

Gesa

FRAUD & SCAM AWARENESS GUIDE

Be on the *alert*. Stay *informed*.



Every day, consumers worldwide receive offers sounding too good to be true. Scammers will target people of all ages and backgrounds, looking to take your heart, money or identification. Stay alert to these potential scams and stay informed on what you can do to prevent yourself from being a victim.

COMMON VICTIMIZATION SCAMS



Romance Scams

These scams involve romantic intention towards a victim, gaining their affection, and then using that goodwill to commit fraud. Fraudulent acts may involve access to the victims' money, bank accounts, credit cards, passports, email accounts, or personal identification.



Lottery Scams

Lottery scams often begin with an unexpected email notification, phone call, or mailing explaining that "You have won!" a large sum of money in a lottery. The target of the scam is then asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but will never receive any lottery payment.



Craigslist Scams

Craigslist scams take on many shapes and forms; being overpaid on a sale, paying via an online escrow service, and/or renting or buying unavailable property listings.



Compassion Scams

Compassion scams involve a parent or grandparent being contacted by an "authority" who claims that the child/grandchild is in some sort of trouble (legal or medical) and will need funds wired immediately in order to help the child.



SCAM WARNING SIGNS

Gesa is here to help you be on the lookout for common red flags that will help you indicate whether or not you are being targeted.



Romance Scams

- Asked to chat offline and keep your relationship a secret.
- Asked to wire money.
- Asked to give up your Online Banking credentials, accounts numbers, or PINs.



Lottery Scams

- You are told you'll win a contest you didn't enter.
- Offered "too-good-to-be-true" prizes.
- You have to pay to win.



Craigslist Scams

- The person only wants you to use their resources for payment.
- The person asks for personal information (Social Security Number or bank account number).
- The person rushes the transaction, making you feel leery about it.



Compassion Scams

- Contacted by an individual claiming they are an "authority."
- Asked to wire money.

WHAT ARE THE POTENTIAL IMPACTS TO YOU?

Engaging in any potential scam may result in many negative impacts to you. Impacts could include:



A loss of goods and/or money that cannot be traced or recovered by Gesa



Identity theft



Negative impacts to your credit history



Loss of membership at Gesa Credit Union



Online Banking can be compromised

What can I do to protect myself from fraud?

- ➔ Do not send money.
- ➔ Do not engage with the scammer. Cut off all communication.
- ➔ Only deal with people locally and in person.
- ➔ Increase security settings on social media.
- ➔ Do not accept friend requests from people you do not know.
- ➔ Limit personal information that you post.
- ➔ Be a skeptic – If it appears too good to be true, it most likely is.

Who should I contact if I think I am a victim of fraud?

- ☎ Contact the local police.
- ✉ Report any suspicious correspondence via email to reportfraud@gesa.com.
- 🌐 Report internet fraud to IC3 at www.ic3.gov/default.aspx.