

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 21

OCTOBER 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*



Announcing the new mail processing and privacy Web site

DHS has launched a new Web site that includes tools and resources to ensure client and employee privacy when the state shuttle or other mail services deliver DHS envelopes and parcels. You can access this site at www.dhs.state.or.us/mail/

Why are we launching this Web site?

DHS is required to protect confidential, sensitive client and employee information. Some of this hard copy information is sent from one office to another through the mail. However, multiple pieces of mail, many with private information, have been misdirected or are undeliverable.

The DHS Human Services Building in Salem reports approximately 30 pieces of undeliverable mail per week; an estimated 75% of this mail contains sensitive or confidential information. DAS Shuttle Service reports several inadequately addressed parcels, including client files, with no return addresses. These pieces cannot be returned to the senders.

A survey of 49 front desk branch office employees revealed they had little to no training on effective mail processes. The survey also showed that only 11% of those offices log incoming client files and 20% log or track outgoing client files.

With these issues in mind, the Mail Processing and Privacy Web site was conceived to provide tools and resources to safeguard confidential, sensitive mail. Following these procedures will allow us to maintain compliance with federal rules, reduce risk of unintended disclosure of confidential and sensitive information, and improve its delivery and tracking.

Tools and resources

The following tools and resources are available on the Mail Processing and Privacy Web site:

"NEW SITE" continued on page 2...

“NEW SITE” continued from page 1

- ◆ Link to state shuttle stops and schedule
- ◆ Link to Human Services Building (HSB) E-Codes (Salem)
- ◆ Link to current branch office/program addresses
- ◆ Link to current Post Office Box numbers
- ◆ Links to the US Postal Service and United Parcel Service Web sites
- ◆ General suggestions to improve successful mail delivery and return
- ◆ Instructions for logging and tracking incoming/outgoing client files
- ◆ Flow charts for field office outgoing mail with and without DAS Shuttle Service
- ◆ Flow charts for HSB incoming and outgoing mail
- ◆ Answers to Frequently Asked Questions

Managers’ action requests

- ◆ Please provide information about this new Web site during your next staff meeting. Discuss how to improve your office’s existing mail processes to ensure the accurate delivery of sensitive information. Make sure your front desk staff is aware of the Web site.
- ◆ Develop a process for logging outgoing and incoming client files. There is no “one size fits all” process for all DHS offices. Lost client files create great risks for our clients and for the department. Lost files create huge workloads for staff when trying to track down the file or literally having to recreate it in time for a court date.
- ◆ If staff receives a piece of shuttle mail that doesn’t belong in your office, they should check the return address and try to contact the sender through phone or e-mail. Do not put the mail back into the shuttle delivery bin because it will likely be returned to your office.
- ◆ Review the forms and documents your office uses regularly. Do they include clear instructions to the recipient about where to return it or what to do with it? Do you have forms or documents that would be more effective or efficient if additional instructions or contact information was provided? If so, work with your program’s administrators and the Office of Document Management to revise the forms.

Contact Jane Alm, DHS Privacy Officer, if you have questions about this Web site: jane.alm@state.or.us; Phone: 503-947-5255

**Privacy
Contacts**

Privacy Officer

Jane Alm, (503) 947-5255

Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Gloria Anderson

CAF/Pro. & Policy, (503) 945-5700

Ronald Barcikowski

CAF/OVRS, (503) 945-6734

Donna Weaver

SPD/Field Services, (503) 945-5977

Marilee Bell

SPD/DD, (503) 947-5262

Diane Duncan

AMH, (503) 945-6083

Steve Modesitt

Public Health, (971) 673-1293

Joni DeTrant

State Hospitals, (503) 945-2981

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



DHS required to comply with new legislation

The passage of Senate Bill 583—*the Oregon Consumer Identity Theft Protection*

Act—means consumers will have more tools to protect them against identity theft and Oregon businesses and government will have clear direction and expectations to ensure the safety of the personal identifying information they maintain.

Personal information includes a consumer's name in combination with a Social Security number, Oregon drivers' license number or identification card number, financial, credit or debit card number along with security or access code or password that would gain access to a financial account.

Each year thousands of Oregonians become victims of identity theft. According to the Federal Trade Commission, Oregon is ranked 13th in the nation for this crime. Victims of identity theft suffer both financially and emotionally.

Those who have had their personal information stolen may encounter multiple unauthorized charges on credit cards and unauthorized withdrawals from their bank accounts.

The result may be damaged credit records, which can take months or even years to clean up. Identity theft victims also lose their sense of security, similar to a home burglary.

Specific protections of the law:

◆ **Security Freeze**—Effective October 1, 2007. All Oregonians will be able to place a security freeze on their credit file maintained by a credit reporting agency, such as Equifax, Experian or TransUnion.

