HAVE YOU BEEN VICTIMIZED? SUBMIT A COMPLAINT (AND SAY YOU'RE MILITARY WHEN ASKED) TO THE CONSUMER FINANCIAL PROTECTION BUREAU: CONSUMERFINANCE.GOV/COMPLAINT OR CALL 855-411-2372.

Don't Get Scammed

To help you protect yourself against schemes that target service members, we compiled advice from three experts: Holly Petraeus, director of the Office of Servicemember Affairs at the Consumer Financial Protection Bureau (CFPB); ID theft expert Robert Siciliano of BestIDTheftCompanys.com; and Shana Mueller, communications and marketing director at TruthInAdvertising.org

SCAM

Payday Loans

WHY IT SEEMS LEGIT:
A short-term cash advance in which you pay a fee to borrow money (for example, a $15 fee for every $100 borrowed) and are expected to repay it in a short time, usually in a couple of weeks.

RED FLAGS: The average annual percentage rate is 390 percent. If you roll over the loan repeatedly because you can't pay it off, the cost can skyrocket, Petraeus says.

WHAT YOU CAN DO: Go to a military relief society, where you can get emergency loans at zero percent interest. Specifically, Guard Soldiers can try Army Emergency Relief (703-428-0000).

SCAM

Mortgage "Relief"

WHY IT SEEMS LEGIT:
A mortgage relief company offers help with your mortgage problems if you pay an advance fee.

RED FLAGS: The fee itself is the red flag, Petraeus says. Mortgage relief companies cannot collect any fees until they have provided you with a written offer from your lender that is acceptable to you and a document from the lender describing key changes to your mortgage. You have the right to reject the offer without any charge.

WHAT YOU CAN DO: Get real help with your mortgage by calling the CFPB at 855-411-CFPB (2372). They will connect you to a U.S. Department of Housing and Urban Development–approved housing counselor. Report any companies that have tried to charge advance fees to the CFPB.

SCAM

Account Fraud

WHY IT SEEMS LEGIT:
This is pure theft. Someone has accessed your Social Security number and opened new lines of credit under your ID while you are deployed.

RED FLAGS: Unfortunately with this type of fraud, the thief usually uses a drop box using your ID, so you'll be in the dark.

WHAT YOU CAN DO:
Before deploying, place an "Active Duty alert" on your credit report. This requires creditors to verify your identity before granting credit in your name. It lasts for one year but can be renewed, says StopFraud.gov.

SCAM

"Work at Home" Job Offers

WHY IT SEEMS LEGIT:
A company promises big bucks to sell its product or service, and you can work from home. All you have to do is recruit more people to sell for you. Military members are targeted because "they have a large group of people to interact with," Mueller says.

RED FLAGS: Your compensation is primarily based on how many participants you recruit rather than how many actual products you sell. This, by legal definition, is a pyramid scheme. Some companies have an "auto order" requirement, meaning they automatically send you more products to sell and charge your credit card. You might decide to stop selling, but the company continues to charge you anyway.

WHAT YOU CAN DO:
Before you agree to a work-at-home job, compare the suggested retail price of the product online with others. Then hit eBay and search for the product. Too many sellers equal excess inventory, low prices and little to no profit for you. Also, calculate business expenses, which also eat into profits. And if you derive more money from recruiting others than by selling, walk away.

SCAM

Phishing

WHY IT SEEMS LEGIT:
Criminals will send a targeted email posing as a government agency, says Siciliano. But they'll ask you for passwords, and then you'll become susceptible to takeover. Siciliano adds that fake charities do the same thing, claiming they support military families.

RED FLAGS: Look for emails with requests for personal financial information. Phishing emails also contain links that, if clicked, will plant spyware on your device or direct you to a website where your keystrokes can be monitored or intercepted.

WHAT YOU CAN DO:
Check your online financial accounts once a week to ensure no one has infiltrated them. If you've been compromised, get a credit freeze: Follow steps for your state at ConsumersUnion.org. With fake charities, realize that "Veterans" and "military families" in a company's name does not mean those people will benefit from the money. The Department of Defense recommends that you instead refer to MilitaryOneSource.mil.

©SHUTTERSTOCK