



October 5, 2009

Dear Media Partner,

We have read with increasing alarm the press surrounding rogue software and malicious advertising that is being placed on websites by individuals pretending to represent legitimate insertion requests.

Recent coverage can be found at:

http://www.nytimes.com/2009/09/15/technology/internet/15adco.html?_r=1&scp=2&sq=vonage&st=cse

These events are the result of individuals impersonating legitimate companies and pretending to place orders that are not authorized by advertisers or their designated agency buyers. As a result, we are reminding you to take extra care if any aspect of a media order seems unusual or out of place.

As stewards of our clients' ad spend, we ask you to work with us to be hyper-vigilant in protecting the requests and insertion orders we make on their behalf. Please notify all personnel in your order-taking operation to accept only the requests or insertion orders that meet the following criteria:

1. The request for insertion is addressed to a specific agency sales representative e.g. Starcom
2. If any information is received from a general sales inquiry on your website or through inside sales, you must contact the agency buyer to confirm the order
3. If you receive a request from an individual that is not familiar to you, contact the agency immediately
4. If the domain name appears to be odd, unfamiliar or in any way manipulated, please question the order and contact the agency rep for confirmation.
5. If you question any request or order for any reason, contact the agency by phone.

We recognize that this will require some additional time and focus, but we will do everything necessary to secure the requests we make on behalf of our clients. We are currently evaluating our internal processes and will take every necessary measure possible to ensure the security of our insertion requests. We appreciate your partnership as we confront this industry issue.

Thank you.