

第8回 デジクエ 詐欺サイトで失敗したときのフォロー

まず相手を知る

どんな種類があるのか

偽物警告画面、偽物セキュリティソフト

ID・パスワードを盗むフィッシング詐欺

アダルトサイト詐欺（ワンクリック詐欺）

ランサムウェア

SNS アカウント乗っ取り

偽ブランド品詐欺、偽販売サイト詐欺

Web サイト改ざんウイルス被害

では何が欲しいのか？

お金です。そのためにあの手この手で情報を収集しようとしてきます。そしてあなたに成りすまして今度はお友達を同じ状況に連れて行こうとします。今日はそうならないように相手を知って相手に踊らされない心構えを勉強したいと思います。

先ほど挙げた詐欺の種類ですが、実際遭ってみたいとどんなものかわかりませんので、ひとつづつこんな手口ですよっていう事を頭に入れておけば安心です。

大切ななのはこれが詐欺なのかどうなのかわかる知識です。

例えば受験する際に過去問をやった方が問題の形式とか傾向もわかるので落ち着いて対処できるっていう感じです。

・偽物警告画面、偽物セキュリティソフト

最近よく問い合わせがあります。インターネット検索で調べ物をしていたら…突然画面が赤や白や黒に連続で切り替わり大きな音で焦らせてきます。ウイルスに感染しましたという文章と一緒にカウントダウンタイマーとここに Microsoft サポートに電話してください電話番号は 05042...みたいな表示が出てきます。これは電話させてお金を振り込みするように促してきます。

実際の体験談ですが、片言の日本語で家族構成や年齢や名前や聞いてくるそうです。

そもそも電話したら駄目です。相手が欲しいのは電話番号でこれにひっかかるとほかの詐欺でも電話がかかってくるつまり詐欺グループの詐欺に引っ掛かりやすい人の名簿に登録されます。絶対電話をしてはいけません。もし電話を掛ける指示が画面に出たら僕もしくは警察に電話をかけてください。一応ウイルスに感染してないかチェックも行ってください。画面右下の上向きの矢印みたいな中に青い盾のマークがあるのでそこからチェックできます。

・ID・パスワードを盗むフィッシング詐欺

メールでよく来るやつです。

例えばアマゾンのアカウントに問題があります。再度ログインしてください。

でそのサイトにそっくりなページに連れていき ID とパスワードを入力させるあとはわかりますね

・アダルトサイト詐欺（ワンクリック詐欺）

アダルトなサイトの再生ボタンを押したら「ご利用ありがとうございます。期日までに 18 万円払ってください」的なあれです。そのページには小さく再生ボタンを押したら利用規約に同意したとみなされます。的なことも書いてありますが 1 回クリックで契約が完結すること自体成立しないのでそっと閉じて何か連絡があっても無視で大丈夫です。やり取りするだけ不利になります。ネット上においてですが、基本的に支払い完了してから利用という流れが一般的です。あとからいくらですは基本ありません。

その手のサイトで安心して楽しみたい方は僕までご連絡を…

・ランサムウェア

画面をロックされてしまうクラッキングです。ランサムつまり身代金を払えば解放しますよってやつです。ニュースで企業のシステムがというやつはこれが多いと思います。これはロックと同時に暗号化もするので、単純にデータだけほかの PC で取り出そうっということとは不可能だと思います。そして暗号化も強制的に行ってしまうので、データが破損して完全に修復できないということも聞いたことがあります。これもメールからのツークリックぐらいで被害を受けるのでメールの相手をしっかり確認しましょう。

・SNS アカウント乗っ取り

フェイスブックやインスタグラムやツイッターでアカウントを乗っ取りそのお友達に詐欺に引っ張るサイトの誘導するメッセージを本人に成りすまして送ります。

SNS においてメッセージャーは便利ですが、意味の分からないものが送ってきたら別の連絡手段で相手に確認してみてください。

・偽ブランド品詐欺、偽販売サイト詐欺

このバックが欲しいなとか思ったらネットで検索すると思います。その時に異常に安いものが出てくることがあります。特に怪しくもなく閉店セールや処分セールなどとうたって安く偽物や代金だけ受け取って商品が届かないまた名前や住所や電話番号そしてクレジットカードとセキュリティーキーもろとも持っていかれてしまいます。

ネットでお買い物をする際は本当に安心なサイトなのか調べてから購入するようにしましょう。もちろんそこでしか売ってないけど買うのにためらっているならペイパルです。

Web サイト改ざんウイルス被害

ホームページを作った経験がある方ならわかると思いますが、このページを開いたらそのページに貼ってある youtube の動画が自動で再生されるとか設定ができます。このような機能を悪用してウイルスを置いておき開いたら自動で感染してしまうというページを作ることも可能です。

これは最初のにせ警告画面やにせセキュリティーソフトもこのやり方で動いています。こういったウイルスのあるページは Microsoft エッジやグーグルクロームが開く直前に遮断してくれます。それでも入りますか？と出たら入らないほうが良いです。

体感ですが、マイクロソフトエッジで yahoo を初期に設定されてる方はよく詐欺のページにたどり着いてしまうことが多い気がします。もし僕が詐欺師で詐欺に引っ掛けるならおなじような設定でやると思います。

まとめ

PCの前で焦る状況になったらまず深呼吸

その画面のままとりあえず LAN と Wi-Fi を切る

画面を写真で撮る

僕に電話する

ウイルススキャンを実行する

心配なら僕のお店に持ち込んでください。