ST. JAMES
Episcopal
CHURCH

Scam Awareness:

A guide to common scams and protection options

Based on guidelines provided by the Office of Consumer Protections
Updated August 2025

Table of Contents

Common Types of Scams:

Resources for Scam Recovery:

Imposter Scams

These scams may include:

1. Someone contacting you with an urgent or "time-sensitive" message.
2. Demanding money or info now to pay taxes/fees or assist someone you love.
3. Talks with a false sense of authority.
4. May ask you to keep the transaction private.
5. Asks for money to be wired or transferred through cryptocurrency or bitcoin.

Scam Ex: "Rev. Rowan" emails you saying they are in a meeting and urgently need gift-cards or electronic payments.

Imposter Scams

How to avoid these scams:

1. NEVER wire money or purchase gift-cards for someone who contacts you asking for money.
2. Avoid using bitcoin machines or transfer cryptocurrency - this is most likely a scam.
3. Never give your card number over the phone.
4. Tell a trusted individual about the interaction, ESPECIALLY if you are asked to keep transactions private.
5. Report the call to the OCP.

Law Enforcement Scams

<u>These scams may include:</u>

1. Someone contacting you saying there is a warrant for your arrest or failed to appear for jury duty.
2. Demanding you pay a fee to avoid charges.
3. May use the real names of judges and police officers.

Scam Ex: A "sheriff" calls you saying that you failed to appear for jury duty and you must pay a fine over the phone to avoid an arrest warrant.

Law Enforcement Scams

How to avoid these scams:

1. Government agencies will NEVER ask you to wire money or cold call you.
2. Immediately hang up the phone.
3. Do NOT send any money.
4. Call your local non-emergency law enforcement number to validate their claim.
5. Report the call to the OCP.

Grandparent Scams

<u>These scams may include:</u>

1. A call from a "family member" informing you that they are in trouble and need money.
2. They may ask you to keep this secret from other family members.
3. They need money immediately and urgently.
4. Remember: AI can be used to mimic the voice of your loved ones.

Scam Ex: Your "granddaughter" calls you saying she was arrested and needs you to bail her out. She tells you to wire her money and not tell her parents.

Grandparent Scams

How to avoid these scams:

1. NEVER give away any personal information over the phone to ANYONE.
2. Contact multiple family members before trying to resolve the crisis yourself.
3. Ask questions that only a family member would know the answer to.
4. Limit conversation with the scammer. Do not reply at all if possible, as the scammer will increase their efforts if you engage.
5. Do not answer numbers you don't recognize - let the call go to voicemail.

Tech Support Scams

<u>These scams may include:</u>

1. A pop-up enrolling you in a fraudulent tech maintenance or warranty program.
2. A pop-up informing you that your device has been "hacked".
    a. Clicking these links often installs mal- or spyware on your device.
3. Requests for financial info to fix the hack.
4. Redirection to fake tech support websites.
5. Your computer or device getting hijacked.

Scam Ex: A pop-up appears on your phone saying you have been hacked and need to click on the link to "prevent" the hack.

Tech Support Scams

How to avoid these scams:

1. NEVER give away any personal information over the phone to ANYONE.
2. Do not give remote access of your device to an unknown 3rd party.
3. Avoid searching online for "Tech Support"- this frequently leads to scam websites.
4. Take your computer or device to a local repair shop to get it cleaned.
5. Change the passwords to your social media/email/bank accounts from a known, clean computer.
6. You may want to reach out to your bank to request a freeze on your bank account.

Sweepstake Scams

These scams may include:

1. Someone notifying you that you won a sweepstake or instant winnings that you did not enter.
2. They often ask for an upfront fee to cover the cost of the sweepstake transfer.
3. They will contact you via mail or online, letting you know you won something.

Scam Ex: Mail arrives at your house letting you know that you won $1000, but you need to send in cash and personal information to claim your reward.

Sweepstake Scams

How to avoid these scams:

1. Remember that foreign lotteries and sweepstakes are illegal in the USA.
2. You cannot win a sweepstake or other type of winning that you did not apply for. This includes lottery tickets.
3. NEVER pay fees "required" to get access to money.
4. Remember that sweepstakes are delivered in person to your home, NEVER via mail or online communication.
5. Immediately throw away or delete these communications.

Romance Scams

<u>These scams may include:</u>

1. A fake dating or online media profile.
2. They may target divorced or older individuals, but everyone is susceptible.
3. No face-to-face communication.
4. Requests for financial assistance with things like medical bills and flights.
5. Someone claiming to be from the USA but saying they working overseas.
6. They say they will come to visit but "emergencies" keep coming up.

