

Slow your Scroll: Spot and Avoid Social Media Scams



You have been advised when shopping online to check things out before checkout. The same advice applies to giveaways on social media sites like Facebook and Instagram. Want to avoid scams on your feed? Slow your Scroll!

Scammers watch businesses on social media and may hijack legitimate giveaways and promotions to [try and get your personal and financial information](#). Imagine your favorite photographer is giving away a free photo session. You follow the steps to enter — liking their page, tagging a few friends, and sharing the post. Then someone who looks like the business owner tags you in a comment saying that you've won. They send you a link — and ask for private financial information like your account number, credit card number or social security number— to claim your prize. What's your next step?

Before you respond, pause. Don't click on any links since they [might contain malware](#). Then:

- Ask yourself: Does this business need information like my social security number to get this free prize? If it's legit, probably not!
- Contact the business using a phone number, email, or website that you know is real. Ask if they really sent the message. If they didn't, report the post and let them know that their account may have been hacked.

Learn more about how to spot, avoid, and report scams—and how to recover money if you've paid a scammer—at [ftc.gov/scams](#). If you spot a scam, report it to the FTC at [ReportFraud.ftc.gov](#).

If you have any questions, please call our Customer First Contact Center at (203) 462-4400
(Monday – Friday (excluding bank holidays) from 8:30 a.m. to 4:30 p.m.)