

フィッシング詐欺誘引メール

大項目	電子メール
小項目	フィッシング詐欺誘引メール
タイトル	フィッシング詐欺誘引メール～フィッシング詐欺の手口と、その対策～
ねらい	「フィッシング詐欺誘引メール」の手口を理解し、メールが届いた時の適切な対処法を身に付けさせる。
作成の意図	<p>メールを使った詐欺の手法は様々なものがあるが、ここ数年問題になっているのが「フィッシング詐欺」である。</p> <p>そこで、「フィッシング詐欺」の大切な情報を盗み取る巧妙な手口を理解させ、フィッシング詐欺誘引メールが届いた時の適切な対処法を身に付けさせる。また、事例を知らせることで、年々巧妙化する手口に対する注意を喚起する。</p>
指導内容	<ul style="list-style-type: none"> ・フィッシング詐欺とは ・フィッシング詐欺の手口 ・フィッシング詐欺誘引メールが届いた時の対処法 ・トラブルに遭った時の対処法 ・フィッシング詐欺誘引メールに関連した被害事例
展開例	<p>(1) 情報モラル啓発資料を配付する。</p> <ul style="list-style-type: none"> ・現在、携帯電話を所有していない者も、一緒に考えさせるようにする。 <p>(2) フィッシング詐欺について考えさせる。</p> <p>① フィッシング詐欺について、理解状況を確認する。</p> <ul style="list-style-type: none"> ・フィッシング詐欺という言葉聞いたことがあるか発問し、生徒の挙手により確認する。 ・聞いたことがある生徒がいる場合は、その意味を知っているか尋ねる。 ・フィッシング詐欺とは、実際にある銀行やクレジットカード会社、オークション会社等になりすましメールを送り付け、それを通して不正に個人情報を入手しようとする詐欺行為であると説明する。 <p>② イラストを見ながらフィッシング詐欺の手口を理解させる。</p> <ul style="list-style-type: none"> ・実際にある銀行やクレジットカード会社、オークション会社等を装い偽メールを送り付け、その文中リンクから、受信者を本物そっくりの偽サイトに誘導し、銀行口座や暗証番号、クレジットカード番号やID、パスワード等を入力させ、不正に個人情報を入手すると説明する。 ・最近は、電子メールの送信者を詐称し、偽のWebサイトも本物のWebサイトと区別がつかないようにするなど、手口が巧妙化しており、フィッシング詐欺にひっかかるケースが増えていることを知らせる。 <p>(3) フィッシング詐欺誘引メールが届いた時の対処法について理解させる。</p> <p>① メールに書かれているURLをむやみにクリックしない。</p> <ul style="list-style-type: none"> ・あやしい電子メールには返信しない。書かれているURLにもアクセスしないようにさせる。 <p>② 個人情報やID、パスワード等を、むやみに入力しない。</p> <ul style="list-style-type: none"> ・自分の利用している銀行やクレジット会社からの電子メールであっても、個人情報やID、パスワードは不用意に入力しないようにさせる。 <p>③ メールの内容をそのまま信用せず、名前が使われた機関の窓口にお問い合わせ、確認する。</p> <ul style="list-style-type: none"> ・個人の重要な情報を尋ねる電子メールが届いた場合は、名前が使われた機関へ必ず電話等で問い合わせ、内容について裏付けを取るようにさせる。 ・「信頼できる会社は、電子メールで個人の重要な情報を聞いてくることはない」ことを知らせる。 <p>(4) トラブルに遭ってしまった時の、対処法について理解させる。</p> <ul style="list-style-type: none"> ・個人情報を入力した後で、フィッシング詐欺に遭ったことに気が付いた時は、すぐに保護者に相談するとともに、実際の銀行やクレジット会社に連絡をして、講座やカードの利用を止める。 ・被害に遭った場合には、すぐに最寄りの警察署か都道府県警察本部のサイバー犯罪相談窓口（フィッシング110番）に相談する。 <p>(5) フィッシング詐欺誘引メールに関連した被害事例を確認させる。</p>