WHAT IS THE CONCERN?
A new email phishing scam has been reported by several credible sources. The scam includes usernames and passwords that have been found in previous data breaches making the message more believable as users should recognize the password. The message reads that the sender has your password and possibly your username, and shows the password in the message. The message continues to say the sender placed malware on an adult site and since you have visited the site, the sender has a video of you viewing the site and urges you to pay an amount in bitcoin.

WHO IS AFFECTED?
Any user whose email may have been involved in a breach at any time.

WHAT ACTION DO I NEED TO TAKE?
Report the message to spam@ou.edu.
Use caution when:

- Receiving emails that you are not expecting
- Messages show a previous password you have used
- Messages that have an urgency to them, i.e. payment in 24 hours

Tips to Avoid Phishing:

- Take your time to read through the message – does it provide specific information or use general terms? i.e. does it list a specific website or generically say “website”
- Does it make sense coming to this email address? i.e using your work email address when it should be your personal email address
- Review our online security training to learn how to spot phishing messages