

よい子のためのPC教室

(お土産編)

使おうよデザリング

- デザリングとはスマホをwi-fiルーターとして利用する機能
- 通信会社によって、有料・無料の別あり
- 使った分はパケットが減ります
- スマホの設定からデザリングを選び、SSIDとパスワードを指定してアクセスポイントを有効にする→繋ぐ機器の方からSSIDを指定しパスワードを入力して完了

ありがちなIDとパスワードの管理

- PCに付箋紙で貼り付けるのはNG
- 自分の誕生日はPIN(暗証番号)としてNG
- windows機はパスワードではなくPIN(暗証番号)でログイン
- windows機は生体認証・物理キー認証・デバイス認証できるならそちらで
- パスワードは英語大文字・小文字と数字と記号のすべてを含み12文字以上で作ること
- パスワードに誕生日やイニシャル、すでにある単語は推奨されない

スマホの風呂場での利用

- 防水機能がついていても風呂場では使わない
風呂場での利用を推奨するスマホはある？
- 感電の危険があるため、充電しながらの利用は厳禁
- 感電の危険があるため、そのままでの利用も推奨されない
- スマホの防水は完璧ではない
- カメラ搭載のため、使わない方が吉(リスクあり)

windowsのアップデートはお早めに

- updateを定期的(最低でも月1回以上)に行う

位置情報・マイク・カメラの許可

- PCやスマートフォンのアプリケーションに対する位置情報・マイク・カメラの許可はトレードオフの関係
- 位置情報・・・生活情報・暮らしの情報の漏洩に
- マイク・・・盗聴されるリスク
- カメラ・・・盗撮されるリスク
- 便利さとリスクとの兼ね合いをどう考えるかバランスが必要

PCの処分

- 基本は記録装置を外して処分する
記録装置＝HDD(ハードディスク)、SSD(ソリッドステートドライブ)
- 処分とは＝PCRサイクル・売却・譲渡
- HDDやSSDを換装すればwindowsインストール可能な場合も
- 買い換えした場合、使っていたソフトウェアの利用は規約による
→ライセンス型は不可能な場合が多い
→クラウド型・アカウント型は再インストール可能な場合が多い
- 連絡が取れないような業者には処分を依頼しないこと

記憶装置の処分

- 記憶装置(HDD、SSD、USBメモリなど)
- データの移行は予め行う
- 消去しただけでは本当には消えていない(復元される危険性)
- 乱数を3回以上上書きした上で処分することを推奨
- 自分でできないようなら専用ソフトまたは業者の利用も検討
- お勧めは取り外してから外付けHDD、SSDとして利用すること
対応ケースはamazonで売っています(¥1000程度)
フォーマットする必要あり(知識が多少必要)
- USBメモリは物理的破壊も検討すべき

古い機器(PC・スマホ・タブレット)

- セキュリティー切れのものはネットワークに繋いで使わない
- ネットワークに繋がらない利用方法はOK

デジカメ、音楽プレイヤー、ICレコーダー、キッチンタイマー、デジタルフォトフレーム、ストップウォッチ、画面付きUSBメモリなど

- 売るなら信用できる業者に(素人ではリスクが高い)
- 初期化してもデータは消えていないと思うべし
- どうしても使いたいなら

スマホはカスタムROMを試してみれば?(要知識)

PCはlinuxを試してみれば?(要知識)

ネットワーク機器のパスワード変更

- モデム・ルーターが初期パスワードのままならすぐ変更
- 失敗したら出荷時に戻るボタン(物理ボタン)で初期化し再変更
- ファームウェアは常に最新のものを(アップデート)
- ネットワークカメラ・ネットワークプリンタ・コピー機も初期パスワードのままなら変更する

不審な訪問者にPCを貸さない

- PCを貸して欲しいと尋ねてくる訪問者に注意
- 「プリンタを使いたい」というお願いをされます
- 親切は不要
- USBメモリは差させない(プログラムを実行される可能性)
- 本当に大切なのは顧客からの信用か見知らぬ人への親切か
- 拾ったUSBを差すのも不可
- どうしても貸したいならguestアカウントを作成すること

駅前のwi-fiフリースポット(野良wi-fi)

- どこが所有・提供しているか分からないwi-fiに接続しない
- 野良wi-fiで「http://」のサイトにアクセスすると入力情報を奪われる
- 野良wi-fiで「https://」のサイトならある程度は・・・(非推奨)
- 基本どこにアクセスしたかは知られる
- 提供元が分かっているwi-fiでもパブリックネットワークに設定
- 提供元が分かっているwi-fiでもVPNの利用を推奨

メールの添付ファイル対策

- wordやexcelのマクロとVBAはプログラムであると認識する
- 添付ファイルのwordやexcelは保護ビューのまま使用
ソフトが保護ビューになるか確認をしておく
- 添付ファイルの拡張子が.exe(実行ファイル)なら絶対に開かない
どうしても.exeを開くなら仮想環境、または専用PCで
仮想環境を自分で用意できないレベルの人は開いてはいけません
- プログラムを内部から実行されることは絶対防ぐこと

野良アプリのインストール

- 野良アプリ＝ストア以外から入手するアプリ
- 野良アプリのインストールはしないこと
- 基本的にアプリストアからはじかれたものがほとんど
- どうしてもインストールしたいなら仮想環境か専用PCで試してから
- アプリストアにもマルウェアは存在する
- アプリの選び方は？

アダルトについて(成人限定)

- 無料アダルトサイトから動画と称するものをダウンロードしない
- 信用できる店舗からDVDで買うのが比較的安全
- 信用できる有名老舗サイトから有料購入するのも比較的安全
※サイトのドメインをしっかり確認すること
- セクシー業界の方々にお金が渡るようにしましょう
- 無料アダルトサイトには危険性があることを十分十二分にも認識しておくべき

フィッシング詐欺対策

- **ドメイン(@以下の部分)を必ず確認**すること
サイト本来のドメイン以外のものの偽サイトに注意
いつもの企業名ではない「.」より上の部分も警戒
(例) @amasendayo.ne... @rakusennanndesu.ma...
サイトが本物でもリダイレクト(転送)されたものには入力しない
- **SMSからのURLを踏まない**こと
- **普段使うサイトはブックマークやアプリからアクセス**すること
- 見た目では判断不能なので留意すること
- フィッシングとは見た目がそっくりなサイトでIDとパスワードをだまし取る詐欺です

windowsを守るには(まとめ)

- メールのお添付ファイルに注意
 - word,excelなどはマクロとVBAの実行がない方法で
 - + .exeは実行しない
- WEB閲覧の注意
 - お金の要求とサイト上のアラートは無視
- 送られてきたURLに注意
 - 基本はクリックしない + もしリダイレクトしたら閉じる
- 野良アプリ
 - インストールしない

おうちに帰ってやる宿題

- モデムとルーターのパスワード変更(初期のままなら)とファームウェアアップデート
- ネットワーク機器のパスワード変更(初期のままなら)
- 簡単すぎたパスワードの変更(数字4文字だけとか簡単な英単語)
- PCに貼った付箋を剥がす(IDやPASSWORD記載のものなら)
- Windowsのアップデート(まだのものがあるなら)
- セキュリティー切れの機器は(使う気なら)こまめにネットワークから切断する
- 家族とPCを同一アカウントで共有しているようなら、それぞれアカウントを作ろう(※未成年の子どもにはルール作りが必要)