



NORTH CAROLINA DEPARTMENT OF THE SECRETARY OF STATE

Securities Division

ARE YOU AN INFORMED INVESTOR?

SOCIAL NETWORKING

Social networking in the Internet age allows people to connect to one another more quickly and easily than ever before. Investment promoters increasingly are logging on to find investors ... and their money.

What are social networks?

A social network is a group of individuals (or organizations) who are connected through common interests, hobbies, lifestyles, relationships, faith or other beliefs. Websites such as Facebook, Twitter, LinkedIn, eHarmony and other online social networks and communities have made it faster and easier for users to meet, interact and establish connections with other users anywhere in the world.

Offline, social networking involves making these connections through membership in community service organizations, professional associations, faith-based organizations, multi-level marketing opportunities and singles groups, among others.

While social networking helps connect people with others who share similar interests or views, con artists infiltrate these social networks looking for victims. By joining and actively participating in a social network or community, the con artist builds credibility and gains the trust of other members of the group.

How do con artists exploit social networks?

In traditional social networks, con artists use the weekly or monthly meetings to establish strong bonds through face-to-face contact and sharing of personal interests and lifestyles.

In online social networks, a con artist can establish this trust and credibility more quickly. The scammer has immediate access to potential victims through their online profiles, which may contain sensitive personal information such as their dates or places of birth, phone numbers, home addresses, religious and political views, employment histories, and even personal photographs.

The con artist takes advantage of how easily people share background and personal information online and uses it to make a skillful and highly targeted pitch. The scam can spread rapidly through a social network as the con artist gains access to the friends and colleagues of the initial target.

What are the red flags of an online investment scam?

Online investment fraud has many of the same characteristics as offline investment fraud. Learn to recognize these red flags:

Before investing through a social network, ask yourself these questions:

- Have I verified that the promoter is legitimate?
- Do I understand the risks of the investment?

Evaluate every investment opportunity in the virtual world the same way you would in the real world.

Visit the Security Division's website www.sosnc.com for more tips on recognizing, avoiding and reporting investment fraud.

For more investor education resources, visit the website of the North American Securities Administrators Association at www.nasaa.org.

- Promises of high returns with no risk.** Many online scams promise unreasonably high short-term profits. Guarantees of returns around 2 percent a day, 14 percent a week or 40 percent a month are too good to be true. Remember that risk and reward go hand-in-hand.
- Offshore operations.** Many scams are headquartered offshore making it more difficult for regulators to shut down the scam and recover investors' funds.
- E-Currency sites.** If you have to open an e-currency account to transfer money, use caution. These sites may not be regulated, and the con artists use them to cover up the money trail.
- Recruit your friends.** Most cons will offer bonuses if you recruit your friends into the scheme.
- Professional websites with little to no information.** These days anyone can put up a website. Scam sites may look professional, but they offer little to no information about the company's management, location or details about the investment.
- No written information.** Online scam promoters often fail to provide a prospectus or other form of written information detailing the risks of the investment and procedures to get your money out.

How can I protect myself from fraud in social networking?

Contact the N.C. Securities Division.

Before investing any money, contact your state securities regulator to learn more about the background of the salesperson and registration

status of the investment. In N.C., call (800) 688-4507 or (919) 733-3925.

Protect your personal information. Many sites will allow you to choose how much personal information you want to make publicly accessible, and how much you want to keep private. Adjust your privacy and security settings accordingly, and think twice before posting personal information online.

Search the names of all persons and companies connected to the investment being offered. The Internet offers anonymity and scam artists take advantage of this. Do a search for the name of the person offering you the investment and the companies involved in the investment. If there are few results, or their name doesn't appear anywhere outside of the one investment program they're offering you, that's a red flag that they may be using multiple aliases, or hiding behind a fake identity.

Beware of the use of names or testimonials from other group members. Scam artists frequently pay out high returns to early investors using money from later arrivals. This type of scam is a Ponzi scheme. Fraud aimed at groups of people who share similar interests is called affinity fraud.

Obtain a prospectus. Ask for written documentation that details the risks of the investment and procedures to get your money out.

Do not take the word of a salesperson.

Don't feel pressured to "act now". Take time to check out the investment yourself, and remember the old adage: "If it sounds too good to be true, it probably is."

To learn more or for help with these or other products, contact:

NC Department of the Secretary of State, Securities Division PO Box 29622, Raleigh, NC 27626-0622
Phone: (800) 688-4507 or (919) 733-3924 | Fax: (919) 807-2183 | E-mail: secdiv@sosnc.com
Visit us at: www.sosnc.com or www.sos.nc.us