Phishing Emails – Don't Take the Bait!

Phishing emails are fraudulent messages designed to obtain your sensitive information and data or trick the recipient into installing malicious software onto a computer. Phishing is a common tactic used by cybercriminals and one of the most prevalent ways to infiltrate computer networks. Phishers will pose as legitimate businesses, organizations or individuals to gain the trust of their victims and convince them to willingly give up information or click on malicious links or attachments.

Phishing emails can be difficult to identify; however, being aware of the threat and being vigilant in examining emails can reduce your risk of falling prey to such an attack. The following Dos and Don'ts serve as helpful reminders to stop and examine email messages before proceeding.

Dos and Don'ts:

DO exercise caution with all email communications you receive, including those that seem to be from a trusted entity. Inspect the sender's information to confirm the email was generated from a legitimate source.

DO keep an eye out for telltale signs of phishing: poor spelling or grammar, the use of threats, or the URL does not match that of the legitimate site. If the message does not feel right, chances are it is not.

DON'T click on links embedded in an unsolicited email.

DON'T open unexpected email attachments. The attached files may be hiding malicious software.

DON'T send your personal information via email. Legitimate businesses will not ask users to send sensitive personal information through email.

DON'T post sensitive information online. The less information you post, the less data you make available to a cybercriminal for use in developing a potential attack or scam.

For more information on phishing scams, as well as steps to mitigate a phishing attempt, visit the NYS Office of Information Technology Services Phishing Awareness resources page at https://its.ny.gov/resources. You will also find phishing quiz resources on this page to test your phishing awareness.