

Ohio Attorney General Mike DeWine warns of

SCAMS TARGETING OHIOANS



Computer Repair Scams: An "employee" of a computer company contacts you claiming your computer has a virus and offers to "fix the problem." The person asks for access to

your computer, which allows the scammer to install malicious software designed to scan your computer for personal information or to lock your computer so that you cannot use it until you pay a "ransom" to unlock it.



Imposter Scams: Someone contacts you pretending to be from a government agency, such as the IRS or the local court. The person demands immediate payment, likely for back taxes or an old court fee, and threatens arrest if payment is not made immediately. The scammer may also request personal information, such as your Social Security number.

Fake Check Scams: Someone sends you a check or money order and asks you to deposit it in your account and wire-transfer back the money, minus a nice

bonus for you, a "thank you" for helping. Regardless of the pitch, the result is the same: The check or money order you received is counterfeit. It will be returned to your bank unpaid, and the full amount will be deducted from your account.

Phishing and Spoofing:

Scammers use clever emails, websites, phone calls, and text messages to "phish" for information by posing as legitimate businesses.

Never give personal information to someone who contacts you unexpectedly, even if they say they are from a trusted source, such as your bank. Scammers can use "spoofing" to disguise the phone number that appears on your caller ID to make their ploys seem more convincing.



Grandparent Scam:

A con artist poses as your grandchild, claims to be in trouble, and asks you to send money via wire-transfer or prepaid card. If you're suspicious, ask a question only a family member would know how to answer, and call your son or daughter to confirm the claim.



Romance Scams: A con artist meets the victim online or over the phone and claims to be temporarily located overseas — perhaps due to a military assignment or mission trip. After developing a relationship, the scammer eventually asks the victim to send money to pay for airfare, medical expenses, or military fees. In reality, there was never "true love," and any money sent will be lost.



Sweepstakes Scams:

Someone falsely claims you have won the lottery or a contest that you never entered. All you need to do to collect the winnings is prepay a fee or a tax. However, your winnings will never arrive because the lottery or contest is fake. Legitimate sweepstakes are free and require no upfront payment.



Home Improvement Scams: Door-to-door contractors offer to repair your roof, pave your driveway, or trim your trees for a great price. After you pay, the contractor disappears without doing the work or after doing a poor job. Never pay in full upfront. If you are solicited at your home, you have three days to cancel the contract, and work should not begin within that period.



MIKE DEWINE

* OHIO ATTORNEY GENERAL *

For information or assistance, visit
www.OhioAttorneyGeneral.gov
or call 800-282-0515.

Phony Charities: Scammers invent fake charities. To verify the legitimacy of a charitable group before making a donation, call the Ohio Attorney General's Help Center at 800-282-0515.

TIPS for AVOIDING SCAMS

ALWAYS:

- Be skeptical when someone requests immediate payment via wire-transfer, prepaid money card, or gift card.
- Look into businesses through the Ohio Attorney General's Office and the Better Business Bureau.
- Beware of strangers who seek new, quick, personal connections with you or a loved one.
- Research charities through the Ohio Attorney General's Office.
- Keep your personal information private and shred documents containing such information.



NEVER:

- Send money via wire-transfer, prepaid money card, or gift card to a stranger.
- Give personal information to someone who has contacted you unexpectedly.
- Carry unnecessary personal information, such as your Social Security card or Medicare card, in your wallet or purse.
- Pay to win a prize or sweepstakes.
- Allow someone "remote access" to your computer.
- Pay the full amount upfront before any work has been done.



OTHER SMART STEPS:

- Use a credit card, rather than debit card, cash, or check. The Fair Credit Billing Act offers certain protections that other payment methods don't.
- For transactions involving large amounts of money sent over the phone or Internet, you may wish to keep a log of who you spoke with and when, their contact information, and any money paid.
- Check your credit report(s) at least once a year at www.annualcreditreport.com or by calling 877-322-8228. If you notice unfamiliar accounts, contact the three major credit reporting agencies (Experian, Equifax, and TransUnion). Also, contact the Ohio Attorney General's Identity Theft Unit at 800-282-0515.

Remember, if it sounds too good to be true, it probably is!



CONSUMER RESOURCES

Annual Credit Report
877-322-8228
www.annualcreditreport.com

Equifax
800-525-6285
www.equifax.com

Experian
888-397-3742
www.experian.com

TransUnion
800-680-7289
www.transunion.com

Better Business Bureau
www.bbb.org

Direct Marketing Association
212-768-7277
www.dmachoice.org

National Do Not Call Registry
888-382-1222
www.donotcall.gov

OptOutPrescreen.com
888-567-8688
www.optoutprescreen.com



MIKE DEWINE
* OHIO ATTORNEY GENERAL *

For information or assistance, visit
www.OhioAttorneyGeneral.gov
or call **800-282-0515**.