

SENIOR CITIZEN FRAUD



How to protect yourself

Why are the elderly such an attractive target for con artists?

Many seniors have a "nest egg," and are less likely to report fraud because they don't know where to go or are too embarrassed to talk about it.

If they do report the crime, it can be hard to remember exact details.

Many of the products/services being hawked by con artists appeal to individuals of a certain age—i.e., anti-aging and other health care products, health care services, and investments related to retirement savings.

The threat to seniors is growing...and changing. Baby boomers (born between 1946 and 1964) are now the largest segment of our population—about 78 million people. That means that the number of senior citizens is rising. Many younger boomers also have considerable computer skills, so criminals are modifying their targeting techniques—using not only traditional telephone calls and mass mailings but also online scams like phishing and e-mail spamming.

The scams

Some common ones to look out for:

- Identity theft (accomplished through "dumpster diving," phishing, address changes, old-fashioned theft)
- Health insurance frauds (medical equipment, "rolling lab" schemes, Medicare fraud, counterfeit prescription drugs)
- Home repair schemes
- Foreign lottery/sweepstakes fraud
- Advance fee/credit card fraud
- Investment fraud
- Charity schemes

Recovery schemes are also worth mentioning because they're especially cold-hearted: they target previous victims by convincing them that their money has been recovered by law enforcement or government officials but that they must pay a fee to get it back.

A few basic tips to avoid being victimized:

- Shred credit card receipts and old bank statements
- Close unused credit card or bank accounts
- Don't give out personal information via the phone, mail, or Internet unless you initiated the contact
- Never respond to an offer you don't understand
- Talk over investments with a trusted friend, family member, or financial advisor
- Require all plans and purchases to be in writing
- Don't pay in advance for services.

Who to call

If you're a senior citizen who has been victimized by fraud, start by calling your local or state law enforcement agency.

ALERT! SCHOLARSHIP & FINANCIAL AID SCAMS



Various schemes target teens, such as scholarship and financial aid and other scams which guarantee funds or winnings.

Teens are being targeted as they prepare for and apply for college scholarships.

Teens are completing applications for scholarships and grants online from various sources, not all are legitimate. These applications include personal-non-public information on the teen and therefore expose them to identity theft.

Online predators prey on individuals' trust and financial needs.

Be careful of offers that claim:

- you can not get this information anywhere else
- the scholarship is guaranteed or your money back
- you must provide a credit card or bank account to hold the scholarship
- you are a finalist in a contest you never entered
- you are the recipient of a scholarship or grant you never applied for

Tips for Safe Banking Over the Internet

As use of the Internet continues to expand, more banks are using the Web to offer products and services or otherwise enhance communications with consumers.

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct banking business, any day, any time. However, safe banking online involves making good choices - decisions that will help you avoid costly surprises or even scams.

Confirm that an Online Bank Is Legitimate and that Your Deposits Are Insured

Read Key Information About the Bank Posted on its Web site

Most bank Web sites have an "About Us" section or something similar that describes the institution. You may find a brief history of the bank, the official name and address of the bank's headquarters, and information about its insurance coverage from the FDIC.

Protect Yourself From Fraudulent Web Sites

Watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as, that of a real financial institution. The intent is to lure you into clicking onto their Web site and giving your personal information, such as your account number and password. Always check to see that you have typed the correct Web site address for your bank before conducting a transaction.

Verify the Bank's Insurance Status

To verify a bank's insurance status, look for the familiar FDIC logo or the words "Member FDIC" or "FDIC Insured" on the Web site.

Also, you should check the FDIC's online database of FDIC-insured institutions. If your bank does not appear on this list, contact the FDIC.

Also remember that not all banks operating on the Internet are insured by the FDIC. Many banks that are not FDIC-insured are chartered overseas. If you

choose to use a bank chartered overseas, it is important for you to know that the FDIC may not insure your deposits.

Protect Your Privacy

Some consumers may want to know how their personal information is used by their bank and whether it is shared with affiliates of the bank or other parties.

Help Keep Your Transaction Secure

The Internet is a public network. Therefore, it is important to learn how to safeguard your banking information, credit card numbers, Social Security Number and other personal data.

Look at Your Bank's Web Site for Information About its Security Practices, or Contact the Bank Directly.

Also learn about and take advantage of security features. Some examples are:

- **Encryption** is the process of scrambling private information to prevent unauthorized access. To show that your transmission is encrypted, some browsers display a small icon on your screen that looks like a "lock" or a "key" whenever you conduct secure transactions online. Avoid sending sensitive information, such as account numbers, through unsecured e-mail.

- **Passwords or personal identification numbers (PINs)** should be used when accessing an account online. Your password should be unique to you and you should change it regularly. Do not use birthdates or other numbers or words that may be easy for others to guess. If you use a financial company that requires your passwords in order to gather your financial data from various sources, make sure you learn about the company's privacy and security practices.

- **General security** over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers or Internet service provider to ensure you have the latest in security updates.

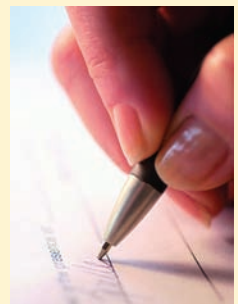


COUNTERFEIT CASHIER'S CHECKS Still a Nemesis

The use of counterfeit cashier's checks has become so common and such a nemesis that we want to ensure that our customers know the following:

- 1 As part of fraud schemes, many people receive cashier's checks that appear legitimate but are really counterfeit.
- 2 You, as the customer, are responsible for any checks you deposit or cash that turn out to be counterfeit.
- 3 You are responsible and liable for a counterfeit cashier's check and its ultimate payment even though your financial institution has already made the funds available to you.
- 4 This holds true whether you cash the check or deposit the check.
- 5 The bank whose name appears on a counterfeit check is not responsible for it.
- 6 Do not respond to unsolicited offers received over the Internet from people you do not know. Ask yourself why you are so lucky to have been selected.
- 7 Be particularly wary of emails apparently originating from overseas.

These are a few of the things our customers need to be knowledgeable about when an offer seems too good to be true.



brought to you by


ChelseaGroton
Feel good about your bank.™

448-4100 • 823-4800 • 599-2406

Member
FDIC

chelseagroton.com



Questions about Chelsea Groton Online Banking?
Call our 24 hours support line @ 800-760-3046.