Fraud

When individual/s (also called fraudsters or scammers) misrepresent (unfair, dishonesty, trick) themselves or a service for financial gain.

COMMON FRAUD SCHEMES

Phishing Scams

Look For: Texts, calls and emails claiming to be from a company and asking for personal information. This can look like a text appearing to come from the credit union! The scammers are usually trying to obtain full card information or online banking credentials.

What to Do: Don't share online banking credentials with anyone. No legitimate company (or FI) will ask for your online banking credentials.

Do not call numbers from a text or email. Go to a verified website to find a trusted number to call.

Identity Theft

Look For: Requests for your personal information like Social Security number (SSN) or bank details.

What to Do: *Do not share this information* unless you are sure of the recipient's* legitimacy.

Housing Scams

Look For: Rental listings that require a deposit before you see the property.

What to Do: Always visit the property and meet the landlord in person before paying.

*Social Security numbers are asked for by employers, credit unions or banks (financial institutions), welfare offices, credit reporting agencies, and the Department of Motor Vehicles (DMV).

Government Impersonation Scams

Look For:

- People pretending to be immigration officials or from other law enforcement agencies.
- Government agencies demanding money over the phone.

What to Do:

- Government agencies do not demand or threaten payment over the phone.
- Call a government agency directly from a trusted phone number to verify.

Employment Scams

Look For:

- Jobs that ask you to send money as part of the employment process.
- Jobs that send you money and ask you to buy things like gift cards or ask you to send the money to someone else in the company.
- Jobs that ask you for your online banking information.

What to Do:

- Legitimate employers do not ask for money to hire you.
- Legitimate employers will never ask for your online banking credentials.
- Legitimate employers will not make you use your personal banking accounts to conduct transfers on behalf of the business.

HOW TO PROTECT YOURSELF

1. **Verify Credentials**

Action: Always check the credentials of anyone offering services, especially related to immigration, employment, or housing.

2. **Do not trust offers you didn't seek out or ask for**

Action: If an offer seems too good to be true, it probably is. Be cautious of unsolicited (unwanted, not asked for) phone calls, emails, or messages.

3. **Use Trusted Resources**

Action: Rely on official government websites and reputable (respected, trusted) organizations for information and assistance.

4. **Don't trust caller ID. Scammers can make any name or number show up on your caller ID.**

Trusted Resources in Vermont - Vermont Refugee Resettlement Program, Association of Africans Living in Vermont, Vermont Immigration and Asylum Advocates, and Vermont Professionals of Color Network.

REPORTING FRAUD

Federal Trade Commission (FTC)

Action: Report fraud at ReportFraud.ftc.gov. Your credit union or bank can help you with this.

Local Law Enforcement/Police

Action: Contact your local police department to file a report.

Internet Crime Complaint Center

Action: Run by the FBI. Used to report internet crimes.

RESOURCES FOR VICTIMS

Vermont Attorney General's Office

Consumer Assistance Program offers guidance for scam victims.

Office for Victims of Crime

Support: Provides resources and support for victims of fraud.

FINRA Foundation

Support: Offers guides and support for those affected by financial fraud.