MISSISSIPPI MANAGEMENT & REPORTING SYSTEM

Meeting the Management Information Needs for the State of Mississippi

Phishing Awareness
Posted: March 5, 2019

To further enhance our agency's cyber defenses, we want to highlight a common cyber-attack that everyone should be aware of – phishing.

"Phishing" is the most common type of cyber-attack that affect organizations. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details. Although we maintain controls to help protect our networks and computers from cyber threats, we rely on you to be our first line of defense. We have outlined a few different types of phishing attacks to watch out for:

- Phishing
  In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.

- Spear Phishing
  Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name, phone number, and refer to ***MS Dept. of Finance and Administration*** in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.

- Whaling
  Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically the CEO or CFO, and ask you for sensitive information (including usernames and passwords).

- Shared Document Phishing
  You may receive an e-mail that appears to come from file-sharing site like SharePoint alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.

What You Can Do

- To avoid these phishing schemes, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognize. Be especially cautious of .zip or other compressed or executable file types. You will receive emails from the following DFA agency addresses. DFASecurity.MAGIC@dfa.ms.gov or MASH@dfa.ms.gov.

- Do not provide sensitive personal information (like usernames and passwords) over email.

- Watch for email senders that use suspicious or misleading domain names.
- Inspect our URL carefully to make sure it is legitimate and not an imposter site. Our URL is https://portal.magic.ms.gov/irj/portal
- Do not try to open any shared document that you are not expecting to receive.
- If you cannot tell if an email is legitimate or not, please contact us at 601-359-1343 option 1.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

If you have any questions please contact the MMRS Call Center at 601-359-1343 or via email at mash@dfa.ms.gov.

Thanks again for helping to keep our network, and our people safe from these cyber threats. Please let us know if you have any questions.