# Protect your benefits from scammers during the holiday season

**Image:** Included in toolkit.

**Suggested Alt Text:** Smiling young women and caption” Stay safe while online shopping.

VA is committed to protecting the benefits of our nation’s heroes. The holiday season is an optimal time to remind Veterans and their loved ones to remain vigilant, to protect their sensitive information, and to verify the security of websites when shopping online.

That’s why VA’s Office of Financial Management teamed up recently with the Federal Trade Commission for a video interview to help warn Veterans to stay safe from digital scammers during the holidays.

## Beware of these scams

There is a spike in digital criminal activity this time of the year, especially with online scammers preying on the generous nature of Veterans with bold [**charity scams**](https://consumer.ftc.gov/features/pass-it-on/charity-fraud). Charity scammers use deception to steal money from people who believe they are donating to legitimate charities. Scammers often exploit natural disasters and other emergencies to take advantage of donors’ sympathy and their generosity. [**Learn more about fraud prevention tips**](https://www.va.gov/files/2023-09/disaster-one-pager_0.pdf) for natural disasters or emergencies.

Additionally, there is a significant increase in smartphone scams. “[**Jack Juicing**](https://www.fcc.gov/juice-jacking-tips-to-avoid-it),” for example, is when bad actors hack public USB ports to infiltrate malware or monitoring software. Be extra careful with charging your devices in public places like airports, hospitals, coffee shops, and other popular public recharging stations.

The latest scam, known as “[**smishing**](https://www.fcc.gov/avoid-temptation-smishing-scams),” sends spam SMS text messages to your smartphone. Text messages purport to be from reputable companies, such as your bank, and are sent to obtain passwords or credit card numbers when you click on the link provided. Bad actors are crafty and will contact Veterans pretending to be government representatives, including working for the [**Federal Bureau of Investigation (FBI)**](https://consumer.ftc.gov/consumer-alerts/2022/11/fbi-wont-ask-you-money-thats-scam), or that they work for [**utility companies**](https://consumer.ftc.gov/articles/scammers-pretend-be-your-utility-company).

Never provide your sensitive personal information or passwords to questionable sources. We advise you to hang up and call the company or business directly.

Find out more information from the FTC at https://www.ftc.gov.