



December 13, 2017

Cyber: Maryland Phishing Attack Offers Lessons for District of Columbia

Last month, a targeted phishing attack on a Maryland school district resulted in the theft of \$57,000 after criminals rerouted the direct deposit pay of dozens of employees. Authorities believe the individuals were targeted with emails tricking them into providing their credentials to a fictitious school human resource system.

- Phishing is the elicitation of user credentials or other sensitive information by masquerading as a trustworthy entity. It is most commonly conducted via email, texts, or phone calls.

DC's Homeland Security and Emergency Management Agency (HSEMA) encourages individuals to be aware of phishing. Below are characteristics to help identify a scam:

- Look for typos, incorrect logos, poor spelling, or weak grammar;
- Emails creating a sense of urgency such as an imminent legal threat or computer update alert;
- A request for account information—legitimate institutions will almost never ask for that information over email or phone;
- Claims from an organization's information technology or security department stating credentials need to be updated or changed;
- Spoof emails appearing to originate from a sender other than the actual source;
- Links with instructions to update an account—instead, navigate directly to the website through an internet browser;
- Verify the source by hovering over any link(s) to confirm hyperlinks go to the destination they claim. See the example below.

