CHECK フィッシング詐欺を見抜くためのチェックリスト

✓ Webサイトを閲覧するとき

1. リンクをクリックする前に、URLの上にマウスカーソルをかざして表示される「参照先」を確認する。
2. 個人情報を扱う正規Webサイトでは、通常HTTPS通信が使用される。ブラウザーに錠前マークが表示されているか確認する。

✓ メールを確認するとき

1. 「個人情報や認証情報を安易に要求してくる」メールに用心する。
2. 「心当たりがないタイミング」で、送られてくるメールは非常に疑わしい。
3. 「登録したものと異なるメールアドレスに届いたメール」は、一斉配信されたスパムメールの可能性あり。
4. 「期限を一方的に決めて早急な対応を求める」「威圧的・脅迫的な内容」のメールはスパムメールの可能性あり。
5. 「普段と異なるドメイン」から送信されたメールは危険信号。Web検索で届いたメールのメールアドレスを確かめるのもよい。
6. 「あいさつ文がない」「個人名を書いていない」等、普段と異なる書式のメールは疑わしい。
7. 「画像を読み込まない」「表示が崩れている」メールは危険。
8. 文法間違いやスペルミス等、「不自然な文章」のメールは注意する。
9. 「無意味な文字列」の件名は、通常ありえない。
10. 自身が使用しているメールクライアントの機能を再確認し、不審なメールはブロックする。
11. 日本の銀行やクレジットカード会社等の金融機関は、基本的にメールによる口座番号や暗証番号・本人確認は行っていない。
12. 会員番号を使用しないサービスから会員番号を含むメールが送られてきた場合は注意が必要。