There is no fee if a person is a victim of identity theft and has reported the theft of their personal information to a law enforcement agency. For other consumers, the credit reporting agency may charge a fee of no more than \$10.

Those who do place a credit freeze on their report can “thaw” their file to apply for new credit. Certain entities such as law enforcement agencies and businesses collecting existing debt still will be able to access the credit file.

◆ **Notification of a Breach**—Effective October 1, 2007. Anyone (business, government, non-profit

or individual) who maintains personal information of Oregon consumers will be required to notify his or her customers if computer files containing that personal information have been subject to a security breach.

The notification must be done as soon as possible unless law enforcement believes the notification will impede a criminal investigation. In most cases you can notify in writing, but the law allows for electronic notice if this is the primary manner of communication between you and your customer.

You may also notify by telephone if you directly contact each customer. If you can demonstrate the cost of notification is more than \$250,000 or the number of individuals to be notified is more than 350,000, you may notify through major Oregon television and newspaper media and through your Web site, if you maintain one.

◆ **Protection of Social Security numbers**—Effective October 1, 2007. Consumers are especially vulnerable to identity theft if their Social Security number has fallen into the wrong hands. Anyone who maintains SSNs will be prohibited from printing Social Security numbers on documents that are mailed if not requested by the customer.

Snail mail alert

There is no Department of Administrative Services (DAS) shuttle service to McMinnville or Roseburg.

For a complete list of DAS' scheduled shuttle stops, go to their online Web site: <http://www.dhs.state.or.us/mail/>

“LEGISLATION”
continued on page 5...

SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM

(Our apologies to Monty Python)

Tired of receiving e-mails offering to help you lose weight, get rich and earn a diploma by simply clicking on a handy link?

You're not alone!

A recent survey by Symantec found that spam levels account for about 66 percent of e-mails. Despite efforts to combat junk e-mail, spammers continue to adopt new methods to evade detection by e-mail filters.

One difficulty faced by those working to reduce spam is the speed with which spammers change their tactics. As recently as six months ago, almost 52 percent of all spam received was image spam, in which the text of the message is presented as a picture in an image file. Last month, this form of spam accounted for only 8 percent of all spam. This is an indication that anti-spam filters are increasingly successful at combating this type of spam.

What is spam?

- **S**tupid **P**ointless **A**nnoying **M**ail?
- **S**ly **P**eople **A**cting **M**oronicallly?
- **S**crambled **P**ieces of **A**sinine **M**arketing

Actually, it doesn't stand for anything—it's just unsolicited e-mail (commercial or otherwise) that comes to your Inbox in droves. How it was named "spam" is debated in countless newsgroups and Web sites. But it is pervasive and one of the most nimble forms of communication on the Internet.

Spammers are highly adaptable and newer styles of spam are on the rise. In the last month, the percentage of spam messages utilizing PDF images rose from 3 percent to 7 percent and is still on the rise. Two other new styles of spam are emerging, involving the attachment of Excel and zip files to spam messages.

However, traditional methods are still used. Fake greeting cards remain a spammer favorite. These cards may appear to come from legitimate sources and instruct the user to click on a link to access their "greeting card." However, by clicking on that link, the user unwittingly downloads a "Trojan Horse" program that installs harmful software onto the computer.

What is the state doing about spam?

The state uses several anti-spam filters to filter spam from our mailboxes. These filters use publicly available "blacklists" to determine if e-mail is coming from a legitimate source.

"SPAM" continued on page 5...

DHS BCP Program Coordinators

Program sponsor: Clyde Saiki, DHS deputy director, 503-945-5731

Program manager: Patty McCary, ISO, 503-945-6996

Manager: Kelli Heftin, ISO, 503-947-5230

Administrative Services

Linda Riddell, Facilities, 503-945-5817

Sharon Domaschofsky, Facilities, 503-947-5018

Dave Wallace, OIS, 503-945-5992

Jeremy Emerson, OC&P, 503-945-6878

Kelly Stoll, OC&P, 503-945-5696

Julie Davie, HR, 503-945-6380

Gary Whitehouse, OPA, 503-945-6934

Debby Williams, OPAR, 503-378-5620

Jan Lemen, FDM, 503-378-3477

Children, Adults and Families

Leona Gildersleeve, CAF Field Admin, 503-945-7000

Irvin Minten, CAF, 503-373-1200 (ext. 543)

Health Services

Maynard Hammer, OSH, 503-945-2866

Dusty Charters, OSH, 503-947-1080

Steve Modesitt, HS/PH, 971-673-1293

Dale Elder, HS/DMAP, 503-945-6589

Robert Furlow, EOTC, 541-276-0810 (ext. 331)

Nick Reed, EOTC, 541-276-0991 (ext. 431)

Edie Woods, HS/AMH, 503-945-6189

Seniors and People with Dis.

