Text Scams

Text scams can have a variety of fake messages attached. Texts may claim that you have won a free prize and have to click on the link provided to receive it, or that you ordered a product and need to click a link to verify the order, or that your account has been suspended and you should click the link to activate service.

Do not believe every text you receive. As a rule, companies cannot send you text messages unless you opt-in to receive them. If you receive a text message from a company you have not permitted to contact you in this way, proceed with caution. In fact, any unsolicited text message should be considered a potential scam.

Here are some tips to help determine if the text is a scam:

- **Think before you click.** Do not click on links in strange or suspicious text messages. This is likely an attempt to gain access to your personal information or install malware on your device.

- **Confirm the information.** If an offer seems strange or too good to be true, contact the company directly by looking up their official contact information online. Call or email customer service to find out if the text message you received is legitimate.

- **Ignore instructions to text "STOP" or "NO".** Even if you realize the message is a scam, **do not text back for any reason**. Scammers may want you to text back to verify that your phone number is an active one. Instead, simply block the number so you will not receive messages from it in the future.

- **Double down on security.** If you clicked on the link, do a security sweep for viruses or any malicious software on your device and update your login credentials.

- **Report any encounters with a scam.** Share your scam experiences to help warn and protect others at BBB Scam Tracker or to the FTC.