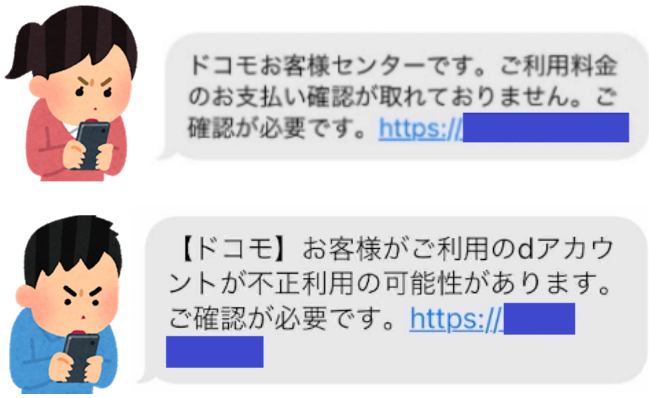
大仁警察サイバー通信　第５号

NTTドコモを装ったフィッシング被害多発!!

ドコモを装ったSMS※や不正アプリによるドコモオンラインショップでのApp Store&iTunesギフトカード等の不正購入事案が発生。

【ドコモからのお知らせ】
https://www.nttdocomo.co.jp/info/notice/page/211002_00.html



実際送られた SMS(内容はあくまで一例です)

URLをクリックすると

誘導された不正サイト

ダウンロードをクリックすると

不正アプリインストール画面

今回の手口

① 利用者の不安をあおり、早急に確認を促す内容です。
② メッセージのリンク先をクリックすると、不正サイトへ誘導されます。
③ 不正アプリ(NTT セキュリティ)をインストールさせられます。
④ ネットワーク暗証番号の入力を求められます。

被害に遭わないために

① 事例のようなＳＭＳが送られて来ても、リンク先をクリックしない。
② 通知内容を確認する際は、ドコモやドコモショップに直接問い合わせる。
③ ID やパスワード、暗証番号などを不用意に入力しない。
④ セキュリティスキャンの実施やアプリ一覧の確認など、不正なアプリが入っていないか確認する。

※ ＳＭＳ：電話番号宛に届くショートメッセージサービス