Office of the Indiana Attorney General
Consumer Protection Division

Beware of these common scams

Nigerian Scams

People claiming to be officials, businessmen or surviving relatives of former government officials in countries around the world send countless offers via e-mail, attempting to convince consumers that they will transfer thousands of dollars into your bank account if you will just pay a fee or "taxes" to help them access their money. If you respond to the initial offer, you may receive documents that look "official." Unfortunately, you will get more e-mails asking you to send more money to cover transaction and transfer costs, attorney's fees, blank letterhead and your bank account numbers and other sensitive, personal information.

Tech Support Scams

A tech support person may call or email you and claim that they are from Windows, Microsoft or another software company. The person says your computer is running slow or has a virus and it's sending out error messages. Scammers will ask you to visit a website that gives them remote access to your computer. If the caller obtains access they can steal personal information, usernames and passwords to commit identity theft or send spam messages. In some cases, the caller may even be asked for a wired payment or credit card information.

Lottery Scams

In foreign lottery scams, you receive an email claiming that you are the winner of a foreign lottery. All you need to do to claim your prize is send money to pay the taxes, insurance, or processing or customs fees. Sometimes, you will be asked to provide a bank account number so the funds can be deposited. In reality, your bank account is likely to be depleted. You end up shelling out your hard earned money for "winnings" you will never receive.

Phishing Emails

Phishing—also known as carding or brand-spoofing—is a type of deception designed to steal your identity. In a phishing scam, a thief tries to get information like credit card numbers, passwords, account information, or other personal information from you by convincing you to provide it under false pretenses.
In a phishing scam, the messages often look very authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes.

Overpayment Scams

In check overpayment scams, the con artist responds to an item you may have for sale online. They send you a check payable for more than the agreed upon price along with a reason why they are writing the check for more. They ask that you deposit the amount in your bank account and wire or transfer the extra amount to a foreign account. The scammer vanishes after the money is deposited. At that point, the check bounces and you are required to pay for the entire amount.

Disaster Relief Scams

Every time there is a disaster like the tsunami, a tornado or an earthquake, millions of do-gooders want to do something to help the victims. Scammers take advantage of this by setting up scam charity institutions which rob the money that you wanted to send to the victims of the disaster. Scammers also attempt phishing by sending you donation requests via email where you can click on a link which then leads you to website designed to steal your passwords and other details.

"Free" Trial Offers

Misleading free trial offers online for diet supplements, penny auctions and money making schemes blanket the internet resulting in thousands of complaints ever year. The free trial offers seem no-risk but complainants state they were repeatedly billed every month and found it extremely difficult to cancel.

Grandparent Scam

In this case, a victim receives a phone call from someone claiming to be their grandchild who is visiting another country and in need of emergency funds. The phone is quickly handed off to someone claiming to be law enforcement, a medical professional or an attorney. The scammer goes on to explain they can take care of the situation quickly and return the grandchild home if a money wire is sent immediately. The caller will try to convince the victim not to call police or contact other family members.

Credit Repair Scams

Advertisements often promise miracles in repairing bad credit reports. Credit service organizations tell consumers that for a fee, bad credit, judgments, bankruptcies and bad debts can be erased from credit reports forever, or that a new credit identity can be created that will solve all the consumer's credit problems. In reality, such ads promise things that cannot be delivered. Indiana law requires that For-Profit Credit Service Organizations:

- Have a written contract with consumers describing in detail the services to be performed.
- Provide consumers with a three-day right to cancel the contract.
- Maintain a $25,000 bond to be used to satisfy consumer claims.

Work from Home Schemes

The thought of earning a lucrative salary from the comfort of home is a tempting one – and that's precisely why so many organizations take advantage of unsuspecting Hoosiers through "work at home" business opportunities. Learn how to avoid being taken advantage of by knowing what to look for.

- A business opportunity is commonly referred to as a "work at home" job. Examples of common business opportunities include:
  - Envelope stuffing
  - Transcribing medical records
  - Operating vending machines
  - Setting up display racks
  - Internet malls
  - Warehouse Worker
- Be wary of investment amounts just under $500 (for example $495) as this is likely an indication that the seller is trying to avoid regulation as a business opportunity seller.
- Most business opportunities are advertised in the classified sections of newspapers or through Internet sites and promise a large monthly income while allowing you to be your own boss and set your own hours.

Fake Debt Collectors Scams

A person receives a call from someone claiming to be a debt collector trying to collect payment for a past due account. The caller tries to convince the person to make payment over the phone by relaying their routing and checking account numbers. This information can be used by the caller to try to access the victim's account online or to create fake checks. They also may provide an address where a personal check can be sent. Many times the victim's check is altered, resent to another potential victim and the dollar amount is changed. The victim may lose money from his accounts and has to change account numbers as a result.

Home Repair Scams

Sometimes a scam artist will just show up at your door. It's commonly referred to as a door-to-door sale and it's a favorite among bogus home improvement operators. Seniors, those who live alone, and victims of weather-related disasters are common targets.

- When to be Skeptical:
  - The person at your door notices that your roof (or another area on your house that is hard to check) needs repair. He may trick you into signing a contract without disclosing all the charges.
  - He says he just finished work on your neighbor's house and has just enough materials to do repair work on yours. He might say he can give you a better bargain if you let him do the work today since he has the supplies now.
  - The contractor is pressuring you to accept an offer.