

SEPTEMBER &
OCTOBER 2022



MON - FRI: 9AM - 4:30PM | SAT: 9AM - 12PM | OPEN 24/7 @ WFSAVINGS.COM

322 MAIN ST, LATROBE, PA 15650 | (724) 539-9755

PLEASE NOTE

**Westmoreland
Federal Savings
will be closed on
Monday,
September 5,
2022,
for Labor Day
and also
Monday,
October 10,
2022,
in observance of
Columbus Day.**



Random Text Threats

Be careful. That unexpected text from the US Postal Service (USPS), Sam's Club or Home Depot telling you about an unclaimed package or a short survey you can complete to claim a nice freebie is not from them. It's a scam.

The Federal Trade Commission (FTC) has seen a recent spike in reports from folks getting text messages that look like they're from well-known businesses, but they're actually from impersonators. The details vary, but the scammers are after the same thing — your money and your personal information.

You may receive a text from someone pretending to be USPS and asking you to confirm your debit card details, so you can get an undelivered package. Or you may see a text about a chance to win a free gift card or a new power drill. To claim your "reward," you just have to click on the link, answer a few questions and maybe pay for shipping. Don't do it.

If you click on the link and submit your card information, you will end up with nothing — but later, you'll probably find unauthorized charges posted to your account. No matter what the random text indicates, the advice is the same.

- **Don't click on links or respond to unexpected texts**, especially ones asking you to fill out surveys to get free stuff. If you think it could be legitimate, contact the company using a website or phone number you trust. Don't ever use information in a random text message.
- **Don't pay to get a package redelivered.** The real USPS will not contact you out of the blue about a delivery (unless you submitted a request first) and they'll never demand payment to redeliver a package.

(Source: FTC "Don't click on that random text. It's a scam." by Gema de las Heras August 8, 2022)



10 Tips to Stay Scam Safe

Although you probably have heard many of these before, some things are worth repeating ...

- 1) If something looks too good to be true, it probably is!
- 2) No reputable website or business will ask for your password!
- 3) Use strong passwords. Longer passwords are better than shorter ones. Avoid using personal details like your birthdate and house number.
- 4) Do not share passwords among different websites or services.
- 5) Never give personal information (Social Security number, bank account or credit card number, driver license, etc.) over the Internet, unless you completely trust the entity.
- 6) Watch for phishing emails or phone calls. Do not get too chatty with strangers.
- 7) Be wary of what you post on social media. Do not broadcast to the world you are on vacation. Then everyone knows your house is empty!
- 8) Avoid quizzes or questionnaires about yourself on social media. While it may be tempting to see what type of dog you are or what song was written for you, many of these questions are similar to security questions that enable access to your accounts.
- 9) Never let someone remotely access or control your computer. Always be cautious of any website that claims to "fix" or "repair" your computer. They can get into your information or hold your computer ransom.
- 10) Reputable organizations do not engage in hard sell or pressure tactics. If someone is demanding an immediate decision without allowing you time to think, the answer is simple ... NO!

(Source: COMMUNITY NEWS "Be on the lookout for scams! Be smart! Stay Safe!" by Amy L. McLendon Spring & Summer, 2022)



Inheritance Inquiry?

The FTC has been getting reports of people receiving letters in the mail from a law firm. They say they're looking for the heir of a multi-million dollar inheritance. And they think it might be you. (Spoiler alert: It's not.)

They offer to split the inheritance with you, their law firm and some charities. They also say you have to keep this a secret and reach out to them by email immediately.

So what's really happening? This is not a lawyer — it's a scammer. And if you email them, they'll probably try to get your personal information, like your Social Security and bank account numbers, and, ultimately, your money. And that inheritance? It doesn't exist.

If you get one of these letters . . .

- Don't respond. Keep your money — and your information — to yourself. Never send money or information to a stranger who promises big rewards.
- Pass this information on to a friend. You probably throw away these kinds of letters. But you may know someone who could use a friendly reminder about scams.
- Report it at [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/report-fraud).

(Source: FTC "Contacted about a long-lost relative's inheritance? Hold on a minute." by Joseph Ferrari August 10, 2022)

