ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●ドコモを装ったフィッシングSMSに注意喚起

https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/
https://www.antiphishing.jp/news/alert/docomo_20190621.html

このニュースをザックリ言うと･･･

- 6月17日（日本時間）、NTTドコモより、同社を装いフィッシングを行おうとするSMS（ショートメッセージサービス）が出回っているとして注意喚起が出されています。

- 同社サイトで挙げられているフィッシングSMSの中には、送信元がドコモ公式SMSと同じ「NTT DOCOMO」となっているものがあり、公式SMSと同じスレッドに表示されてしまう可能性もあるとしています。

- 同21日にはフィッシング対策協議会からも注意喚起が出されています。

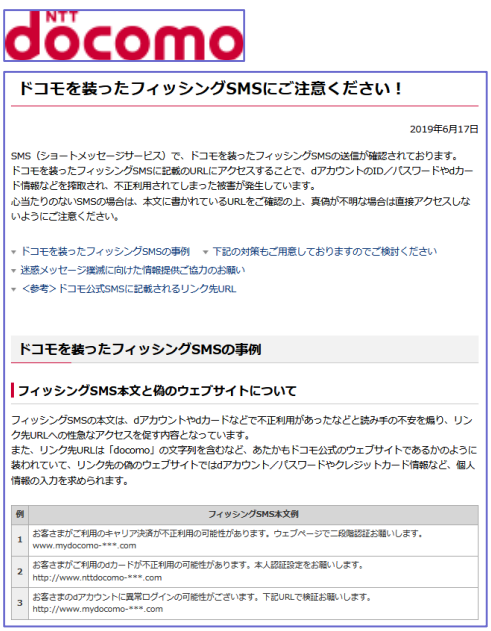
AUS便りからの所感等

- フィッシングSMSの一例として、本文に以下の文言が記載されたものが挙げられています。

◆ お客さまがご利用のキャリア決済が不正利用の可能性があります。ウェブページで二段階認証お願いします。
◆ お客さまがご利用のdカードが不正利用の可能性があります。本人認証設定をお願いします。
◆ お客さまのdアカウントに異常ログインの可能性がございます。下記URLで検証お願いします。

- ドコモからの注意喚起ページでは、回避策として「国際SMS拒否」機能を設定することを挙げている他、同社が実際に使用しているドメイン名の一覧も示されており、リンク先がこれらと異なるドメインでないか確認するのが良いでしょう。

- このような不審なSMSやメールを受信した際にフィッシング等を回避するための基本的な方策として「心当たりがないメッセージは開かない」「メッセージに記載されたURLへ安易に接続しない」「ID、パスワードを入力する際は、正規サイトであることを確認する」等に注意することはもちろん、Twitter等での報告がないか調査しつつ、落ち着いて行動して頂ければ幸いです。


ドコモを装ったフィッシングSMSにご注意ください！

2019年6月17日

SMS（ショートメッセージサービス）で、ドコモを装ったフィッシングSMSの送信が確認されております。
ドコモを装ったフィッシングSMSに記載のURLにアクセスすることで、dアカウントのID／パスワードやdカード情報などを搾取され、不正利用されてしまった被害が発生しています。
心当たりのないSMSの場合は、本文に書かれているURLをご確認の上、真偽が不明な場合は直接アクセスしないようにご注意ください。

