<!DOCTYPE html>

<html>

<head>

<title> Phishing, Vishing, and Smishing</title>

</head>

<body>

<h1 style="background-color:orange;"> Phishing, Vishing, and Smishing</h1>

<p style="color:green;"> A more thorough description of these attacks can be found <a href="https://www.hp.com/us-en/shop/tech-takes/smishing-vs-phishing-vs-vishing" target="\_blank"> here. </a> </p>

<img src="data:image/jpeg;base64,">

<table>

<tr>

<th>Attack</th>

<th>Method of Contact</th>

</tr>

<tr>

<td>Phishing</td>

<td>Email</td>

</tr>

<tr>

<td>Smishing</td>

<td>Text message</td>

<tr>

<td>Vishing</td>

<td>Phone call</td>

</tr>

</table>

<h2 style="color:slateblue; font-family:impact;"> Phishing </h2>

<p> Phishing is attempting to trick people infto clicking on fraudlent links in emails. The link may contain malware or it could be a semmingly legitmitate form that asks people to enter private information such as online banking usernames and passwords. There are many ways attackers get people to click on the email, like titling it URGENT or sending from a email that looks legitimate at first glance but is mispelled by one character. Here is an example of a phishing email.

<img style="background-color:black;"src="https://www.msvu.ca/wp-content/uploads/2017/10/account-termination-phish-2022-09-29\_12-05-23.png" alt="alternatetext">

Here are some things to look out for if you're suspicous of an email:

<ul>

<li>Mispelling in email</li>

<li>Promise of compensation</li>

<li>Requests you enter personal information</li>

<li>Email was sent at an odd time (for example, sent at 4am)</li>

<li>Poor grammar and spelling</li>

</ul>

Here's another example of a phishing email. Often times, phishers will pretend the victim has unclaimed funds, and they need to enter information to be able to get the money.

<img style="background-color:gray;"src="https://www.pcrisk.com/images/stories/screenshots202301/abandoned-funds-email-scam-main.jpg" alt="alternate text">

<h2 style="color:slateblue; font-family:impact;"> Smishing </h2>

<p style="color:orange; background-color:black;"> Smishing is similar to phishing, except it is done over text. Never click on a link from a phone number that you do not recognize.

<img src="https://www.paloaltonetworks.com/content/dam/pan/en\_US/images/cyberpedia/screenshot-of-a-smishing-attempt.png?imwidth=480" alt="alternatetext" </p>

<h2 style="color:slateblue; font-family:impact;"> Vishing </h2>

<p> Vishing involves scammers calling victims, often using prerecorded robocalls, pretending to be a legitimate company to solicit person information. Read about some examples of vishing attacks <a href="https://www.incognia.com/the-authentication-reference/what-is-vishing-attack-definition-examples-and-tips-to-protect-from-it#:~:text=Vishing%20attacks%20examples%20include%3A&text=The%20fraudster%20calls%20the%20victim,number%20to%20resolve%20the%20issue." target="\_blank">here.</a>

</body>

</html>