

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

Fake Credit Report Sites: Cashing in on Your Personal Information

You may have seen Web sites or received unsolicited email offering credit reports, sometimes for free. Be aware that some of these online operators may not actually provide credit reports, but may be using these sites as a way to capture your personal information. From there, they may sell your information to others who may use it to commit fraud, including identity theft.

This is a variation on “phishing,” also called “carding,” a high-tech scam that uses spam or fraudulent Web sites to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

The Federal Trade Commission (FTC), the nation’s consumer protection agency, urges you to take the following precautions when visiting sites or responding to email that offer credit reports:

- If you get an email offering a credit report, don’t reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you **know** to be genuine.
- Be skeptical of unsolicited email offering credit reports. Keep an eye out for email from an atypical address, like **XYZ123@website.net**, or an email address ending in a top level domain other than .com, like .ru or .de.
- Check whether the company has a working telephone number and legitimate address. You can check addresses at Web sites like **www.switchboard.com**, and phone numbers through reverse lookup search engines like **www.anywho.com**.
- Check for misspellings and grammatical errors. Silly mistakes and sloppy copy — for example, an area code that doesn’t match an address — often are giveaways that the site is a scam. Look at the company’s Web address: is it a real company’s address or it is a misspelled version of a legitimate company’s Web address?
- Check to see whether the email address matches the Web site address. That is, when you enter the company’s Web address into the browser, does it go to the sender’s site or re-direct you to a different Web address? If it re-directs you, that’s a red flag that you should cease the transaction.
- Find out who owns the Web site by using a “Whois” search such as the search at **http://www.networksolutions.com**.

- Exit from any Web site that asks for unnecessary personal information, like a Personal Identification Number (PIN) for your bank account, the three-digit code on the back of your credit card, or your passport number and issuing country. Legitimate sites don't ask for this information.
- All legitimate sites will want to verify who you are, and will respond to an electronic request for a credit report by asking you for an additional piece of information. If a site does not ask a follow-up question, the site is almost certainly a fake.
- Use only secure Web sites. Look for the "lock" icon on the browser's status bar, and the phrase "https" in the URL address for a Web site, to be sure your information is secure during transmission. All real sites are secure.
- Watch your mailbox and credit card statements: If you've responded to a bogus site, you may never receive the credit report they offered for free. If you paid one of these sites for a credit report, your credit card may never be charged. If you find that you have unauthorized charges, contact your financial institutions and credit card issuers immediately.
- Report suspicious activity to the FTC and the U.S. Secret Service. Send the actual spam to the Los Angeles Electronic Crimes Task Force at LA.ECTF.reports@uss.dhs.gov and to the FTC at spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov and then visit the FTC's Identity Theft Web site (www.consumer.gov/idtheft) to learn how to minimize your risk of damage from identity theft.

For More Information and to Complain

For a copy of your credit report from the major credit bureaus, contact:

- Equifax — www.equifax.com; 1-800-685-1111
- Experian — www.experian.com; 1-888-EXPERIAN (397-3742)
- TransUnion — www.transunion.com; 1-800-888-4213

The Federal Trade Commission works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad. Consumers also can call their local office of the Secret Service.

