

Date: July 22, 2009
Audience: All DHS employees
From: Kyle Miller, DHS Information Security Officer
Subject: Malicious Trojan/virus alert!

We are experiencing a high number of virus infections on DHS computers related to the 'Pushdo' Trojan. These infections appear to be occurring on computers where users have logged into their personal e-mail accounts, such as Gmail, Yahoo, and Hotmail via the Internet. Several reports indicate that the source of the virus may be spam e-mail containing an invitation to view a fake e-card.

Research on Pushdo indicates it is generally delivered via spam e-mail and encourages the recipient to visit a fake web site. Favorite targets are customers of financial institutions or other organizations where an online account is utilized. Some examples: PayPal; airlines; social networking sites like Facebook, MySpace, and Classmates. Pushdo installs files on your computer that silently collect logins and passwords (via a keylogger), personal information, and computer settings.

Protect yourself

Do not open e-mails from unknown senders and especially avoid clicking on any web links contained in these e-mails. Avoid clicking on pop-ups and advertising links when visiting websites. Generally, legitimate organizations will not ask you to update your information by clicking a link. They *may* ask you to log in to your account independently (outside of the e-mail) to verify your information. If in doubt, contact them by phone or in-person.

Symptoms of infection

- You are bombarded by pop-up ads, even when you aren't browsing the Internet.
- Your browser home page is changed unexpectedly.
- Your computer is sluggish or appears to lock up.

Removal of Pushdo can be difficult because it can reinstall itself each time your computer is restarted. It also shuts down many common anti-virus, spyware, and firewall programs. Generally, an infected computer must be wiped clean and then re-imaged to its original state wiping out all files on the C-drive including favorites, special software, and custom settings.

If you have questions about Pushdo or other viruses, contact the Information Security Office (ISO) at: security.dhsinfo@state.or.us or 503-945-6812.

If you believe your computer may have a virus, contact the OIS Service Desk, 503-945-5623 or dhs.servicedesk@state.or.us.

