

---

# FTC Consumer Alert

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

## Is Someone “Phishing” for Your Information?

Internet scammers casting about for people’s financial information have a new way to lure unsuspecting victims: they go “phishing.” Phishing is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information.

According to the Federal Trade Commission (FTC), the latest phishing scam involves emails that claim to be from *regulations.gov*, a Web site where consumers can participate in government rulemaking by submitting comments. The emails’ subject lines typically read “Official information” or “Urgent information to all credit card holders!” The message’s text claims, “Due to recent changes in Rules and Regulations, it is required by Law for all Internet users to identify themselves in compliance with CFR (Code of Federal Regulations) to create a secure and safer Internet community.” The email includes a link to a Web site that mimics *regulations.gov* and asks readers to provide their personal and financial information.

**In fact, there is no law requiring all Internet users to register with the government. And *regulations.gov* does not collect financial information or charge consumers a fee for submitting comments. Consumers who provide their financial information in response to an unsolicited email could be at risk of identity theft.**

If you get an unsolicited email that claims to be from the federal government and asks for your information, do not respond. Send the spam to the FTC at [spam@uce.gov](mailto:spam@uce.gov) so that it can be available to law enforcement.

Avoid emailing personal and financial information. If you get an unexpected email from a company or government agency asking for your personal information, contact the company or agency cited in the email using a telephone number you know to be genuine, or start a new Internet session and type in the Web address that you know is correct.

If you have recently shared your credit card or bank account information in response to an unsolicited email that claimed to be from *regulations.gov*, you should notify your credit card company or bank immediately and discuss whether you should cancel your accounts. In any event, you should carefully monitor your accounts. If you provided your Social Security number, you should contact one of the three national consumer reporting agencies, ask that a fraud alert be placed on your accounts and obtain copies of your credit reports. You also should visit the FTC’s Identity Theft Web site ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) to file a complaint and learn more about how to minimize your risk of damage from identity theft.

*Regulations.gov* is operated by the United States Environmental Protection Agency in association with the Food and Drug Administration, the National Archives and Records Administration/Office of

---

the Federal Register, and the Government Printing Office. The FTC and other federal agencies use the *regulations.gov* portal to receive comments from the public regarding proposed rules and regulations.

The FTC 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](http://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.



*March 2004*

---