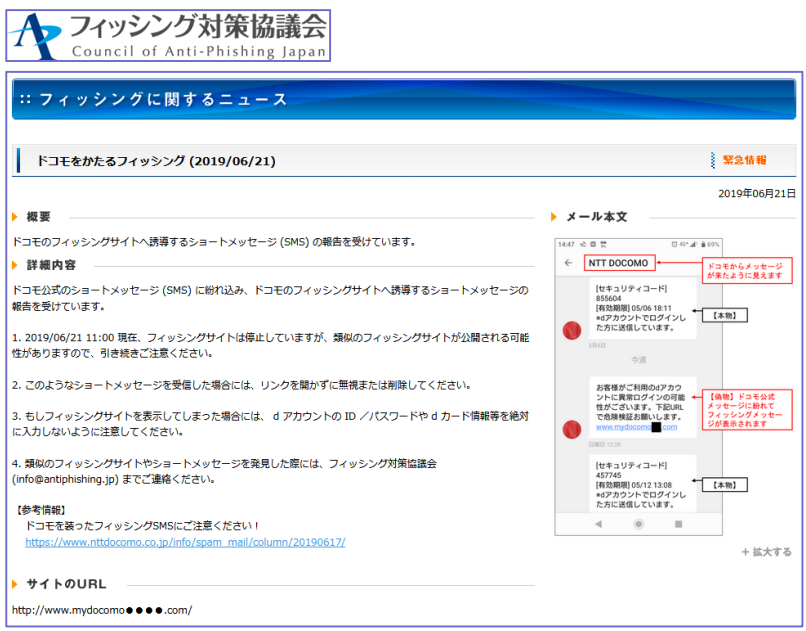
- ドコモを装ったフィッシングSMSの事例
- 下記の対策もご用意しておりますのでご検討ください
- 迷惑メッセージ撲滅に向けた情報提供ご協力のお願い
- <参考>ドコモ公式SMSに記載されるリンク先URL

ドコモを装ったフィッシングSMSの事例

フィッシングSMS本文と偽のウェブサイトについて

フィッシングSMSの本文は、dアカウントやdカードなどで不正利用があったなどと読み手の不安を煽り、リンク先URLへの性急なアクセスを促す内容となっています。
また、リンク先URLは「docomo」の文字列を含むなど、あたかもドコモ公式のウェブサイトであるかのように装われていて、リンク先の偽のウェブサイトではdアカウント／パスワードやクレジットカード情報など、個人情報の入力を求められます。

例	フィッシングSMS本文例
1	お客さまがご利用のキャリア決済が不正利用の可能性があります。ウェブページで二段階認証お願いします。 www.mydocomo-***.com
2	お客さまがご利用のdカードが不正利用の可能性があります。本人認証設定をお願いします。 http://www.nttdocomo-***.com
3	お客さまのdアカウントに異常ログインの可能性がございます。下記URLで検証お願いします。 http://www.mydocomo-***.com


:: フィッシングに関するニュース

ドコモをかたるフィッシング (2019/06/21)　緊急情報

2019年06月21日

概要

ドコモのフィッシングサイトへ誘導するショートメッセージ (SMS) の報告を受けています。

詳細内容

ドコモ公式のショートメッセージ (SMS) に紛れ込み、ドコモのフィッシングサイトへ誘導するショートメッセージの報告を受けています。

1. 2019/06/21 11:00 現在、フィッシングサイトは停止していますが、類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。

2. このようなショートメッセージを受信した場合には、リンクを開かずに無視または削除してください。

3. もしフィッシングサイトを表示してしまった場合には、 d アカウントの ID ／パスワードや d カード情報等を絶対に入力しないように注意してください。

4. 類似のフィッシングサイトやショートメッセージを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

【参考情報】
ドコモを装ったフィッシングSMSにご注意ください！
https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/

サイトのURL

http://www.mydocomo●●●●.com/

メール本文

NTT DOCOMO
ドコモからメッセージが来たように見えます
【偽物】ドコモ公式メッセージに紛れてフィッシングメッセージが表示されます
【本物】
【本物】
＋拡大する

●イオンカード不正利用約2,200万円、リスト型攻撃→アプリ不正登録で発生

https://this.kiji.is/512090474421929057

このニュースをザックリ言うと･･･

- 6月14日（日本時間）、イオン銀行とイオンクレジットサービス株式会社より、各社等で運営するイオンカードの公式サイト「暮らしのマネーサイト」において不正ログインが発生し、イオンカードの不正利用被害が生じたと発表されました。

- 5月28日～6月3日の間にカード会員数1,917件が不正ログイン、うち708件についてカードが不正利用されており、被害額は22,044,816円に上るとされています。

