

PROTECTING YOURSELF AGAINST PHISHING SCHEMES

To combat the proliferation of fraudulent credit card schemes, Citi is committed to pursuing all reports of suspicious activity and providing our customers with the information they need in order to best protect themselves. In response to recent fraudulent solicitations, we wanted to underscore that although many of the requests sound reasonable at face value, ***Citi will never ask for your password or for you to update personal and/or business information via unsolicited email or telephone call.***

The following tips will help protect both cardholders and the organization from fraud:

- ***Make sure your computer has the most current anti-virus software and a personal firewall.*** Anti-virus software needs to be updated frequently to guard against new viruses. Make sure you download updates as soon as you are notified that they are available. A personal firewall can help prevent unauthorized access to your home computer.
- ***DO NOT click on links in unsolicited emails, especially those asking for personal information.*** Even if you do not supply information, just clicking on a link can enable fraudsters to access your computer, record your keystrokes, and capture passwords you use to log on a various websites. Citi will never under any circumstances email you to ask for your password or to update your personal information.
- ***Go directly to the website you are trying to find.*** The best way to get to any site is to type its address (URL) into your browser and then bookmark it.
- ***Set up a login "cookie".*** Many websites including Citibank.com offer to "remember" your User ID. This way, when you return to the site to sign on, your User ID will be visible in the Sign on box. A spoof website will not be able to display your User ID. Note: Never set up a login cookie on a public or shared computer.
- ***Create "hard-to-guess" passwords.*** Use at least six characters and a mix of letters and numbers. Do not use all or part of your Online User ID or email address, or the names of your children, spouse or pet. Use a different password for each of your online accounts.
- ***DO NOT give personal or account information as a result of an unsolicited email/internet request.*** Citi will never under any circumstances email you to ask for your password or to update your personal information.
- ***DO NOT give personal or account information to someone calling on the phone.*** Citi will never under any circumstances call you to ask for your password or to update your personal information.
- ***Never call the 800 numbers listed in suspicious emails.*** Cardholders should always call the number listed on the back of their cards, billing statement or listed on Citi's web site.
- ***Keep track of your account.*** Sign up for banking alerts to monitor your accounts daily. **If you don't recognize a transaction or suspect fraud, call 1-800-374-9700 immediately.**

Forward suspicious emails to:

- Citi
submitphishing@citi.com
- AND
- Federal Trade Commission
spam@uce.gov

Please DO NOT change or retype the subject line since this inhibits the ability to properly investigate.

Keep a list of ALL your debit and credit cards, and account numbers. This information is critical to have when reporting a problem.

How to Identify a Phishing Email or Website

Every Internet user should know about spoof (a.k.a. phishing or hoax) e-mails that appear to be from a well-known company but can put you at risk.

A spoof website is one that mimics a popular company's website to lure you into disclosing confidential information. To make spoof sites seem legitimate, thieves use the names, logos, graphics and even code of the real company's site.

They can even fake the URL that appears in the address field at the top of your browser window and the padlock that appears in the lower right corner. 🗝️ The links in the spoof e-mails almost always direct you to a spoof web site.

Although they can be difficult to spot, they generally ask you to click a link back to a spoof web site and provide, update or confirm sensitive personal information. To bait you, they may allude to an urgent or threatening condition concerning your account.

What spoof emails are after:

- Password or PIN
- Credit card validation (CCV) code
- ATM/Debit or Credit Card number
- Social Security number (SSN)
- Bank account number

Even if you don't provide what they ask for, simply clicking the link could subject you to background installations of key logging software or viruses. Key logging is the recording of your keystrokes, which could reveal password or personal information.

