Division of Public and Behavioral Health (DPBH)

INTRODUCTION TO DPBH SECURE EMAIL

Updated November 2015

What is secure email?

Secure email ensures that Personal Information (PI), Personal Health Information (PHI) and other sensitive information is protected and can only be read by the recipient through the use of the leading identity-based encryption technology. Secure email is easy to use and enables you to receive, reply to and initiate secure email without the need to download or install any software. You can manually trigger secure email to encrpt a message **(even if it does not include PI, PHI or other sensitive information)**, by use of the phrase "**secure email**" in the email subject line.

Why does DPBH need secure email?

Various state / federal laws and federal information exchange agreements require the use of encryption when transmitting PI, PHI, or other sensitive data.

Assembly Bill (AB)179, revised provisions governing personal information in NRS 603A effective 07/01/2015. This bill expands the definition of PI: to include electronic mail addresses and passwords, driver's authorization card numbers, medical and health insurance identification numbers and other similar information.

What is personal information?

As amended, NRS 603A.040 defines personal information (PI) as follows:

1. Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
    (a) Social security number.
    (b) Driver's license number, driver authorization card number or identification card number.
    (c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.
    (d) A medical identification number or a health insurance identification number.
    (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records."

Is the DPBH Outlook email system within the State of Nevada, Enterprise IT Service's (EITS) email system?

Yes.

What is the impact of secure email to entities on the State of Nevada, EITS' email system?

There will not be any visible difference to users within the State of Nevada email system for the majority of state email recipients (see next section for exceptions). For example, an email you sent from your computer to a co-worker within the State of Nevada email system (jsmith@dhhs.nv.gov) will be received exactly as it is today.

Only recipients that are external to the State of Nevada email system will see the impact of secure email. For example, if you send an email with PI, PHI or other sensitive information from your work computer to someone outside the State of Nevada email system (jsmith@sbcglobal.net) they can follow the instructions provided in this document to access and read the email. **This document is publically available at DBPH.NV.GOV** by clicking on the CONTACT link, clicking on the Secure Email link, then clicking the Introduction to Secure Email link.

What government entities email systems are NOT within the State of Nevada, EITS' email system?

All Federal, County and some State entities are not part of the State of Nevada, EITS' email system. The known state entities are listed below:

- Controller's Office
- Public Employees Benefit Program
- Department of Motor Vehicles
- Supreme Court
- Attorney General's Office
- Nevada Department of Transportation
- Department of Corrections
- Department of Employment Training and Rehabilitation

What is Tranport Layer Security (TLS)?

The primary goal of TLS protocol is to provide privacy and data integrity between communicating systems by encrypting the data through a point to point tunnel.

As an external entity with the ability to support TLS, can we choose to use TLS so DPBH's use of secure email will have zero impact to our email users?

Yes, we highly encourage the use of TLS for those external entities that routinely receive DPBH email that may contain PI, PHI or sensitive information. **Please have your technical support staff contact the DPBH Information Security Officer (ISO) to initiate the use of TLS process**:

Kelly Kelly
775-684-3226
kellykelly@dpbh.nv.gov

If an external entity is using TLS do I still need to ensure the email goes through our Secure Email tool by using the phrase "secure email" in the subject line?

No. The external entity addresses below use TLS. The email communications between the DPBH email users and the external entity is encrypted in transit and will appear in the recipient's inbox as any other unencrypted email.

hms.com	hp.com	hpe.com
ibm.com	isysllc.com	lasvegasnevada.gov
lvmpd.com	magellanhealth.com	mail.co.washoe.nv.us
ntst.com	nvenergy.com	oisrt.state.nv.us
sedgwick.com	sedgwickcms.com	ssa.gov
switchlv.com	sxc.com	thomsonreuters.com
uhc.com	vistahealthplan.com	washoecounty.us

Secure email provides email usage reports for administration. What gives my employer the right to view my email usage?

DHHS Email Acceptable Use Policy states in part, "Employees are advised email sent and/or received is the property of the Department and employees have no right to privacy with regard to email usage on State information systems. Email sent or received by an employee containing unencrypted Personal Information (PI), Personally Identifiable Information (PII), and Protected Health Information (PHI), Social Security Administration data, or Federal Tax Information (FTI) data must not be stored by an employee on non-state approved systems. Email is subject to monitoring, recording, and review. All outgoing PI/PII/PHI/FTI/SSA data must be securely transmitted and protected from unauthorized disclosure. All PI/PII/PHI/FTI/SSA data sent using the State email system must be encrypted when being transmitted outside the State of Nevada email system."

How does secure email work?

When an email is initiated or responded to by a DPBH account (identified by the extension **health.nv.gov**), secure email will determine if encryption is needed. This decision is based on predefined criteria. If the criteria are met, the email will be encrypted and sent to the recipient. You can also manually trigger encryption by typing the phrase "secure email" in the email subject line (even if it does not contain PHI, PI, PII, etc).

As a secure email recipient, do I need Cookies turned on?

Yes. As an email recipient external to the State's email system, you will need to enable Cookies. Instructions on enabling Cookies are included in the secure email help and within the pages of this document.

