

Privacy/Security UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 17

JAN. 2007

Resources

Privacy Program

(503) 945-5780

Information Security

(503) 945-6812

Information Security/ Privacy Web site

[www.oregon.gov/DHS/
admin/infosec/](http://www.oregon.gov/DHS/admin/infosec/)

Privacy Help Email

PrivacyHelp, DHS

Information Security Email SECURITY, DHSINFO

Privacy Policies

[www.dhs.state.or.us/policy/
admin/privacylist.htm](http://www.dhs.state.or.us/policy/admin/privacylist.htm)

Information Security Policies

[www.dhs.state.or.us/policy/
admin/infosecuritylist.htm](http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm)

*Send requests for
future Privacy/Security
Update topics to:
dhs.privacyhelp@state.or.us*



EAP Assistance Available for Identity Theft Victims

Becoming a victim of identity theft is a frightening, time-consuming, and often expensive experience. There is a lot of information available on how to prevent identity theft and what to do about it should you become a victim.

You are encouraged to continue to educate yourself on prevention and what to do if it happens. Cascade Centers, the DHS Employee Assistance Program, presented a series of articles on Identity Theft. They are on the Web at www.cascadecenters.com/employee_feature_archive.htm#cascade.

Should identity theft actually happen to you, chances are you won't have time to read back through the articles. You would likely be too upset to do so, and could benefit from talking to someone who could provide you with guidance.

Cascade Centers can provide this help. You can call them at 1-800-433-2320 any time—day or night—for advice on an actual incident. For more information, there is a flyer on the DHS Safety and Health Web site at www.dhs.state.or.us/admin/hr/safety/health.htm#eap.

The DHS Information Security Office has Federal Trade Commission brochures that are filled with helpful information as well as phone numbers for all of the credit reporting agencies.

To request a copy of the brochure you can phone 503-945-6812 or email dhsinfosecurity@state.or.us.

DHS Business Continuity Management Program Update

DHS has implemented a Business Continuity Management program. This program coordinates the planning efforts for **three key areas:**

Emergency Management, Business Continuity Planning and Disaster Recovery.

The program is housed within the Information Security Office (ISO), which lives within Administrative Services; however Public Health, Information Security Office and Office of Information Services individually manage the three key areas respectively.

Emergency Management (EM) consists of two components: Health and safety of the public that affects all Oregonians relating to large scale events.

"CONTINUITY" cont. page 4...

A Different Kettle of "Phish"

"Phish" emails are emails that are designed to trick a recipient into revealing confidential information, such as passwords and credit card details. The sender usually masquerades as a trustworthy person or a legitimate business. Almost all of us have received "Phishing" emails here at DHS. Most of the Phishing attempts have targeted customers of banks and online payment services, but a new method has emerged that is one of the sneakier scams that you should be aware of. This method is designed to trick you into revealing not only your credit card account information, but also the three digit security code on the back of your credit card. This code is now being used by legitimate businesses to ensure that the person using the card has the card in their possession and has not just obtained the account number.

How the Scam Works

A user receives an email that thanks them for their purchase of an item. It states they will be billed a certain amount and that they can expect shipment any day.

(However, the user hasn't purchased anything!) The email contains a link that directs the user to a Web site in case there is any dispute. Unsuspecting users are concerned that they might be charged something they didn't order so they click on the link to the page. The Web site asks that the user confirm their account information by entering in the credit card number and the three digit security code. They are then told they will be taken to a page where they can cancel the bogus order.

In many cases, they can actually go to that page and "cancel" the order (the page is there just to maintain the illusion.) However, the damage has been done and the Phishers now have the information they need. The user won't know that they have been scammed until the bad guys use the card and the user receives a bill from the credit card company.

ISO has also seen a version of this scam that asks users to call a phone number to confirm the order. So the moral of this particular story is to not give out any confidential information unless you are absolutely certain it is legitimate!

How to Protect Yourself

Users who are contacted about an account needing to be "verified" can take steps to avoid Phishing attempts by contacting the company that is the subject of the email to check that the email is legitimate or by typing in a trusted Web address for the company's Web site into the address bar of their browser to bypass the link in the suspected Phishing message. It is very rare that a company will ask you to verify your account information via email. Nearly all legitimate email messages from companies to their customers will contain an item of information that is not readily available to Phishers.

Some companies, like PayPal, always address their customers by their username in emails, so if an email addresses a user in a generic fashion ("Dear PayPal customer") it is likely to be an attempt at Phishing. Emails from banks and credit card companies will often include partial account numbers. Therefore, one should always be suspicious if the message does not contain specific personal information.

“CONTINUITY” continued...

EM also includes the health and safety of DHS employees relating to incidents that affect only one building or a small number of buildings.

These efforts are facilitated by Public Health, DHS building evacuation plans, etc.

Business Continuity Planning addresses the details on how to continue the business functions in the event of a disruption of everyday services. These efforts are facilitated through the Information Security Office (ISO), with representation from across the department.

Disaster Recovery efforts address the technology recovery in the event of a disruption and are facilitated through the Office of Information Systems (OIS).

How does this affect you?

Since specific sections are handling Emergency Management and Disaster Recovery, the Divisions’ focus is on Business Continuity Planning.

The Information Security Office has been working with representatives from each division and from offices within DHS to address Business Continuity Planning.

DHS has already identified its business functions, including those functions considered critical for each division.

Initial planning will be centered around those daily events that are more likely to happen (i.e., fire in a building, power outage, etc.) rather than those that may be more catastrophic and will require statewide and/or county efforts.

Key business continuity program efforts over the next six months include:

A. Alternate site planning—Planning for relocation of business functions for each building.

B. Policy development—ISO will lead the departments efforts in developing policy and procedures for continuity planning

C. Identifying staff resources—Each division/office is identifying staff that will be responsible for coordinating their planning efforts and using the electronic management tool for plan development.

D. Patient re-location—an aggressive six-month plan is in place to address re-location strategies for

patients at our facilities. The initial focus will be on relocating patients if one or more of the building is uninhabitable.

E. Electronic management tool—DHS has purchased an electronic management tool to collect planning information and help coordinate plans. The tool is currently being structured to accommodate DHS planning efforts throughout DHS. Rollout to plan managers begins in February 2007

F. All staff training—each employee will be required to complete the 15-minute training session regarding Business Continuity Planning that is in development.

For additional information, questions and key contacts for your area, visit the Business Continuity Planning Web site at www.dhs.state.or.us/admin/infosec/bcp/

The information provided in the Privacy/Security Update is intended for employees of the Oregon Department of Human Services. It is not intended as advice, legal or other, to any entity outside of the Department.