



Northwestern District Attorney's Office Consumer Protection Unit *Scam Alert Newsletter*



GOVERNMENT IMPOSTER

What to look for: A phone call claiming to be from the Social Security Administration, IRS, Medicare, FBI, sheriff or police department. They want you to verify personal information because your Social Security number has been compromised; or you failed to report for jury duty & you need to pay a fine; or you didn't pay your taxes & they need your money now. If you don't, you will be arrested or your benefits will be taken away.

What to do:

- **HANG UP**
- **Look up** the number for the government agency
- **Call** the agency directly to report the call & verify the information

Government agencies will not call you looking for money or personal information.

GRANDPARENT/FAMILY EMERGENCY SCAM

What to look for: A phone call claiming to be about or from a grandchild or other family member in distress. The caller says the situation is urgent & you need to wire money or buy gift cards to pay for bail or to help resolve the situation. They ask you not to tell their parents.

What to do:

- **Verify** that it is your grandchild by asking a question only your real grandchildren would know the answer to
- If you cannot easily verify it is your grandchild, **HANG UP**
- **Contact** their parents
- **Resist** pressure to send money quickly and secretly
- **Refuse** to send money through wire transfer, overnight delivery service, or buying gift cards

CHARITIES SCAM

What to look for: You get a phone call or letter from a charity asking for a donation. The caller pressures you to donate now & asks for your credit card number.

What to do:

- **Don't** feel pressured to make a donation
- **Research** the charity – make sure it is real & something you want to donate to

ROMANCE SCAM

What to look for: An on-line love interest asks you for money. You have never met, but they have an emergency & need some financial assistance or they have an investment deal too good to pass up.

What to do:

- **Don't** send money to someone you have never met
- **Talk** it over with a friend or family member
- **Stop** communicating with them



Northwestern District Attorney's Office Consumer Protection Unit *Scam Alert Newsletter*



BANK & CREDIT CARD IMPOSTERS

What to look for: You get a call or email from your bank or credit card company stating that there is a problem with your account or a charge has been declined. You need to call now or click on a link to resolve the problem.

What to do:

- **HANG UP**
- **Call** your bank or credit card company directly to report the call & verify the information
- **Visit** your local bank to resolve the problem

UTILITY COMPANY IMPOSTERS

What to look for: A phone call or email claiming to be from your utility or cable company. They say you are behind on your payments & you need to send money now or your service will be shut off.

What to do:

- **HANG UP**
- **Find** your bill or statement
- **Call** the company's customer service number to verify that your account is in good standing

TECH SUPPORT SCAM

What to look for: You receive a call, email, or a message pops up on your computer claiming your computer has been infected with a virus or is not working properly. The caller claims that he can remove the virus or fix your computer for a fee & you need to allow him to remotely access your computer. In some cases, they steal personal or financial information on your computer to steal your money or your identity. Other times, the scam artist may attempt to install malware on your computer, allowing them to control the computer remotely, or display fake security alerts to convince you to pay for a useless service.

What to do:

- **HANG UP**
- **Shut down** your computer immediately
- **Run** your anti-virus program
- **Don't** let anyone have remote access to your computer
- **Take** your computer to a repair shop you trust if you believe there is a problem

Microsoft and Apple do not monitor your computer looking for problems. They will not call you or send you an email about a virus on your computer.



Northwestern District Attorney's Office Consumer Protection Unit Scam Alert Newsletter



MEDICARE/MEDICAL EQUIPMENT SCAM

What to look for: You get a call offering to send you a free medical alert system, a free back brace, or other medical equipment. The caller tells you they will bill Medicare and send you the equipment for free! They just need your Medicare or Social Security number in order to process your order.

What to do:

- **HANG UP**
- **Don't** give out personal information such as your Medicare or Social Security number over the phone
- **Beware** of "free" offers

Talk to your doctor if you think you need a brace or any medical device

LOTTERY & SWEEPSTAKES SCAM

What to look for: An unexpected email, letter or phone call from someone who claims you have won money in a lottery or sweepstakes. They ask you to send money to pay taxes, insurance or other fees to claim the winnings. They may ask for your bank account information, so your winnings can be directly transferred into your account.

What to do:

- **Slow down and remember:** you can't win if you didn't enter
- **Don't** give bank account information to anyone over the phone
- **Don't** send money
- **HANG UP**

Foreign lotteries are illegal. You should never have to send money or grant access to your bank account in order to claim a prize.

Different Story, Same Old Scam

Scams can involve dramatic or convincing stories to convince you to pay through money wiring service, gift cards or even by sending cash.

- Friend-in-Need Scams
- Advance Fee Loan Scams
- Apartment Rental Scams
- Online Purchase Scams
- Mystery Shopper Scams
- Overpayment Scams

What to do:

- **Verify** the information before you pay
 - **Don't** accept checks from someone you don't know
 - **Remember:** gift cards are for gifts not for payments
 - **HANG UP**
-



Northwestern District Attorney's Office Consumer Protection Unit *Scam Alert Newsletter*



Don't rely on caller ID: Criminals often use "spoofing" technology that tricks your caller ID into displaying a fake number. It may look as though the call is coming from someone in your neighborhood or from a government agency.

Screen your calls: If possible, send all calls you don't recognize to voice mail or let the answering machine pick up. If you accidentally pick up a call from someone you don't know, just hang up quietly.

Report suspicious activity: Check out an unknown company before you sign up, especially if business is done over the phone. If a caller seems suspicious, hang up & report it.

Stay safe on the computer:

- Don't trust unsolicited emails
- Treat email attachments with caution & never click on links in emails unless you've verified the sender
- Install antivirus software & make sure to keep it up to date
- Filter spam messages
- Check for spelling mistakes in email addresses
- Don't call the number they give you, look it up yourself
- Never share passwords or give control of your computer to anyone who contacts you

Keep your personal information private: Don't share your Social Security number, Medicare number, date of birth, credit card or bank account numbers with someone who contacts you no matter who they claim to be.

Remember that criminals try to play on your emotions: If someone tells you to keep it a secret, rushes you or scares you, it is probably a scam. Remember, they are trying to **trick** you into sending them money!

Payment Demands: Criminals want easy, fast payments like money wiring, gift cards or even cash