

SCAMS TARGET OHIOANS



Computer Repair Scams: An “employee” of a computer company or government agency contacts you claiming your computer has a virus and offers to “fix the problem.” But first you need to provide personal information or payment. The person may even request remote access to your computer.

By granting access or clicking on links, you may be allowing a scammer to install malicious software designed to scan your computer for personal information or downloading a virus.



Identity Theft: Identity theft occurs when someone fraudulently obtains and uses your personal information — such as a bank account number or Social Security number — without your permission to obtain credit, take out a loan, receive medical treatment, or otherwise pretend to be you. Protect yourself by shredding documents and keeping personal information private.



Fake Check Scams: Someone sends you a check or money order and asks you to deposit it in your account and

wire-transfer him the money, minus a nice “thank you” for helping. Regardless of the pitch, the result is the same: The check or money order you receive will be counterfeit. It will be returned to your bank unpaid, and the bank will deduct the amount from your account.

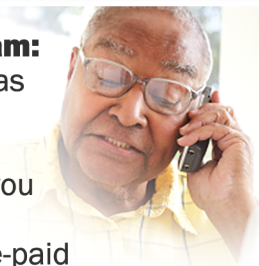
Phishing and Spoofing:

Scammers often use clever emails, websites, letters, phone calls, and text messages to “phish” for information. 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 pre-paid credit 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.



Health Care Scams: Someone contacts you claiming to offer a “free” medical alert device, but first you must provide a bank account or credit card number. In addition to unauthorized charges, you may be risking identity theft. Scammers may also ask for a copy of your Medicare card, which lists your Social Security number.



Sweepstakes Scams:

Someone may falsely claim 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 up-front payment.



Home Improvement Scams: Door-to-door contractors will offer to repair your roof, pave your driveway, or trim your trees for a great price. After you pay, the contractor disappears without doing any work or after doing a poor job. Never pay in full up front. If you are solicited at your home, you have three days to cancel any 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: Ohio law requires charities to register with the Ohio Attorney General’s Office. Before you donate, verify the charity is legitimate by calling the Attorney General’s Help Center, **800-282-0515**.

TIPS for AVOIDING SCAMS

ALWAYS:

- Look into businesses through the Attorney General's Office and Better Business Bureau
- Shred all documents that contain personal information before discarding them
- Beware of strangers who seek new, quick, personal connections with you or a loved one
- Research charities through the Attorney General's Office

NEVER:

- Send money by wire-transfer or pre-paid credit card to a stranger
- Pay to win a prize or sweepstakes
- 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
- Accept verbal estimates rather than getting the exact cost and all promises in writing
- Make large down payments

OTHER SMART STEPS:

- Use a credit card, rather than a debit card, cash, or check. The Fair Credit Billing Act offers certain protections that other payment methods don't.
- Check your credit report(s) at least once a year at www.annualcreditreport.com or by calling **877-322-8222**. If you notice unfamiliar accounts, contact the three major credit reporting agencies (Experian, Equifax, and TransUnion) and file a police report immediately. 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

Better Business Bureau
www.bbb.org

Federal Trade Commission
877-382-4357
www.ftc.gov

Ohio Department of Insurance
800-686-1526
www.insurance.ohio.gov

Ohio Legal Services
866-529-6446
www.ohiolegalservices.org

Equifax
800-525-6285
www.equifax.com

Experian
888-397-3742
www.experian.com

TransUnion
800-680-7289
www.transunion.com



MIKE DEWINE
★ OHIO ATTORNEY GENERAL ★

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