Subject line of email: Security Incident Impacting Your GoDaddy Web Hosting Account

Dear <name>:

We need to inform you of a security incident impacting your GoDaddy web hosting account credentials.

We recently identified suspicious activity on a subset of our servers and immediately began an investigation. The investigation found that an unauthorized individual had access to your login information used to connect to SSH on your hosting account. We have no evidence that any files were added or modified on your account. The unauthorized individual has been blocked from our systems, and we continue to investigate potential impact across our environment.

We have proactively reset your hosting account login information to help prevent any potential unauthorized access; you will need to follow these steps in order to regain access. Out of an abundance of caution, we recommend you conduct an audit of your hosting account.

This incident is limited in scope to your hosting account. Your main GoDaddy.com customer account, and the information stored within your customer account, was not accessible by this threat actor.

On behalf of the entire GoDaddy team, we want to say how much we appreciate your business and that we sincerely regret this incident occurred. We are providing you one year of Website Security Deluxe and Express Malware Removal at no cost. These services run scans on your website to identify and alert you of any potential security vulnerabilities. With this service, if a problem arises, there is a special way to contact our security team and they will be there to help.

Again, we apologize for any inconvenience this may have caused. We have already taken and will continue to take measures to enhance our security in light of this incident.

If you have any questions, or you need further assistance, please call [*insert call center number and hours of operation*].

Thank you,

Demetrius Comes