



Subscribe to
Aperture Aside
Photographer's Journal

Be Aware of Artist Scamming



Compiled by DiscoveredArtists.com
And reprinted with permission

1. Be skeptical...

Artists are increasingly being targeted in Internet scams. After all, what artist hasn't dreamed of being "discovered" and selling several works of art to an admiring collector or a wealthy buyer? A few tell-tale signs to look for in any email you receive from a prospective buyer: misspelled words, poor grammar, and an urgent overseas buyer (particularly one from Nigeria). They also typically want to make the shipping arrangements themselves or have someone pick the work up for them, rather than have you ship it to them ~ probably because they don't want the authorities to track them to a particular address. Or worse, they are looking for an excuse to enter your home. [Email scams aimed at artists »](#)

2. Never ship your artwork to someone without making sure the payment has cleared.

Be aware that even though your bank may give you cash for cashier's checks and postal money orders, they can still be counterfeit. Cashier's checks and postal money orders can take up to a month to fully clear. If the payment turns out to be fraudulent, you could be held responsible for the entire amount withdrawn from your bank.

3. Beware if you have been overpaid for an item you are selling by cashier's check or postal money order and have been instructed to return the overpayment amount to the buyer or other party.

Never agree to return an overpayment. See explanation #2 above.

4. Don't deal with persons who insist it is "urgent" or those who claim that they need the item in a hurry (perhaps for a gift).

Con artists will try to pressure you so you don't have time to ensure the funds have cleared. Honest buyers should understand that you need to wait until their check has had time to clear.

5. Perform due diligence if a gallery wants to exhibit your work, or a company wants to license your art.

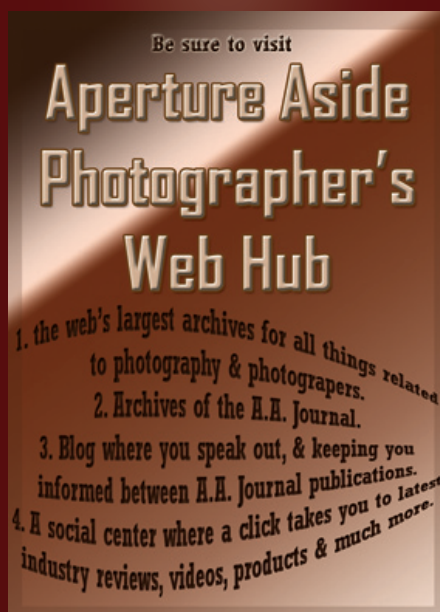
Check with the local better Business Bureau or Chamber of Commerce as well as your Attorney General's office to find out if they are a legitimate business and to learn if there have been any complaints lodged against them. Insist on a contract with all of the terms in writing, signed and dated by both parties. Carefully scrutinize the document and read all terms of the agreement before signing. Don't sign anything you are uncomfortable with or anything you do not fully understand. Remember too that contract terms are often negotiable. [Links to more advice for artists »](#)

6. Beware of vanity galleries and publishers who charge artists to have their work included in a publication.

Vanity galleries charge exhibition fees for artists to exhibit their work, rather than commissions on sales. The fees can be very high and the galleries do not have an incentive to effectively promote your work since they make their money from exhibition fees, rather than sales of your art. The same is true for vanity publications - publishers who charge artists to have their work published. [Links to more advice for artists »](#)

7. Beware of phony emails disguised as legitimate businesses.

Criminals attempt to get you to provide personal and confidential information, such as online IDs and passwords, or Social Security numbers and account numbers by posing as your bank, an online payment service such as PayPal ([read PayPal's Phishing Guide here](#)), a Credit Card company, or just about any company with which you might do business. These emails, referred to as "phishing", often use text, images, or logos from the legitimate site to fool you. Typically, they make claims that your account has been compromised, needs to be updated, or is soon to become inactivate. **Do not reply or click on any links provided in such emails.** If you believe you may actually need to update your credit card information, etc., open a web browser and type in the company's website address yourself. Log in to your account and proceed from there. The FTC recommends that you forward spam that is phishing for information to <mailto:spam@uce.gov> and to the company, bank, or organization impersonated in the phishing email. NOTE: Many companies now post consumer fraud alerts on their websites and often provide an email address for reporting fraudulent or suspicious emails that use their company name. Also, the latest version of Microsoft's Internet Explorer (version 7) includes a new Phishing Filter that alerts you when a website appears to be fraudulent. [Examples of fraudulent PayPal emails »](#)



Subscribe to
Aperture Aside
Photographer's Journal

8. Beware of emails from a Nigerian or other foreign government official requesting assistance in the transfer of excess funds from a foreign country into your bank account.

Again, these scam artists attempt to steal your money. The persons perpetrating these scams are considered extremely dangerous.

9. Safeguard your online transactions to help prevent identity theft or unauthorized credit card charges.

Purchase only from a trusted retailer or use an online payment service, such as PayPal, which allows you to shop without sharing financial information. Website pages which request financial information, such as credit card numbers, should always have a website address that begins with "https". The "s" lets you know that your personal information is encrypted when it is sent, preventing unauthorized people from seeing the information that is sent across the Internet. Also, a padlock symbol is displayed by some web browsers (usually in the status bar in the bottom right hand corner) to indicate you are viewing a secure web page. Never send personal or financial information, including credit card numbers, in an email. Emails are not transmitted securely across the Internet. 5

Actions to help protect yourself from identity theft »

10. Protect your computer from viruses, spyware, adware, worms, trojans, or other malware.

Use anti-virus and anti-spyware software programs (offered by companies such as *McAfee* or *Symantec*), and keep them up to date. Also, use a firewall to shield access to your computer. Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them (It is easy for someone to fake their true identity). Never open email attachments with a .exe, .pif, or .vbs filename extension or a double extension, like "heythere.doc.pif". Finally, use pop-up blockers to avoid pop-up advertisements which can harbor dangerous spyware or adware.

11. Don't open spam. Delete it unread.

Spam can be used to access computers without authorization and transmit viruses. Never respond to spam as this will confirm to the sender that it is a "live" email address. Have a primary and secondary email address - one for people you know and one for all other purposes. Avoid giving out your email address unless you know how it will be used. Never purchase anything advertised through an unsolicited email.

12. Don't forward hoax emails.

Check to see if an email you receive is really just a hoax: *About.com's Hoax Encyclopedia»*

13. If you suspect fraud or are a victim of fraud, take action.

Contact your State Attorney General's Office of Consumer Affairs if you are uncertain or suspicious of a telephone, mail or email solicitation. If you feel you have been the victim of fraud, you can access *the Internet Fraud Complaint Center* (IFCC) at or contact the *Federal Trade Commission*. Forward spam that is phishing for information to *mailto:spam@uce.gov* and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See *www.annualcreditreport.com* for details on ordering a free annual credit report. You can learn other ways to avoid email scams and deal with deceptive spam at *www.ftc.gov/spam*.

14. Stay informed by keeping abreast of consumer fraud trends.

Several artists have already fallen victim to the scams described above, and it is our sincere hope that the advice provided here will prevent this from happening to other artists. There are also other website resources that provide excellent sources of information.

Compiled by:

www.discoveredartists.com

