



Greeting Card Association

Contact: Barbara Miller
Tel: (202) 207-1113
media@greetingcard.org

How to Recognize and Avoid E-card Scams

The popularity of e-cards with Americans has unfortunately made electronic greeting cards a target of spammers and "phishing" scams designed to introduce a virus or malicious software into your computer.

Millions of these fraudulent e-mails -- posing as notification that someone has sent you an e-card -- have been sent to consumers and businesses around the country in recent years. They are often sent during holidays when e-card exchanges are most popular.

The Greeting Card Association urges consumers to beware of e-mails claiming you've received an electronic greeting card from an unnamed individual, someone you don't know, or a generic friend...classmate...family member...etc.

These false e-mails are designed to fool you into thinking they involve legitimate greeting card publishers or e-card websites.

How The Scams Work

The scam e-mails, which often look very legitimate, instruct you to click on a link in the e-mail message to collect or view your e-card. Clicking on the link can introduce a virus or malicious software into your computer.

Consumers should know that a legitimate e-card notification will always include the full name or personal e-mail address of the sender. The sender will never be identified by a generic term such as a "friend" or "family member."

Unless you recognize the full name or personal e-mail address of the sender, the e-mail is fraudulent and should be immediately deleted. Do not click on the link.

How to Protect Yourself

All legitimate e-card publishers provide a way to collect an e-card directly from their websites and avoid the use of potentially fraudulent links that can introduce a virus into your computer. If you have the slightest doubt that the e-card is legitimate, do not click on the link. Instead, follow these directions for safely retrieving an e-card:

- Manually type the name of the card publisher's website URL into your browser window (for example, www.greetingcard.org). Do not "cut and paste" the link into your browser
- Locate the "e-card pick up" area on the publisher's website.
- Take the card number or retrieval code information from the e-mail and enter it into the appropriate box or boxes on the publisher's e-card pick-up area.
- If there is no card awaiting you, the e-mail you received was a scam. Delete it.

(more)

Both the FBI and the Federal Trade Commission are aware of the “phishing scams” associated with e-cards. In addition, the greeting card industry is working with the FBI’s Internet Crime Complaint Center, Internet security organizations and Internet Service Providers to stem the malicious efforts of these scammers.

If you receive a fraudulent e-mail regarding e-cards, the Greeting Card Association recommends that you file a complaint with the FBI’s Internet Crime Complaint Center at www.ic3.gov.

Basic Rules of Cyber Safety

The e-card “phishing” scam is just one of many fraudulent Internet schemes that prey on unsuspecting consumers.

To protect yourself from unwanted spam and fraudulent Internet schemes, the Greeting Card Association urges consumers to follow these basic precautions:

- **Install and regularly update anti-virus software for your computer.**
- **Be cautious when downloading items or opening e-mail attachments.** Never open an e-mail attachment coming from someone you don’t know, or being forwarded to you from someone you don’t know.
- **Ignore e-mails asking for personal or financial information.** Reputable companies and financial institutions will never ask you for personal or financial information via e-mail. If you think the e-mail is legitimate, phone the company directly using a phone number that you know is accurate, not a number listed in the e-mail.
- **Turn off your computer when not in use.** Leaving your computer on can make it vulnerable to unwanted attacks. Turning it off when not in use saves energy too.
- **Delete spam without opening it, and do not respond to it.** This tells the spammer that he has reached a real e-mail address, and will generate more spam.
- **Only purchase items on the Internet from reputable sources.** Do not purchase from an unsolicited e-mail offer. Do not give your credit card number unless you know the site is secure. Be extremely cautious of purchasing items from websites that do not also provide you with a street address and phone number for contacting the company directly.
- **Avoid clicking on links to websites from unsolicited e-mails.** Go directly to the website by manually typing in the appropriate URL.
- **Learn more about protecting yourself from Internet fraud and “phishing” scams.** These U.S. government websites are very informative: www.ic3.gov and www.OnGuardOnline.gov

###