Scam Ex: You have never met your partner in person, and they have cancelled all meetups, but have "medical bills" they need help with.

Romance Scams

How to avoid these scams:

1. Beware of declarations of "love" or "destiny" that occur fast.
2. Notice refusals to speak on the phone or meet in-person.
3. Beware of individuals who claim to be from the USA but are away as part of military service or business travels
4. Discuss your relationship with someone you trust and disclose if your partner is asking for financial assistance.
5. Demand to speak via FaceTime or another form of video communication to verify who you are talking.

Home Improvement Scams

<u>These scams may include:</u>

1. Contractors not setting a project end date.
2. Someone performing unwanted work on your home without permission.
3. Someone claiming they were "working in the neighborhood" and offering to fix something on your home.
4. Not having the correct licensing and insurance information.

Scam Ex: A repairman in the neighborhood rings your doorbell and offers to repave your driveway, without you calling them or requesting an estimate.

Home Improvement Scams

How to avoid these scams:

1. Get many estimates from various contractors.
2. Call the city or OCP to verify the contractors insurance, workers comp, and bond information.
3. Get all estimates in writing.
4. Have a clear, distinct contract with a specificied **end date** for the project.
5. Have any contract changes put in writing.
6. Make sure to research all contractors that you work with, both by verifying information with the city and checking their online presence and reviews.

Other Common Scams

<u>These scams may include:</u>

1. Text scams saying:
    a. You missed a toll bill.
    b. Your package was undeliverable.
    c. An unknown number is asking how you are.
    d. You were approved for a loan you didn't apply for.
    e. Your card was used an a store you didn't shop at.
    f. You are eligible for a job or offer you didn't apply for.
2. Phone calls asking you to donate to specific organizations.
3. Packages delivered to you that you didn't order.
4. QR Codes that install malware on your device.

Other Common Scams

How to avoid these scams:

1. NEVER respond to text messages from unknown senders or click on links in messages that you are unsure of.
2. Do not answer calls from unknown numbers.
3. Ask family and friends to leave voicemails for you to respond to if they are calling from an unknown number.
4. Delete all of these messages from your phone.
5. Remember, most financial institutions will NEVER text you, especially asking for confidential information.
6. Return unknown packages to the post office or refuse delivery.

Other Common Scams

How to avoid these scams:

7. Call the official number of the organization claiming to be texting you and verify if the message is real.
    a. Call your bank if you got a message saying your card was used for a fraudulent purchase.
    b. Verify the identity of people soliciting donations by calling the organization.
8. Make sure you know the organization you are scanning a QR code from. Try to enter the website address if possible.

Freezing your Credit

Freezing your credit prevents someone from opening accounts under your identity:

1. There are 3 companies you must freeze your credit with:
    a. **Experian (888-397-3742)**
    b. **Transunion (800-680-7289)**
    c. **Equifax (800-525-6285)**
2. To open a new card or take out a loan, you must unfreeze your credit. You may:
    a. Unfreeze for 30 days
    b. Permanently unfreeze your credit.
    c. Permanently unfreeze with notices when accounts are opened.
3. Remember your passwords! It is hard to unfreeze the accounts without them!

End of Life Registry

If you are someone with an Advanced Directive (AD) and you are worried about someone taking advantage of your estate or end-of-life plans, you may register your AD on the End-Of-Life Registry:

1. Complete an AD with your doctor.
2. Go to **https://app.mt.gov/registry/**
    a. Submit your AD to the registry. This registers your AD with the state and prevents your information from being stolen, as well as prevents individuals from taking advantage of your estate.
    b. This also ensures that any end of life directives are honored, such as Do Not Resuscitate orders.

Reporting a scam to the Office of Consumer Protections

1. The Office of Consumer Protections (OCP) is the Montana fraud protection agency.
2. Alert the OCP when you are the victim of scam, identity & contractor theft, lemon-laws, door-to-door salesmen fraud, credit and debit card fraud, unauthorized repairs, fraudulent medical billing and more.
3. To contact the OCP:
    a. **Website:** https://dojmt.gov/office-of-consumer-protection/
    b. **Email:** contactocp@mt.gov
    c. **Phone:** (406)-444-4500

Federal Protection Options

1. You can also report fraud to the FBI at the following web address:
    a. **www.ic3.gov**
2. Add yourself to the DONOTCALL registry through the federal government's website. This decreases the number of spam calls that go to your phone.
    a. **https://www.donotcall.gov/**
3. Register at the following website to opt of out junk mail at your physical address:
    a. **https://dmachoice.org/**