

Security Notice from GovDelivery, Inc.

Due to the increasing amount of fraudulent emails circulating the Internet, we would like you to review the following guidelines to ensure the security and integrity of your data within the GovDelivery system.

One of the more common scams today is the practice of “phishing”. In a phishing attack, email or instant messaging is used to guide people to a Web site that may look quite legitimate, but is masquerading as a login page of a website you would normally use. You are asked to “login” or disclose confidential and/or sensitive information, which is captured, and can then be used to interact with the actual system with the stolen credentials.

Most Importantly, GovDelivery will never initiate contact with you (phone, email, instant messaging, etc) asking for your username and/or password. If you receive any suspicious request asking for this type of information, please contact your account manager immediately and forward the request to security@govdelivery.com.

Steps you can take to protect yourself from phishing scams:

- Do not open email attachments from senders you do not recognize
- Do not respond to emails requesting passwords, usernames, or other sensitive and/or confidential information
- Be wary of emails containing GovDelivery images and logo’s embedded in the email
- Be extremely cautious with emails that indicate an urgent response is required
- These “scare” tactics usually involve account deletion or past-due bill scenario’s
- Verify the authenticity of any website that asks for your sensitive information (username, password, credit cards, etc). See the section below for details on verifying the authenticity of the GovDelivery site.

What is GovDelivery doing to ensure the security of the GovDelivery application?

GovDelivery is dedicated to providing a secure and reliable platform for our clients. GovDelivery uses industry standard network and application security techniques within our infrastructure. In addition to this, we are:

- Developing Internet security educational material available for all clients
- Evaluating and implementing new security features within our platform

What can our clients do to ensure the security of their account within the GovDelivery system?

- Educate yourself on the basics of phishing attempts and how to spot them
- Use industry standard security solutions to detect and alert you to the presence of spam and malware
- Use strong passwords (containing upper and lower case letters, numbers, and special characters)
- GovDelivery provides a built-in password strength meter, on the password reset form, to assist you in your password choices
- Attend GovDelivery educational webinars (Coming Soon)
- Ensure that the access level assigned to specific administrators is not higher than the level required to use GovDelivery effectively
- Remove administrators from the GovDelivery system when they no longer require access or are otherwise inactive

How do I verify a website’s authenticity?

Internet security is a very serious matter, requiring your cooperation. Please do not hesitate to contact us if you have any questions or concerns.

Sincerely,

Sarah Heikkila
Director of Client Services
GovDelivery, Inc.
Sarah.Heikkila@govdelivery.com

Brent Kastner
Manager of Technical Operations
GovDelivery, Inc.
Brent.Kastner@govdelivery.com