April 2016
Volume 11, Issue 4

Phishing Emails and You

OhioDAS
SERVICE · SUPPORT · SOLUTIONS
DEPARTMENT OF ADMINISTRATIVE SERVICES

Office of Information Security and Privacy

From the Desk of Russ Forsythe, Interim Chief Information Security Officer

When it comes to email, we've all come across a phishing email that appeared to be a legitimate email. Phishers take advantage of the fact that it is difficult to know with absolute certainty with whom you are communicating via email. They use this uncertainty to pose as legitimate businesses, organizations, or individuals, and gain our trust, which they can leverage to convince us to willingly give up information or click on malicious links or attachments.

Be Aware of Phishing Scams

First and foremost you should utilize a spam filter (this service is should be provided by your email provider), keep all of your systems patched and your anti-virus software up to date. The second line of defense against phishing is you. If you are vigilant, and watch for telltale signs of a phishing email, you can minimize your risk of falling for one. Telltale signs of a potential phishing email or message include messages from companies you don't have accounts with, spelling mistakes, messages from the wrong email address (e.g. info@yourbank.fakewebsite.com instead of info@yourbank.com), generic greetings (e.g. "Dear user" instead of your name), and unexpected messages with a sense of urgency designed to prompt you into responding quickly, without checking the facts. "Resume" and "Unpaid Invoice" are popular attachments used in phishing campaigns. Here are some scenarios you may encounter:

An email appearing to be from the "fraud department" of a well-known company that asks you to verify your information because they suspect you may be a victim of identity theft.

An email that references a current event, such as a major data breach, with a malicious link to setup your "free credit reporting."

An email claiming to be from a state lottery commission requests your banking information to deposit the "winnings" into your account.

An email with a link asking you to provide your login credentials to a website from which you receive legitimate services, such as a bank, credit card company, or even your

> Social engineering refers to the methoc attackers use to manipulate people int sharing sensitive information, or taking a action, such as downloading a file Sometimes social engineers interact with the victim to persuade the victim to shar details or perform an action, such as entering information into a login page.