月刊 赤松事務機 通信

2月

2017年2月号

❖ 【 お知らせ 】 ❖
Windows Liveメールのサポートが2017年1月10日に終了しました

マイクロソフトは2017年1月10日にWindows Liveメールのサポートを終了しました。

多くの方がWindows Liveメールを使っていたと思いますが、サポートが終了すると、セキュリティの脆弱性やプログラムのバグがあっても修正されることはなく、危険で不安定な状態になります。また、プログラムの提供が終了すれば、インストールすることもできなくなります。

サポートが終了しても現在使用中のWindows Liveメールが使えなくなるわけではないですが、トラブルにあわないためにも早めにメールソフトの移行を検討することをお勧めします。

❊今月の豆知識❊ ～ 内臓は食べられる魚と食べられない魚の違い ～

魚の内臓は苦味があるので、基本的には食べないで処理する必要がありますが、サンマのように内臓も美味しく食べられる魚もいます。
なぜこのような違いが生まれるのかというと、実は食べた食べ物を消化する時間が関係していると言われているのです。

【内臓を食べない魚】 例えば、タイのエサはエビやカニ、自分よりも小さい小魚で消化する時間はおよそ10時間をかけて消化します。内臓には胃があり、食べたエサを胃で消化するのですが漁で水揚げされたタイの胃の中には食べたエサが残っていて、これが苦味の原因となるので内臓を食べない、食べられないという事になります。

【内臓を食べる魚】 サンマのエサとなるのは小さな動物性プランクトン。エサを食べてから消化するまでの時間はおよそ30分と短い。なぜサンマの消化がこれほど早いのかというと、食べているエサがプランクトンであることもあるのですが、サンマは無胃魚という胃のない魚だからなのです。食べたものは30分程度で排出されるので内臓にエサが残っている事がなく内臓も食べることが出来るのです。
ちなみに、サンマの他にトビウオも無胃魚と言われています。トビウオは外敵から身を守るために海の上を飛んで逃げることがありますが、体を軽くして飛ぶために胃袋がないとされているのです。

❊information❊

弊社では、Office365Businessをお勧めしております。
また、情報セキュリティ対策でご心配や困ったこと等がございましたらお気軽に弊社までご相談下さい！
情報セキュリティに関する国家資格を持ったスタッフが、親身に対応させて頂きます！

赤松事務機株式会社
本社　TEL：087-833-3434　FAX：087-835-2485
岡山　TEL：086-271-1206　FAX：086-273-7356　URL：http://www.akamatsu-jimuki.co.jp

裏面へ

❖ 『OFFICEのプロダクトキーが不正コピーされています』フィッシングメールが大量拡散 ❖

1月12日の早朝に「ご注意!！OFFICEのプロダクトキーが不正コピーされています。」という件名のメールが大量拡散されました。このメールはOffice製品のプロダクトキー侵害の名目でマイクロソフトを偽装したフィッシングサイトへ誘導し、最終的にマイクロソフトアカウントからクレジットカード情報まで詐取することを狙ったものです。

1月12日早朝の数時間のみで日本国内で1万件以上の拡散が確認されています。フィッシングメール内に表示されている差出人は「support@microsoft-securityprotection-support」の文字列を含むアドレスになっており、マイクロソフトのサポートからのメールと誤解されることを狙ったものと考えられます。
本文では「オフィスソフトのプロダクトキーが違法コピーされた可能性」の名目で受信者に「検証作業」を要求します。誤解した受信者がメール本文の「今すぐ認証」部分のリンクにアクセスすると、マイクロソフトの正規サイトに偽装したフィッシングサイトへ誘導されます。このフィッシングサイトのURLは差出人のメールアドレスのドメインと同一であり、受信者の誤解を誘うための一貫性が見られます。

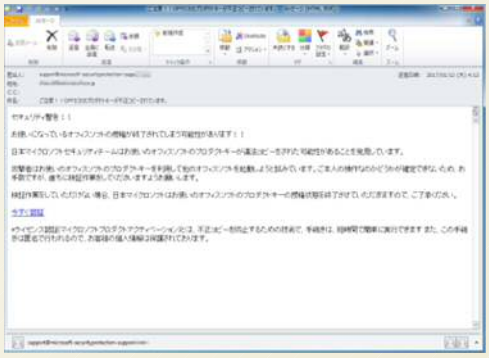

図1：今回確認されているフィッシングメールの例

このフィッシングサイト上ではメール本文と同じ警告文がポップアップ表示され、さらに受信者をあおります。ページ内の「今すぐ認証」のリンクをクリックすると、マイクロソフトアカウントのサインイン画面を偽装したページが表示されます。当然この画面はマイクロソフトアカウントの詐取を狙う偽画面です。

図2：誘導されるフィッシングサイトの表示例

サインインするとさらにアカウント認証のために必要、との名目で氏名や住所などの個人情報からクレジットカード番号やセキュリティコードまでの入力を促されます。

図3：フィッシングサイト上の偽のサインイン画面例

ここまでの情報を入力すると「修復が完了しました」との表示があります。メールやサイトがマイクロソフトのものと誤解したままの利用者は正規の手続きの様に感じ、だまされたことに気づかないかもしれません。

図4：フィッシングサイト上の「お客様情報追加」画面例

今回詐取対象となったマイクロソフトアカウントをはじめとして、Apple ID、Googleアカウントのように、複数のサービスの利用に使用可能なアカウントの情報はサイバー犯罪者にとって利用価値が高く、継続的に狙われる情報となっています。現在のスパムメール攻撃では短時間で送信を終える手口が多いため、今回のフィッシングメールに関しても2017年1月12日15時時点でさらなる拡散は見られていません。しかし同時にインターバルを置いて送信を繰り返す手口も多いため、今後も同様の手口のメールが拡散する可能性は高いものと考えられます。

図5：フィッシングサイト上の「修復完了」画面例

■ 被害に遭わないためには ■

攻撃者は自身の攻撃を成功させるために常に攻撃手口を変化させていきます。今回お伝えした攻撃の内容は次回から全く異なるものになっているかもしれません。常に最新の脅威動向を知り、新たな手口に騙されないよう注意を払ってください。また、そもそも不審なメールを可能な限りフィルタリングし、手元に届かないようにする対策も重要です。メールなどから誘導されるWebに関しては必ずURLのドメインを確認して下さい。

参考資料：ﾄﾚﾝﾄﾞﾏｲｸﾛｾｷｭﾘﾃｨﾌﾞﾛｸﾞ