



DEPARTMENT OF INFORMATION TECHNOLOGY

Thursday, August 27, 2020

Dear SCS Team,

To enhance Shelby County Schools cyber defenses, IT Security wants to highlight a common cyber-attack that everyone should be aware of – “Phishing.”

"Phishing" is the most common type of cyber-attack that affects organizations like ours. 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 and phone number and refer to a familiar company or service 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 district, typically the Superintendent or CFO, and ask you for sensitive information (including usernames and passwords).

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 wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Watch for email senders that use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they are legitimate and not imposter sites.
- 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 SCS IT for assistance.

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.

Regards,

Lakshmi Visvanathan
CIO, Shelby County Schools