Scam Alerts – Phishers

From: Putnam County State Bank – To keep it from happening to you

The definition of Phishing (from Dictionary.com) is trying to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.

The scammer usually sends out emails, but now they are moving to cell phones and texting.

The scam works this way:

- The scammer sends a text message impersonating your bank.
- The text message contains a link to a website, supposedly your bank's website.
- The website will look genuine and will ask for personal details to unlock or verify your account.

What you need to do (How to respond):

- **NEVER** follow a link that is provided in an unsolicited text or email, even one that you have to manually type in.
- **NEVER** provide confidential information unless you know the site is secure. A secure website address will begin with https instead of http. There is also a padlock in the address bar of your browser.

The aftermath:

- If you have clicked on a link like this, remove your computer from the internet and have it cleaned by a professional.
- If you gave out account information, call your bank.
- Change your passwords.
- Report it to the Federal Trade Commission https://www.ftccomplaintassistant.gov.
- Tell people you know about the call.