What is Phishing?

Phishing, pronounced “fishing,” is a type of social engineering cyber attack that relies on email or text messages. Phishing messages appear to be from a legitimate sender and include a request for you to take some sort of action, the end result of which is obtaining sensitive information for malicious purposes. Phishing continues to be one of the greatest threats to online privacy and security, and it targets your personal information as well as firm information. Phishing messages that target personal information often appear to come from reputable companies, such as financial institutions, credit card companies, or benefit providers.

Other Types of Phishing

Spear Phishing

Spear phishing is a more targeted approach to phishing and is distinguished by three elements. First, the message appears to come from someone who is known and trusted by the recipient. Second, the message contains specific information that gives it credibility. And, third, the request in the spear phishing message appears to be reasonable, based on the alleged sender of the message.

Smishing

Smishing is text-based, or SMS (Short Message Service)-based, phishing scams. Smishing messages arrive in a mobile device’s message application in 140 characters or less and promise prizes or continuation of current services by requesting a number be called or a link in the message be clicked.

Best Practices - Avoid Becoming a Phishing Victim

Follow these practices to avoid being the victim of a phishing scam:

* Even if a message appears to be from someone familiar, if it contains a request that seems unusual, it is best to use caution and call the person to verify the request is legitimate. If using email or SMS to verify the request, do not use the Reply feature. Instead, open a new message and enter the recipient’s email or text address directly.
* Do not open an unexpected email attachment without first scanning it for viruses, even if the sender appears to be someone familiar.
* Always trust your instincts. If a message contains an unusual request for assistance or doesn’t sound like something the sender would write, contains incorrect details, or includes an unusual request, confirm the content with the sender.
* If an email message contains a link to a website, open a browser and type the website address directly or use a search engine to locate the website rather than click the link contained in the email message.

(Continued on Page 2)

Anatomy of a Phishing Email Message – Warning Signs

|  |
| --- |
| **6**. The message asks you to take action immediately, often to avoid a negative result; -OR- the message contains spelling or grammar errors that are unusual for this sender; -OR- the request is unusual and no advance verbal communication has been received.  **5**. When you mouse over a link in the message, the URL does not match the designated site or the URL contains a misspelling of the designated site; -OR- the message includes an attachment that doesn’t have a logical connection to the message itself or is very unusual for this sender.  **4**. The subject line doesn’t seem relevant to the content of the message itself, or shows that the message is a reply, but you did not send a message with that subject.  **3**. The email was sent to more than one person, or the other recipients are not familiar to you, or it seems like an unusual combination of recipients – for example, the recipients all have last names that start with the same letter, or the email is related to a client or case, but not all of the recipients work on that matter.  **2**. The date and time are unusual for this sender.  **1**. The sender is someone from your firm, but not someone with whom you normally work; -OR- The sender is familiar but not someone who normally communicates with you via email; -OR- You were not expecting to receive an email from this sender, and the email contains a link or attachment; -OR- The name in the **From** field is someone who works at your firm, but the email address is not their firm email address. |