



SCAM ALERT

Scam: Phishing - Fake Emails Target: All Seniors

Phishing is when a scam artist sends an email or text pretending to be a legitimate business in order to obtain access to your personal information through you or through infecting your computer or cell phone with malware. This convincing phishing scam lures you in when you assume the sender is legitimate.

The messages look real, will have correct company colors and the subject line seems legitimate. The body of the message instructs you to click on a link and access the shared file. *Don't fall for it! This is a scam!* The link downloads malware to your device so that scam artists can capture your passwords and obtain sensitive and personal information.

Phishing Scam: Fake emails from scam artists!

The Better Business Bureau (BBB) offers the following suggestions on how to spot a phishing scam:

- ✦ *Be wary of unexpected emails that contain links or attachments.* Do not click on links or open files in unfamiliar emails.
- ✦ *Check the reply address.* One easy way to spot an email scam is to look at the reply email. The address should be on a company domain.
- ✦ *Don't believe what you see.* Just because an email looks real; it doesn't mean it is. Scam artists can fake anything from a company logo to the email address from which they are sending the email.
- ✦ *Consider how the organization normally contacts you.* If an organization normally reaches you by U. S. Mail, be suspicious if you suddenly start receiving emails or text messages without ever opting into these new forms of communication.
- ✦ *Be cautious of generic emails.* Scam Artists try to cast a wide net by including little or no specific information in their fake emails. Be especially wary of messages from services you have not subscribed to or companies you have never done business with in the past.

**If you think you may be a victim of a scam, contact
San Bernardino County Adult Protective Services (APS) at
877-565-2020, or your local police department.**