Bob Clabby, SPD, 541 276-4511 (ext. 470)

Donna Weaver, SPD, Field Services Manager, 503-945-5977

Conrad Bozlee, SOCP

“LEGISLATION” continued from page 4...

In addition the SSN cannot be printed on cards or documents that must be used by customers to obtain goods or services, nor can it be publicly displayed or posted such as on a Web site. This doesn't apply to the use of SSNs for internal verification purposes. The law allows an exception for records that are required by law to be made available to the public.

◆ **Safeguarding personal information—Effective January 1, 2008.** If you own and maintain consumers' personal information such as driver's license numbers, Social Security numbers or financial information, you must develop, implement and maintain reasonable safeguards to protect the security and confidentiality of the information. This also includes the proper disposal of information.

The Department of Consumer and Business Services is charged with enforcing these new laws. The department's Division of Finance and Corporate Securities has developed materials and presentations for businesses and consumers to better understand their rights and responsibilities.

A copy of Senate Bill 583 and other detailed information is available on the Web at www.dfcs.oregon.gov. Click on Identity Theft.

“SPAM” continued from page 4...

Unfortunately, spammers also have access to the blacklists and can adjust their e-mails to bypass the filters. This does not mean that the blacklists are not effective.

In fact, the blacklists ensure that the state isn't bombarded by “old spam” each day. These filters are blocking 50-75 percent of spam directed at the state each day.

What is DHS doing about spam?

DHS uses a secure email product called Tumbleweed. Part of this secure e-mail solution includes dynamic anti-spam (DAS) filtering. DAS filtering uses real-time updates to the spam filters to determine what e-mail is spam and what e-mail is legitimate.

The updates occur approximately every two hours. DHS has been using these filters since July 30, and the traffic is substantial.

For instance, between August 1 and August 19, DHS received 340,000 emails. The statistics for that two-week period showed that only 54 percent of our e-mail traffic was legitimate.

Of all the e-mails we received, 103,532 emails could be classified as definite spam and 54,990 as “probable.”

The spam filters stop the definite spam but have to allow the e-mail messages marked as probable because of the addressing scheme used by the e-mails.

But I'm still receiving spam!

Yes, you certainly are. The residual spam that creeps through the state spam filters is “new” and sent from addresses that haven't yet made it to the blacklists.

Often times, spammers are able to use e-mail addresses that fool or “spoof” the filters.

These are addresses that can't be placed on blacklists because they appear to be from legitimate servers such as “state.or.us.”

But notice that you usually do not receive them from the same address each time.

In addition to using the DAS filters supplied by Tumbleweed, Information Security Office (ISO) senior analysts have created supplemental filters to combat image spam (such as the PDF spam) and e-mail addresses that haven't yet made it to the blacklists.

These supplemental policies are adjusted each day based on the spam traffic captured by the Tumbleweed device.

How can I combat spam?

Unfortunately, spam is not likely to go away any time soon. The battle for supremacy between spammers and spam filters will continue.

However, you can help yourself in a big way. The best way to combat spam is to delete it without opening it. Ask

“SPAM” continued on page 6...

ISO's Business Continuity Program

'Even the best plan will seldom prove perfect in the first encounter with the enemy, but the act of planning puts the odds of victory in our favor'

—*SunTzu (paraphrased from the "Art of War")*

The Business Continuity Planning Program forges ahead. Nearly 60 DHS planning coordinators and team members have been attending training for the electronic management tool.

This tool will assist DHS in its planning efforts as well as maintain current data and information. What one coordinator had to say:

"We all know that the old way, a dusty old binder on a shelf, doesn't meet the need in most cases and rarely gets the attention and upkeep that it must have to be useful. I think having any automated/electronic tool will help to ensure that plans and all the "parts" are kept up to date and accessible from anywhere and by anyone who needs to have access. I think that eBRP will be helpful in achieving the long-term goal of this project."

—*Facilities Manager Sharon Domaschofsky*

According to industry analysts, 80 percent of unplanned downtime is caused by people and process issues. Reducing the number of people backing up critical data can dramatically increase protection and physical security.



COMING SOON
DHS Business
Continuity Planning
(BCP) training online!

"SPAM" continued from page 5...

yourself, "Do I know where this came from?" "Did I ask for this product or information?" "Do I know who sent this?" It is best to be cautious if you don't know the answers to these questions.

Avoid replying to the sender

Replying and typing "REMOVE" in the subject line is the best way to let a spammer know that they reached a legitimate address. It's like waving a flag that says, "Go ahead and send me more!"

Think before you "click on the link" in the e-mail. DHS users should be wary when clicking on unfamiliar links in e-mails and users should also watch for warning signs.

Examine the link and watch for anything suspicious. For instance, an exposed IP address which indicates the e-mail is probably not a legitimate source.

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 otherwise, to any entity outside of the department.