迷惑メール被害防止対策

「ハッキングした！」というのは本当なの？

端末のハッキングを装う迷惑メールに注意！

ハッキングを装う迷惑メールとは？

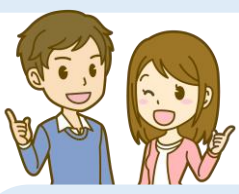
「端末をハッキングしてあなたの性的な映像を入手しました。」等と脅して
暗号資産（仮想通貨など）や電子マネーなどで金銭を要求します！

このような迷惑メールは、２０１８年ころから全国的に広まっており、新潟県内でも継続的に相談が寄せられています。

独立行政法人情報処理推進機構（IPA）の調査によれば、メール文中には盗んだとされる情報や画像・映像ファイルなどの添付はなく、単なる迷惑メールの可能性が非常に高いとされています。

このようなハッキングを装ったメールを自分のパソコンや携帯電話機で受信しても、金銭の要求に応じないようにしましょう。

出典：独立行政法人情報処理推進機構（IPA）安心相談窓口だより
「性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意」
URL：https://www.ipa.go.jp/security/anshin/mgdayori20181010.html



迷惑メールへの対処方法は？

受信したメールは無視する

このメールは、迷惑メールの一種の可能性が高いので、メールは無視し、金銭の支払いに応じないようにしましょう。

メール本文に記載されていたパスワードは変更する

万が一、メール本文の中に現在使用しているパスワードが記載されていた場合は、直ぐにパスワードの変更をしましょう。
また、サービスによって可能であれば２段階認証の設定を行いましょう。
パスワードは出来るだけ「長く」、「複雑」にし、複数サービスで使いまわさないようにすることが重要です。

プロバイダ、携帯会社、メールソフトなどのフィルタリングサービスや機能を使って迷惑メールのフィルタリングをする

迷惑メールをブロックするために、プロバイダ、携帯会社、メールソフト、ウイルス対策ソフトなどのフィルタリング機能を利用してメールのご利用環境ごとに、迷惑メールのフィルタリングしましょう。

※これまでに、撮影したとされる画像・映像ファイル等の情報が、メール内に添付されていたという事例や支払いに応じなかったため映像等が実際にばらまかれたなどの事例は確認されていないとされています。

迷惑メールの特徴は？

差出人と送信元いずれも自分のメールアドレスになっている場合があります!!

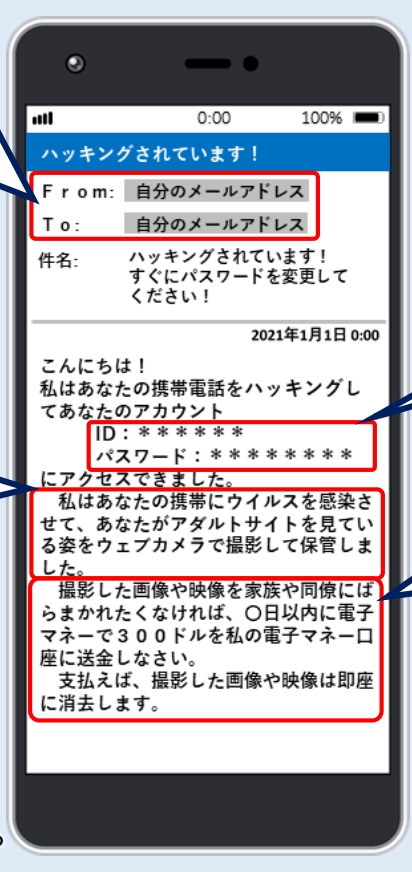
差出人のメールアドレスを受信者のメールアドレスに偽装して、あたかもメールアカウントがハッキングされていると信じさせようとします。
※差出人メールアドレスを偽装することは技術的に可能です。

アダルトサイトを閲覧している姿を撮影した 連絡先情報を収集した と脅します!等と書かれています!

事例の他にも「あなたが見たアダルトサイトにウイルスを仕込んだ。」「あなたの連絡先情報を収集した。」などの内容が書かれているケースもあります。

※文面にはいくつかのパターンが確認されています。

【メール受信画面の一例】
ースマートフォンの場合ー



自分のID・パスワードが記載されている場合があります!

受信者が実際に使用しているＩＤやパスワードが本文中に記載されている場合があります。「これがあなたのパスワードであることを知っている。」などの説明がされている場合もあります。
これは、過去に何らかの原因でデータが漏洩して、それをもとに記載されているものだと考えられます。
※流出経路と原因は分かりません。

暗号資産や電子マネーで金銭を要求します!

「撮影したあなたの画像や映像を家族や同僚にばらまかれたくなければ、ビットコインで＊＊＊ドルを支払え。」「支払えば、即座にデータは消去する。」などと記載されています。

※メールの内容は一例です。