

DON'T FALL FOR FRAUD

**Protect yourself
- and your hard-earned cash -
from scammers.**



CL Cayuga Lake
NB National Bank





THE GRANDKID SCAM

You get a call: “Grandma, I need money for bail,” - or money for a medical bill or some other kind of trouble.

The caller says it’s urgent - and tells you to keep it a secret.

But is the caller who you think it is?

Scammers are good at pretending to be someone they’re not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one’s email account, to make it seem more real.

And they'll pressure you to send money before you have time to think.

Here’s what you can do to help protect yourself:

1. STOP! Check it out. Look up your grandkid’s phone number yourself or call another family member.

2. Pass this information on to a friend. You may not have gotten one of these calls, but chances are you know someone who will get one - if they haven't already.

IDENTITY THEFT



Someone gets your personal information and runs up charges in your name.

They might use your:

- Social Security or Medicare number,
- Your credit card, or
- Your medical insurance...
- Along with your good name.

Here are signs someone is using your identity:

- You get bills for things you didn't buy or services you didn't use.
- Your bank account has withdrawals you didn't make. You don't get bills you expect.
- You check your credit report and find accounts you never knew about.

Here's what you can do to help protect yourself:

- **Protect your information:**
 - Shred documents before you throw them out
 - Give your Social Security number only when you must
 - Use strong passwords online.
- **Check your monthly statements and your credit:** Read your account statements and explanations of benefits. Be sure you recognize what they show.
- **Once a year, get a FREE copy of your credit report:** You can do so by going online to AnnualCreditReport.com or by calling 1-877-322-8228. The law entitles you to one free report each year from each credit bureau. If you see something you don't recognize, deal with it right away.

ROMANCE SCAMS



Someone contacts you on social media - and says they're interested in getting to know you. Or maybe you meet someone special on a dating website or mobile app.

Soon the person wants to write to you directly or start talking on the phone.

They say it's true love, but they live far away - maybe because of work, or because they're in the military.

Then... they start asking for money. Maybe it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers of all ages, genders, and sexual orientations make fake profiles, sometimes using photos of other people - even stolen pictures of real military personnel.

They build relationships - some even pretend to plan weddings - before they disappear with your money.

Here's what you can do to help protect yourself:

- **STOP! DON'T SEND MONEY. NEVER** send cash, or send money using gift cards, wire transfers, cryptocurrency, or a payment app to an online love interest. Once you pay this way, it's hard to get your money back.
- Pass this information on to a friend. You may not have gotten tangled up with a romance scam, but chances are, you know someone who will - if they haven't already.



IRS IMPOSTER SCAMS



You get a call from someone who says he's from the IRS. He says you owe back taxes and threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. He tells you to put money on a prepaid debit card and give him the card numbers.

The caller may know some of your Social Security number. And your caller ID might show a Washington, DC area code or even show the name IRS! But is it really the IRS calling? No! It's a scam! (Caller IDs can be faked!)

The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone.

And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone.

Here's what you can do to help protect yourself:

1. STOP! HANG UP THE PHONE!

You're not being rude by hanging up - these people are expert scammers and will try everything to get money from you. They may be kind and act like they're your friend - or they may act in a threatening manner. **JUST HANG UP!**

Don't wire money or pay with a prepaid debit card. Once you send it, the money is gone.

(If you have tax questions, go to [irs.gov](https://www.irs.gov) or call the IRS at 800-829-1040.)



“YOU’VE WON” SCAMS



You get a call, letter, email, or text saying that you won! Maybe it's a vacation or cruise, a lottery or a sweepstakes.

The person contacting you about your prize is so excited. They can't wait for you to get your winnings.

But here's what happens next...

They say there are fees, taxes, or customs duties to pay.

Then they ask for your credit card number or bank account information. Or they insist you can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.

If you pay a scammer or share information, you lose. There is no prize. Instead, you get more requests for money, and more false promises that you won big.

Here's what you can do to help protect yourself:

- **Keep your money - and your information - to yourself. NEVER** share your financial information with someone who contacts you and claims to need it. And never pay anyone who insists you send cash or can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.