フィッシングメールへの注意

フィッシングサイトについて

フィッシングサイトとは、実在する企業やサービスの公式サイトとそっくりの偽サイトを作成し、ユーザ ID やパスワード・個人情報を入手しようとするサイトのことです。

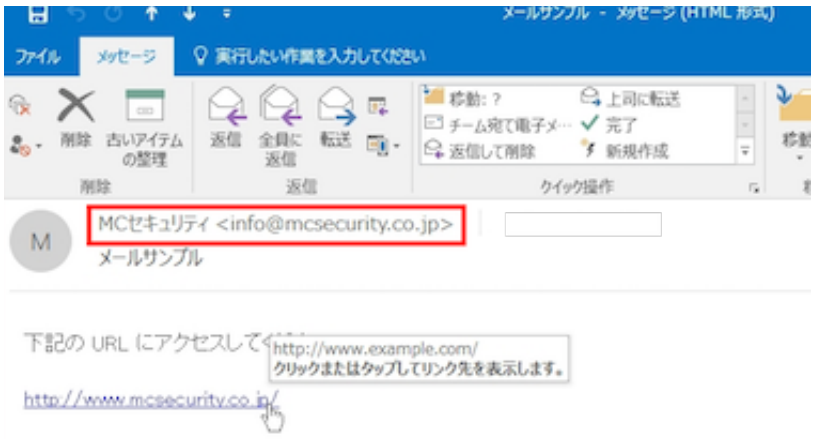
フィッシングサイトは年々巧妙になっており、本物と見分けがつかない程、精巧に作られていたり、公式の画像やアイコンを複製したサイトを作成し、偽物と分かりにくいサイトにしているケースが多くなっています。

メールを開く前、もしくはリンクをクリックする前に注意するポイントについてご説明しますので、メールを開かれる際には、気をつけていただければと思います。

メール内容の判断

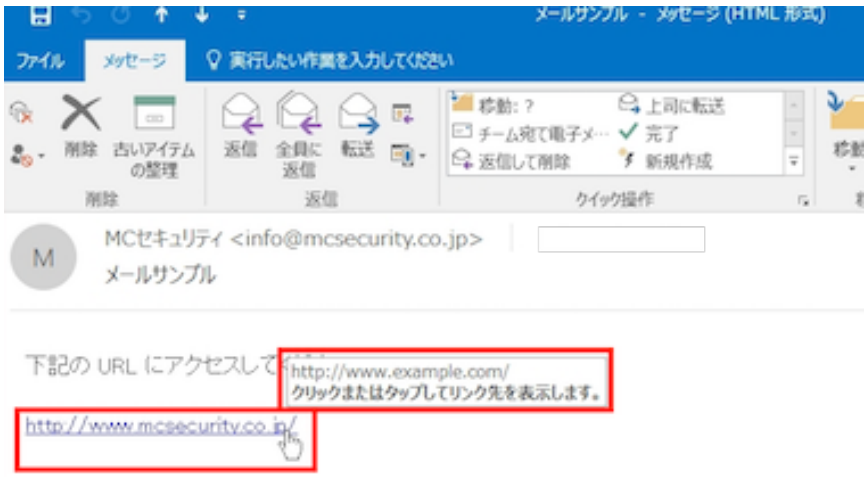
メールのリンクを開く際に注意していただきたい点は主に 2 点あります。

- 送信者(From：)
  下記の画面のように、メールの送信者アドレスは、ほとんどの場合、会社名や名前とメールアドレスが含まれる形式になっています。
  <> でくくられたメールアドレスが正規のものであるか確認してください。



  また、送信者のアドレスは偽装されている場合があります。正規のメールアドレスが表示されていても過信しすぎずに注意してください。

- リンクの URL
  メールの本文に掲載されている URL のリンクは、見かけの URL と本当に転送される URL が異なる場合があります。
  下記の画面は、MC セキュリティの URL(www.mcsecurity.co.jp)と見せかけて、別の URL(www.example.com)に転送されるリンクの例です。
  リンクの上にマウスポインタを持っていくと、実際に転送される URL が表示されます。
  クリックする前に、実際に転送されるリンク先を確認してください。



NetStable での検知

NetStable では、利用者が多い様々なサイトのフィッシングサイトを検知するシグネチャをリリースしています。

- 楽天を騙るフィッシングサイトへのアクセスを検知するシグネチャ
  sid:6100643 - 6100660 Rakuten Phishing URL SSL Request 129 ~ 146
  sid:6100661 - 6100664 Rakuten Phishing URL HTTP Request 71 ~ 74

- Amazon を騙るフィッシングサイトへのアクセスを検知するシグネチャ
  sid:6100627 - 6100628 Amazon Phishing URL SSL Request 122 ~ 123
  sid:6100629 - 6100642 Amazon Phishing URL HTTP Request 183 ~ 196

- 特定定額給付金に関する通知を装うフィッシングサイトへのアクセスを検知するシグネチャ
  sid:6100665 - 6100675 Soumu Phishing URL SSL Request 1 ~ 11
  sid:6100676 Soumu Phishing URL HTTP Request 1

- 三井住友銀行および三井住友カードを騙るフィッシングサイトへのアクセスを検知するシグネチャ
  sid:6100624 Mitsui Sumitomo Card Phishing URL SSL Request 1
  sid:6100625 Mitsui Sumitomo Card Phishing URL HTTP Request 1

- 日本郵政を騙るフィッシングサイトへのアクセスを検知するシグネチャ
  sid:6100626 Japan Post Phishing URL SSL Request 1

まとめ

- フィッシングサイトは年々巧妙になっていて、見分けるのが難しい
- 送信者が偽装されている場合があるので注意が必要
- メールの送信者とリンクの URL が正規のものかどうか確認が必要