AUS便りからの所感等


KYODO
イオンカードで不正利用
2200万円、ネット被害
2019/6/14 11:24 (JST)　6/14 11:31 (JST) updated　©一般社団法人共同通信社
イオン銀行とイオンクレジットサービスは14日、会員向けインターネットサイトが不正アクセスを受け、クレジットカードが不正利用されたと明らかにした。1917件のアカウントに不正ログインがあり、不正利用の被害は判明分だけで708人の約2200万円に上る。個人情報も流出したとみられる。
イオングループのカード会員向けサービス「暮らしのマネーサイト」とスマートフォンアプリ「イオンウォレット」に5月28日～6月3日、不正ログインがあった。何者かが会員登録された電話番号を改変し、番号で認証できる別のスマホアプリと連携させることで、不正利用された疑いがあるという。

- 同社の説明によれば、いわゆる「リスト型攻撃」による不正ログインの後、電話番号を攻撃者のものに変更され、イオンカード公式のスマートフォン向けウォレットアプリとさらに別の決済アプリとの連携により、カードの不正利用が行われたとしています。

- ユーザ認証にはSMS等による二段階認証もあったと思われますが、一旦不正ログインされ、SMSによるチェックが行われないまま、そのSMSの送信先である電話番号を変更される等、一連の攻撃過程を阻止できなかったことは残念なことです。

- 今回についてユーザ側で実施可能であった対策は、リスト型攻撃への対策として度々挙げている「Webサービス毎に異なるパスワードを使用する」ことに尽き、これを行っていればカードの不正利用には至らなかったとも言えますので、二段階認証があるからとパスワードを安易なものや他のサイトと共通のものに設定するのではなく、確実に安全なパスワードを設定するよう心がけることを推奨致します。

●Firefoxのセキュリティアップデート相次ぐ…67.0.4あるいはESR 60.7.2へ更新を

https://internet.watch.impress.co.jp/docs/news/1191818.html

このニュースをザックリ言うと･･･

- 6月18日（現地時間）、Firefoxブラウザを提供するMozilla Foundationより、Firefoxを不正終了させられる可能性がある致命的な脆弱性が発見されたと発表され、セキュリティアップデートがリリースされました。

- 次いで同20日には、また別の脆弱性が報告され、再びセキュリティアップデートがリリースされています。

- 6月21日時点の最新バージョンは「Firefox 67.0.4」「Firefox ESR 60.7.2」となっており、Mozillaでは至急アップデートを呼びかけています。

AUS便りからの所感等


INTERNET Watch
「Firefox 67.0.4」リリース、サンドボックスを回避する脆弱性を修正
磯谷 智仁　2019年6月21日 13:57
Mozilla Foundation Security Advisory 2019-19
米Mozillaは20日、Firefoxの最新バージョン「Firefox 67.0.4」「Firefox ESR 60.7.2」を公開した。このアップデートでは危険度"high"の脆弱性を修正した。
サンドボックスの内外でやり取りされるメッセージの値検証が十分でない問題があり、サンドボックスで保護されていない親プロセスが、子プロセスから渡されたウェブコンテンツを開くことが可能になる。ほかの脆弱性を組み合わせることで、任意のコードを実行される恐れがある。
同脆弱性の影響を受けるのは「Firefox 67.0.4」「Firefox ESR 60.7.2」より前のバージョンになる。
最新バージョンへの更新は、メニューボタンの「ヘルプ」→「Firefoxについて」からアクセスできるバージョン情報ダイアログからアップデートできる。
6月18日に「Firefox 67.0.3」「Firefox ESR 60.7.1」を公開してからわずか2日でのアップデートとなる。

- 例えば18日のアップデート実施により、既に最新になったものと勘違いしている恐れも考えられますので、メニューボタン→「ヘルプ」→「Firefoxについて」にて、最新バージョンになっているか確認の上、そうでなければそこからアップデートを実施するようにしてください。

- 6月18日に発表された脆弱性の方は、その時点で既に悪用する攻撃が確認されていた（ゼロデイ脆弱性）とのことで、このようなケースではアップデートまでの間に攻撃を受ける恐れも考えられるため、アンチウイルスやUTM等による防御も併せて実行することが重要です。