

SNSを悪用したフィッシング被害が発生!

今回の手口は、「友人を装った者から送られて来たメッセージに動画が添付されており」、動画をクリックするとID、パスワードの入力を求められます。

その際、ID・パスワードを入力すると「iPhone11Proが当選した」と称して、「アンケートへ移行し、クレジットカード情報などの入力を求められる」という二段構えの手口です。

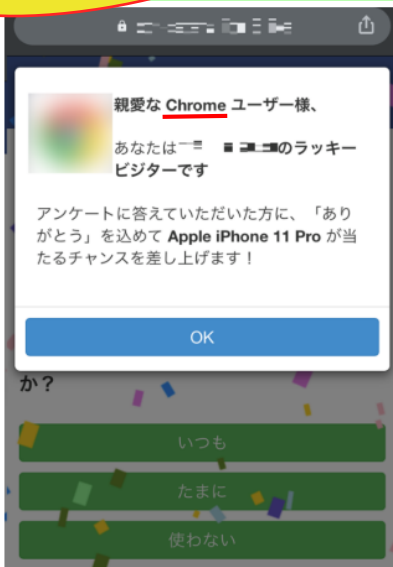
こんな内容のメッセージと動画が送られて来たら注意!



- ◆ このビデオはあなたのものでしょうか?
- ◆ このビデオはいつですか?
- ◆ このビデオはあなたですか?



当然フィッシングサイト!



ID、パスワードを入力するとこんなアンケート画面へ導かれます

※ フィッシングサイトに情報を入力すると
🔥 アカウントの乗っ取り
🔥 商品の不正購入
などの被害に.....

そんな上手い話あるわけないじゃん♪



SNSの基本的なセキュリティ対策

- ① 身に覚えのないアプリ連携がないか確認。
- ② 利用しなくなったアカウントの退会手続きや情報の削除などを行い、悪用されないようにする。
- ③ 公開範囲やダイレクトメッセージを受信する範囲を制限する。
- ④ アカウントを乗っ取られてもログインできる場合は、直ちにパスワードを変更する。ログインできない場合は、管理者に直ちに申し出る。

