



Iowa Department of Human Services

Kim Reynolds
Governor

Adam Gregg
Lt. Governor

Jerry R. Foxhoven
Director

October 20, 2017

Email Phishing Campaign Leads to Notification of Data Breach ***DHS Takes Steps to Protect Information***

DES MOINES, IOWA - The Department of Human Services (DHS) was the target of a phishing email campaign on August 23, 2017. Hackers were able to mask their identities and send very carefully designed phishing emails to employees to appear like they were sent from another trusted DHS employee. As a result, nine DHS employees provided their passwords which gave the hackers access to their email accounts.

Fortunately, the campaign was discovered the same day the phishing email was sent to DHS, and the employees changed their passwords as soon as possible to block access to their email accounts and to minimize the potential for confidential information to be exposed. All DHS employees were quickly alerted to the phishing email campaign to prevent access to additional email accounts.

The hackers potentially accessed Protected Health Information (PHI) for 820 individuals during the timeframe before passwords were changed. At this time, DHS does not have any evidence to indicate the hackers actually accessed any of the exposed emails.

All individuals potentially affected are being notified by mail. Although the chance that these individual's personal information will be misused is small, DHS will provide up to a year of credit monitoring through TransUnion Interactive at no charge to all those affected.

Since phishing emails are often sent to government agencies, DHS takes a number of steps to continually educate staff on how to recognize and report phishing emails and to protect their usernames and passwords. Information on encrypting all emails that contain confidential information is being sent to all DHS employees. DHS is also implementing technological controls to prevent a hacker from accessing DHS email accounts by obtaining a user's password. Also, all DHS employees are required to sign an annual confidentiality statement and complete annual confidentiality training.

The DHS employees who inadvertently provided their passwords when they received the phishing email were required to re-take the annual confidentiality training sessions which include detailed information about phishing emails and password protection.

If you suspect your identity has been stolen, contact your local enforcement officials or call the Attorney General's Consumer Protection Division at 1-888-777-4590.

For more information, please visit <https://dhs.iowa.gov/news-releases/data-breach-notifications> or contact Matt Highland at mhighla@dhs.state.ia.us or 515-281-4848.

###