Avoid these Zelle® and P2P Pay Apps Scams!

How to AVOID SCAMS Presented By:

OMEGA Federal
omegafcu.com

"Zelle Yourself" Scam

- Fraudsters send a text alert to members –appearing to come from the credit union –asking the members if they attempted a Zelle transfer
- Spoofing the credit union's phone number, fraudsters call members who respond 'NO' and claim to be from the credit union fraud department
- Fraudster tells member the Zelle transfer went through –however, the stolen funds can be recovered
- Fraudster explains to recover the stolen funds, the member must use Zelle to transfer the money to himself/herself using the member's mobile number
- The Zelle transfer is actually sent to the fraudster

How do fraudsters pull this off?

- Fraudster establishes a Zelle account with member's mobile phone number
- Cons member into disabling member's mobile phone number associated with member's Zelle account
- Instructs member to Zelle funds to himself/herself using member's mobile phone number
- Fraudster receives the funds

OMEGA will never contact you to request that you send money using Zelle to anyone, including yourself, or to share a code to resolve fraud.

Stay Vigilant.
Don't become a victim of a payment scam.

"Nearly 18 million Americans were defrauded through scams involving digital wallets and person-to-person (P2P) payment apps in 2020."
The New York Times, Javelin Strategy & Research

3 Tips to Avoid Crowd Funding Scams

How to AVOID SCAMS Presented By:

OMEGA Federal
omegafcu.com

1. Research the creator of the campaign.

Does their name appear in other scams?
Are they claiming to do something that seems too difficult as a solo project?
Or seems outside of their area of expertise?
If anything you find raises a flag, that's a good sign you should steer clear of that campaign.

2. Ask yourself whether the project seems realistic.

Several GoFundMe accounts have been set up, by a single individual, with the goal of fighting ISIS.
Unless you're Rambo, that's probably not a good idea.
Not only is the idea crazy—it's also completely unrealistic.
Say "no, thanks" to these crowdfunding campaigns.

3. Don't let emotion get the better of you.

When it comes to need-based donations, make sure you can verify the truth of the claimed need.
As in the case of the Iowa woman, some scammers are more than willing to fake illnesses and accidents to prey on kindhearted donors.

You've heard the saying "buyer beware?"
When it comes to crowdfunding campaigns,
we have two words for you: donor beware!

On-line Job Scam Warning Signs

How to AVOID SCAMS Presented By:

OMEGA Federal
omegafcu.com

Job Fraudsters

There are many on-line job scams that take advantage of job seekers in a variety of ways. Scammers have several purposes, depending on the scam—to collect confidential information to use for identity theft, to get you to cash fraudulent checks or to wire or send money, and to get you to pay for services or supplies.

Job scams are posted on Craigslist and other job boards and forums, as well as on social networking sites like Facebook and Twitter. In other cases, you may receive unsolicited emails from scammers. It's important to be vigilant and check out every job you're interested in to make sure it's legitimate.

How do fraudsters pull this off?

- You're offered a job without an application, interview, or discussion with the employer.
- The company asks you to wire money or asks for your credit card information.
- You are told you have to pay for training.
- You're asked to cash a check and forward some of the money to a third party.
- You are promised high pay for not much work.
- The salary details aren't clear. If the company doesn't pay an hourly rate or a salary, carefully investigate the details.

Investigate the Company

1. Googling the company name plus "scam" or "rip-off" will give you some information on the company if it's not legitimate.
2. Visit the company's website and if they don't have one or it doesn't have contact information, consider that a warning sign.
3. Check out the company with the Better Business Bureau. www.bbb.org

3 Ways to Spot Student Loan Scams

How to AVOID SCAMS Presented By:

OMEGA Federal
omegafcu.com

1. You're Asked to Pay an Upfront Cost or Monthly Fees

A student loan debt relief company asks you for payment in exchange for help navigating your student loans. However, there's nothing they can do that you can't do yourself, especially with the help of your loan servicer. If you're having a hard time making your monthly payments, your loan servicer can work with you to switch to a more affordable repayment plan at any time, at no additional cost to you.

2. You're Promised Immediate Loan Forgiveness

No one can promise immediate and total student loan forgiveness or cancellation. A student loan debt relief company may claim to get rid of your loans quickly, but most government forgiveness programs require many years of qualifying payments and/or qualifying employment in certain fields before loans can be forgiven. Your loan servicer can also help you determine if you qualify for loan forgiveness, at no cost.

3. You Must Provide Your FSA ID Password

Neither ED nor your loan servicer will ask you for your FSA ID password. Your FSA ID is used to sign legally binding documents electronically. It has the same legal status as a written signature. Do not give your FSA ID password to anyone or allow anyone to create an FSA ID for you. And if the debt relief company collects fees from you, but never actually makes any payments on your behalf, you will still be responsible for those outstanding payments, interest accruals, and late fees.

Think You've Already Been Scammed?

The Federal Trade Commission (FTC) has taken legal action against the following student loan debt relief companies:

- AI DocPrep, Inc.
- American Student Loan Consolidators (ASLC)
- Alliance Document Preparation
- Student Aid Center
- Strategic Student Solutions
- Student Debt Doctor (SDD)
- Student Debt Relief Group (SDRG)

Source: https://studentaid.gov/articles/student-loan-scams/