

# サイバーセキュリティ・ニュース

## CS-NEWS

令和3年2月  
サイバー犯罪対策課

件名：【重要】●●から緊急のご連絡

利用規約違反により、アカウントを停止しました。本人確認のため、直ちにログインをしてください。<http://0000.00/>

「すぐに対応しなければ」と  
思わせる内容です！



送信元アドレスや件名  
などで、正規の送信者を  
装っています！

件名：●●宅配便

お荷物をお届けにありがとうございました。  
が不在のため持ち帰りました。  
下記よりご確認ください。

<http://0000.00/>

### フィッシング詐欺 の手法



2 受信者が  
メールを開封し、  
メール内の  
URL にアクセス

1 犯罪者が  
フィッシングメールを  
不特定多数に送信

3 偽サイトでアカウント情報  
やクレジットカード情報を  
入力させる

偽サイト (フィッシングサイト)



見た目は本物の  
ホームページにそっくり。  
絶対に入力しないで  
ください！

### 「フィッシング詐欺」にだまされないために

- 1 身に覚えのないメールは不用意に開かない。
- 2 メール内の URL を安易に押さない。  
(ID・パスワードの入力や、アプリのダウンロードを促すものは要注意)
- 3 正しいウェブサイトの URL は事前にブックマークに登録し、  
アクセスする際は必ずブックマークからアクセスする。
- 4 ログインの際、多要素認証<sup>※</sup>を使っているサービスを利用する。  
※多要素認証…本人確認を強化するため、パスワードに加えて複数の種類の要素  
(指紋や顔、合言葉など)を使う認証方式。
- 5 万一、不審なウェブサイトでパスワードなどを入力  
した場合は、警察安全相談電話や国民生活センター、  
地域の消費生活センターなどに相談する。

警察安全相談電話 ☎ #9110  
(つながらない場合は ☎ 059・224・9110)  
相談受付：9時～17時 (土日祝日・年末年始を除く)



「フィッシング詐欺」とは、実在する有名企業をかたるメールを使って「偽のウェブサイト(フィッシングサイト)へ誘導し、銀行口座やクレジットカード情報などの重要な個人情報やパスワードをだまし取る行為のことを言います。手口は年々巧妙化し、私たちの心理をついてくるものが多くなっています。被害に遭わないためにも、手口を知り、対策を理解することが大切です。

「フィッシング詐欺」にご注意

だまされないためには、知ることが大切です！

### テレワークも注意しましょう！

テレワークが急速に普及する中、サイバーセキュリティ対策を怠ると、パソコンなどのウイルス感染や重要なデータの流出につながります。下記の安全確認を徹底しましょう。

- パソコンの OS やウイルス対策ソフトは、常に最新の状態に更新する
- 自宅の Wi-Fi ルーターを使う場合は、ルーターの ID を初期設定から必ず変更する
- 知人や取引先を装うメールに注意し、安易に添付ファイルを開かない

2月1日(月)から3月18日(木)は

### サイバーセキュリティ月間です

この月間にあたって、サイバーセキュリティ対策を見直しましょう。対策に関する詳細は、県警察本部ホームページをご覧ください。

三重県 サイバー 🔍 検索



問い合わせ先 県警察本部 生活安全部 サイバー犯罪対策課 ☎ 059・222・0110 (代表)