメッセージが表示され、連絡先に電話をしたら、無理矢理サポート契約をさせられ、パソコンを乗っ取られた。

- 普段から使用しているセキュリティソフトによる警告ではない場合、無視して画面を閉じましょう。画面を閉じられない場合は、機器を再起動しましょう。

ネット家電(IoT機器・ゲーム機等)のセキュリティ対策

例えば IoT機器が初期設定のままだったので、外部から侵入され、情報を盗み見られた。



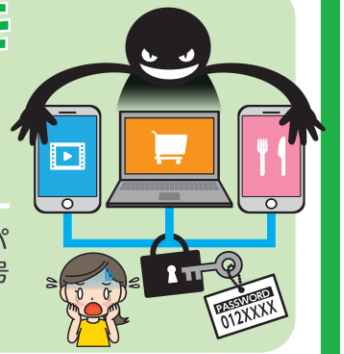
- 初期設定のパスワードの変更や各種セキュリティ機能(通信制限、ログインを要求する機能など)の設定を行いましょう。
- 使用しないときは電源を切り、ウイルス感染や不正な遠隔操作を防止しましょう。

基本的なセキュリティ対策

パスワードは使い回しをせず適切な管理を!

使い回していると、他のサービスにも不正にログインされることがあります。

サービスごとにパスワードを使い分けましょう。またパスワードは、アルファベットの大文字、小文字、数字、記号を組み合わせて簡単に推測されないようにしましょう。



OSやアプリは最新バージョンに更新を!

更新せずにしておくと、セキュリティに脆弱性がある状態になりとても危険です。

OSやアプリは、アップデートが公開されたら、すみやかにアップデートしましょう。

ウイルス対策ソフトの導入を!

ウイルス対策ソフトを導入しないと、ウイルスに感染しやすくなります。

ウイルス対策ソフトを導入し、パソコンやスマートフォンをウイルス感染から守りましょう。