Is that Email Real or Fake?

Email spoofing is when a cybercriminal fakes an individual's sender address so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in phishing attacks because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, with personal identifiable information (PII) such as login credentials, credit card numbers, date of birth, Social Security Number (SSN), etc.

Email spoofing is one of the easiest types of phishing used to get data from users without their knowledge. It can be done in different ways:

- Sending an email through a familiar username
- Sending an email impersonating your supervisors and asking for some important data, gift cards, or other urgent requests
- Impersonating the identity of an organization and asking employees to share sensitive data

Here is one example of spoofed email:

From: Mike Smith < jake.hackenstaff@my.com>
Sent: Saturday, April 09, 2019 7:36 AM
To: YOUR NAME <YOUR Name@kent.edu>
Subject: Urgent

Are you available?

--
Best Regards,

Mike Smith
(Your Manager)

While this email is simple and doesn't have any malicious attachments, it is using social engineering to get a response from an unsuspecting recipient. However, the sender's actual address doesn't match their actual email address (highlighted above).

Once someone interacts with this type of scam, the sender makes up an excuse about being in a meeting and wants the recipient to do an important favor as soon as possible. An example of a requested favor is for the recipient to purchase gift cards (iTunes, Amazon, etc.), scratch off the back to reveal the codes, send back a picture of the cards and codes. Remember to always check the

actual address of who the email is coming from. Many times, scammers will use a similar name, or try and add “Kent State” to the address to trick you.

If you are using a mobile device, sometimes the actual full sender’s email address does not automatically display. You can check the address by clicking on the “Details” link. This is usually located at the top of the email with the sender, recipient, and date information.

What should you do if you receive a spoofed email?

After you have investigated the sender’s address, you should verify with the sender of the email that the inquiry is legitimate through other trusted avenues (e.g. by verifying the request in-person/via phone call/via text etc.). If you do receive a request such as this via email, please report it immediately to your IT department and to the Office of Security and Access Management using these steps. **DO NOT RESPOND** to the sender.