***WARNING ABOUT SCAMS !***

***The Oklahoma Employment Security Commission does not use text messages to reach customers, charge customers fees to use our website, or release customer debit card numbers to private companies! If you are contacted by text, telephone, or e-mail, do not give out your debit card number! If you suspect a scam involving any activity related to your unemployment claim or debit card, immediately report it to the Oklahoma Employment Security Commission at (405) 557-5400 or to the Attorney General's Public Protection Unit at (405) 521-2029.***

## Phishing Scam FAQ's

1. What is phishing, Smishing and Vishing?
Three popular ways fraudsters use to trick uneducated consumers into revealing personal information that can be then used to commit account take over or identity theft.

Phishing is when criminals spam thousands of computers with spoofed emails and copycat financial organization websites designed to fool consumers into revealing data such as credit card numbers, account usernames and passwords, social security numbers, etc.

Vishing is a social engineering technique for stealing information or money from consumers using the telephone network. The term comes from combining "voice" with "phishing".

Smishing is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device. It can also refer to Vishing attempts using SMS texting instead of calling consumers. SMiShing is short for "SMS phishing."

2. What does phishing/Vishing/Smishing look like?
It always purports to come from a trustworthy company. To gain the consumer's trust, criminals will hijack logos, letterheads, and include hyperlinks within the email or text message that appears to redirect to the company's official site or 800 numbers.

3. How do the scams work?
In common scams, the emails/texts/voice mails use pressure, by warning that failure to respond will result in the consumer no longer having access to their account. Other scams could claim that the company has detected suspicious activity in the account or is implementing new privacy software or identity theft solutions.

The same communication will provide a link to take the consumer to a copycat website, or an 800 number to call the "company". At that page or phone #, they

are prompted to enter personal information, which is then captured by the fraudster.

4. How do phishers get email addresses or phone numbers?
Most of it is completely random. The email or text messages are just generic enough to apply to anyone in many cases or the fraudsters will use very large organizations that have many customers. They will send these out to ranges of email addresses, phone number sequences, etc. Literally millions of these messages could be sent out in one attempt.

5. How does the consumer protect themselves?

- Be aware. Consumers need to know that these scams exist and are increasingly popular.
- Be suspicious. Consumers should be just as suspicious of phone calls and text messages as they are of e-mails asking for personal information.
- Never respond. The golden rule to avoid being phished is to never hit "reply" or click the links within a suspicious email. Likewise, never respond to the voice mail or text message using the numbers provided in the text message or voice mail message.

If the consumer is unsure, they should contact the institution directly using a published phone number.