



Iowa Department of Human Services

Kim Reynolds
Governor

Adam Gregg
Lt. Governor

Jerry R. Foxhoven
Director

Frequently Asked Questions

Email Phishing Campaign August 23, 2017

Q: What happened?

A: 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.

Q: Why was there a delay between the incident and notifying me that this happened?

A: DHS began an investigation on August 23, 2017 which included:

- Reviewing all unencrypted email that may have been accessed
- Investigating the lists of impacted individuals to identify specific individuals whose confidential information may have been exposed

Q: I received a letter that said my personal information may have been exposed. What does that mean?

A: Your personal information may have potentially been accessed by the hackers during the timeframe before passwords were changed. 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. At this time, DHS does not have any evidence to indicate the hackers actually accessed any of the exposed emails.

Q: How many people are impacted by this incident?

A: 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.

Q: What can I do to protect myself from identity theft?

A: If your personal information was possibly exposed as a result of this incident, you will receive a letter with instructions on how to receive one year of free credit monitoring services from TransUnion Interactive, a global leader in the credit monitoring field. This service includes daily credit monitoring, alerts of key changes to credit files and identity theft insurance. Potentially affected individuals will be able to enroll in this free service through the Iowa Concern Hotline beginning October 23, 2017 through January 31, 2018.

Q: What is DHS doing to address this issue?

A: DHS is taking the following steps in light of this incident:

- Continually educate staff on how to recognize and report phishing emails and to protect their usernames and passwords
- Implement technological controls to prevent a hacker from accessing DHS email accounts by obtaining a user's passwords
- Details on encrypting all emails that contain confidential information is being sent to all DHS employees
- All DHS employees complete an annual confidentiality training, which includes phishing emails and password protection information
- All DHS employees sign a confidentiality statement
- Employees who inadvertently provided their passwords were required to re-take the confidentiality training

DHS is addressing the concerns of potentially affected individuals by:

- Sending a notification letter to each person potentially affected by this incident
- Offering free credit monitoring for one year to all individuals receiving a notification letter
- Utilizing the Iowa Concern Hotline; individuals who received a letter may call 800-447-1985 for more information about the data breach between 8:00 a.m. and 8:00 p.m. Monday through Friday, excluding federal and state holidays

Iowa Concern Hotline: 800-447-1985