



State of Oregon, DHS Call Center FAQ

What happened?

On January 28, 2019, DHS and the Enterprise Security Office confirmed that information may have been compromised through targeted phishing. Nine individual employees opened a spear phishing e-mail and clicked on a link that compromised their email boxes, allowing the malicious sender to potentially access e-mail information.

Because DHS takes privacy and the confidentiality of client information seriously. The department has information technology security processes in place, which enabled the department to detect and contain the incident.

When did this happen?

DHS became aware on January 28, 2019 that information might have been compromised when they began hearing from DHS employees whose mailboxes had been deleted. Passwords were immediately reset to stop access, and security officials began investigating to determine the scope of the incident and the specifics of the information involved.

What personal information was exposed?

The department does not yet know the extent of the breach or if any personal information has been accessed, viewed by an unauthorized person, or used inappropriately. However, it is notifying the public as a precautionary measure.

While access to the e-mail boxes was successfully stopped, it is taking time to thoroughly review the nearly two million emails involved and determine the number of emails that might contain personal information of clients receiving services from DHS. The state's Enterprise Security Office has confirmed impacted information from within the emails.

Was the information protected/encrypted?

Some information might be encrypted and the security review currently underway will provide more information.

How many people are involved?

That information has not been determined.



Who is the State of Oregon, DHS? I don't remember that name or I never went there.

DHS Programs are: Child Welfare, Self-Sufficiency Program, Aging and People with Disabilities, Vocational Rehabilitation, Intellectually/Developmentally Disabled and Oregon Health Plan eligibility.

Have the police have been notified? If so, with which police department?

The Oregon State Police were notified and will continue to receive updates on the analysis of the event.

How can I have my information removed from the server/directory?

I understand your concern. Due to state and federal regulations records must remain on file.

Why didn't you tell affected individuals about the loss of the data sooner?

With any such event, it takes time to investigate if an incident even occurred, gather the relevant information, identify the affected individuals and make the appropriate decisions to line-up the services that are being offered to identified affected individuals.

What is the State of Oregon, DHS doing to prevent this kind of loss from happening again?

The security and confidentiality of personal information is critical to DHS. While there is no indication that any personal information was copied from its email system or used inappropriately, the Dept will be offering identity theft recovery services for potentially impacted individuals. DHS is in the process of determining whose information was affected by this breach. Once confirmed, a vendor, IDExperts, will send individual notices to identified individuals, including notices to clients whose HIPAA protected information was involved, with instructions on how to register for services, which includes free credit monitoring.

IDExperts has also established a toll-free information line at (800) 792-1750, which will be available Friday (March 22, 2019).

If there are any updates regarding this letter, how will I be notified?

We will also update our State of Oregon, DHS website with the most recent information.

Has the information been misused?

At this time, there is no evidence that there has been any use or attempted use of the information exposed in this incident.



I am not listed in your system; however, I would like information regarding this incident.

I appreciate your concern. Unfortunately, I am unable to provide information except to those individuals that have received a notification letter.

What are the risks of identity theft with the information that was exposed?

Receiving a letter does not mean that you are a victim of identity theft. We are recommending that people review their letter and the recommendations provided. Currently, we are in the process of determining the possible risk for individuals, as a result of this incident.

Is there anything I need to do to in response to the exposure of my personal information?

Once you are enrolled in the ID Experts membership, you may also take advantage of your rights to the free fraud alert services offered by the three major credit bureaus. Placing fraud alerts will provide your credit with additional protection. In addition, doing so will give you access to copies of each of your credit reports at no cost to you.

My [spouse/child/family member/partner] has passed away and I handle their affairs. Can you speak/assist me regarding this letter?

Yes, I would be happy to help. Before we begin can I please have your name and relationship so that I can document this in our system?

[Agent – Please record the caller’s information]

I am with (Media); can you provide me with further information about the recent data breach with State of Oregon, DHS?

Media questions should go to DHS Communications at 503-945-6331 or <https://www.oregon.gov/DHS/DHSNEWS/Pages/Media-Request.aspx>

Is the letter legitimate? I’m worried this is a scam.

I can assure you the letter is legitimate and not a scam. You can check us out at www.oregon.gov/dhs. DHS is committed to protecting individuals’ security and privacy and takes this incident very seriously. We regret any inconvenience this may cause you.

I am calling on behalf of [letter recipient], can you assist me on their behalf?

[Agents: Please make sure you receive approval prior to speaking with someone other than the recipient.]



Questions beyond this list:

Please know, any additional questions that are asked specific to this event (not listed above), the agent will respond with, "Unfortunately that information has not been provided to me."

If we begin to see a common question not addressed above, we will work with your team to develop an appropriate response and then add it to the list.

We will be able to answer hundreds of other specific proprietary questions as it relates to identity theft, fraud alerts, credit bureaus, credit reports, security freeze, etc.