

## BBB tips to guard against online scams

Written by

Wednesday, 21 August 2013 03:09

---



While there is no foolproof way to protect against all emerging technology-based scams, the Better Business Bureau of Minnesota and North Dakota (BBB) says consumers can better defend themselves by understanding the two major objectives of online criminals: cheating people out of money and tricking them into divulging personal information with which to commit identity theft.

"With online fraud, just as with many common maladies, an ounce of prevention is worth a pound of cure," said Dana Badgerow, president and CEO of the BBB of Minnesota and North Dakota. "In this case, awareness of and skepticism about suspicious online offers can often help people avoid getting scammed out of thousands of dollars."

The most common Internet scams to cheat consumers involve obtaining credit card information or getting people to send money by wire transfer. This type of fraud usually occurs via phony or lookalike websites, predatory offers such as credit-repair services, friendship swindles, fake check scams, and emails requesting upfront payments to collect alleged lottery winnings.

The second category of cybercrime involves coaxing consumers to reveal personal information, such as their Social Security number, date of birth, address and telephone numbers. This is usually done by sending out authentic-looking communications supposedly from government

## BBB tips to guard against online scams

Written by

Wednesday, 21 August 2013 03:09

---

agencies, retailers, financial institutions and other businesses. These emails typically contain hyperlinks that lead to online forms requesting personal information or download malicious software that can steal login information or passwords.

The BBB offers the following advice to stay ahead of cybercriminals:

**Make sure things check out** – Research unfamiliar retailer and charity websites at [bbb.org](http://bbb.org) before entering a credit card number. Confirm your online purchase is secure by looking at your browser for the "s" in https:// and in the lower-right corner for the "lock" symbol before paying.

**Be wary of unsolicited emails** – Government agencies, credit card companies and banks will never ask for personal information such as a Social Security or Medicare number through email (or over the phone). In addition, when you receive a link to a "special deal" or coupon through a social network site, type in the Internet address yourself. A link's true destination may be hidden, taking you to a lookalike website or download malware onto your computer.

**Always use secure payment methods** – Never send money by wire transfer to someone you don't know. Use a credit card, online payment system or escrow service to pay for auction or classified ad items.

**Beware of overpayment scams** – Cybercriminals use scams that involve sending legitimate-looking checks for more than the purchase price and asking that the monetary difference be returned to them by wire transfer. Though the check may initially be accepted for deposit at a bank, it may take several days to bounce, resulting in the loss of any money wired away as well as overdraft penalties.

**Be selfish with personal information** – Social media sites encourage the sharing of information. However, avoid sharing your birth date, address and other information that may be used to help put together a profile that can be used to steal your identity. Check the privacy settings for your profile and considering hiding your profile unless you approve a friendship/contact request.

**Practice safe computing** – Don't use short passwords, or the same password for multiple sites. Passwords should contain a variety of upper and lower case letters and digits or characters. Ensure your computer antivirus software and operating system are current with the latest security updates and run malware scans on a weekly basis.

There is no telling what new online threats might lurk around the corner, however, common sense and an abundance of caution go a long way towards protecting yourself from online crime.

*The mission of the Better Business Bureau is to be the leader in building marketplace trust by promoting, through self-regulation, the highest standards of business ethics and conduct, and to instill confidence in responsible businesses through programs of education and action that inform, assist and protect the general public. We are open 8 a.m. to 5 p.m. Monday through Friday. Contact the BBB at [bbb.org](http://bbb.org) or 651-699-1111, toll-free at 1-800-646-6222.*