Phishing

✓ Alaska USA will never call, email, or text you to ask for account information ✓ Learn to identify fraudulent emails and texts

Protect your confidential information by not responding to the fraudulent email and text scam known as Phishing.

Fraudulent emails and texts are sent by individuals who are attempting to steal confidential information, such as credit card numbers, Social Security Numbers, and passwords. These scams can be run from anywhere in the world.

How to know if an email or text message is a Phishing scam

- Look for misspelled words and other grammatical errors, although this clue is less common as crooks become more sophisticated.
- Before you log in to any secure site, check to make sure the Lock or Key icon is displayed in your browser. These symbols indicate that the page you are using will protect and keep confidential any data sent from your computer.
- Make sure the web address (URL) starts with "https" before entering confidential information (for example, https://www.alaskausa.org).

When the return address looks real

The return address on Phishing messages is "spoofed," or made to appear as an address different than the sender's actual address. Never rely on the return address to identify the sender, even if it seems like the message came from a trusted source. Remember, Alaska USA will never call or email you to ask for account information.

How your contact information is collected

In most cases, the crooks don't know your email address, phone number, or where you live. They will locate a vulnerable mail server and send fake messages to every address on it, or obtain a list of email addresses and phone numbers and send their Phishing attacks to everything on the list. Computer viruses can also cause messages to be sent from an infected machine without the user's knowledge.

What you can do

Most email programs have spam filters that will help keep harmful or dangerous emails out of your inbox. However, if you suspect that a message is a potential Phishing scam, here are some tips:

- Never click on the links contained in the message, or open any related attachments.
- Set up security systems on your mobile devices and add your phone numbers to the Do Not Call Registry
- If you aren't sure if the message can be trusted, open a new browser window and type the business address in yourself, or contact the business by phone. If the email is indeed a scam, you can report it and set your mind at ease at the same time.
- Help friends and family avoid the dangers of Phishing by sharing your knowledge with them. Although anyone is a potential victim to this form of fraud, it can be particularly effective against people who are unfamiliar with computers. Phishing victims "drop their guard" because of a combination of confusion, panic, or the promise of an easy reward. Help educate friends and family who may be uncomfortable with computer technology, or perhaps too trusting for their own good.

Terms to know

Phishing
The practice of sending a fraudulent email or text that looks like a legitimate message. When you click a link within the message, you're asked to provide information such as pass codes and financial details.

Spoofing
Making a return address on an email look different than the sender's real address.

https
One indication that a site is legitimate: the web address will start with "https."