Will secure email distinguish between a Social Security Number (SSN) and any other nine digit number?

No. As a result, secure email will encrypt any message with a nine digit number.

Will secure email scan for sensitive information captured within a scanned document, snap shot, or screen shot?

NO. Secure email only scans text and views a scanned document, screen shot or snap shot as a graphic. Screen shots or snap shots that contain sensitive information should minimally be password protected with the sender provider the password through another means (such as a phone call or text).

When did secure email begin?

DHHS Divisions began using secure email as early as October 26, 2009.

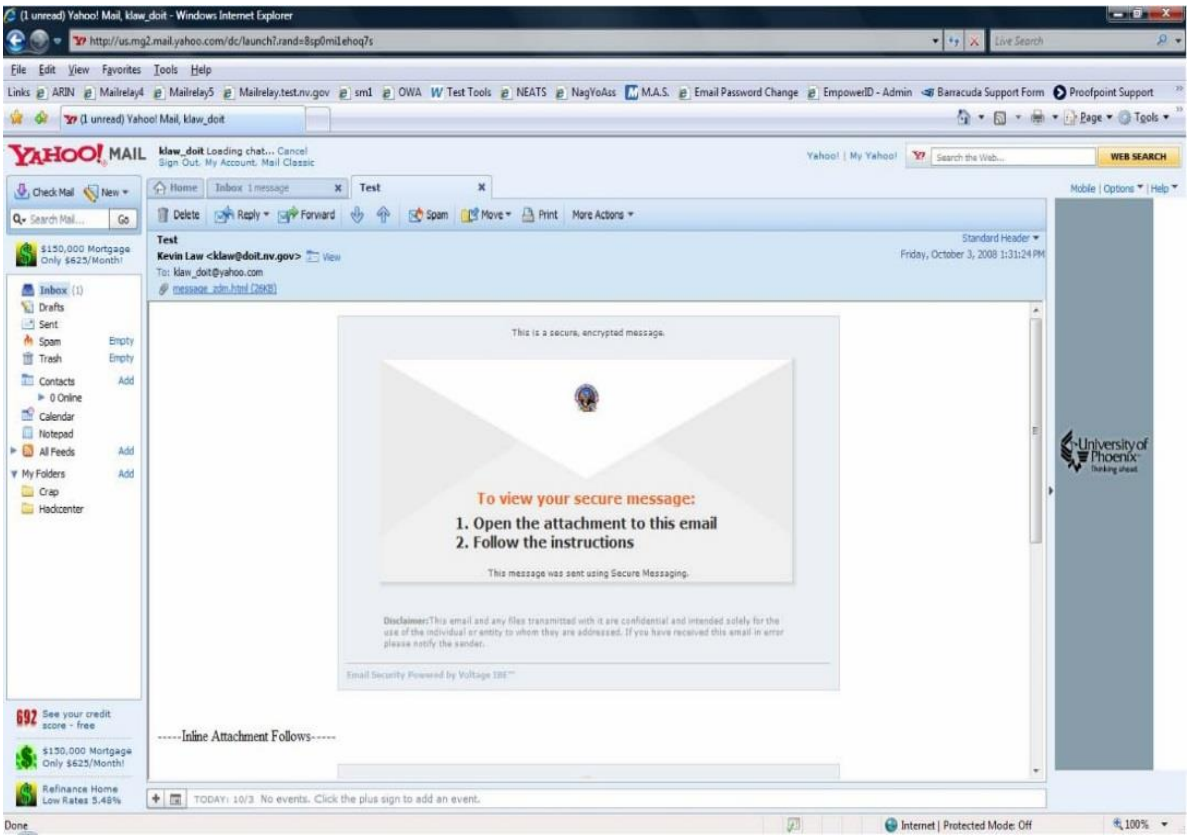
How do I as the recipient read a secure email?

The recipient must create an account within the State of Nevada secure email system to open secure emails from any Division under the Nevada Department of Health and Human Services. The recipient will be prompted to do this the first time they open a secure email.

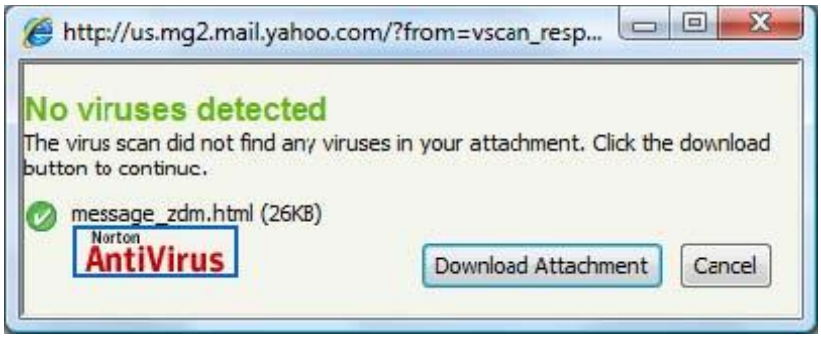
The end user presentation may differ depending on which web browser is being used by the recipient. This document uses both Yahoo and Charter to illustrate the end user presentation.

See the following instructions:

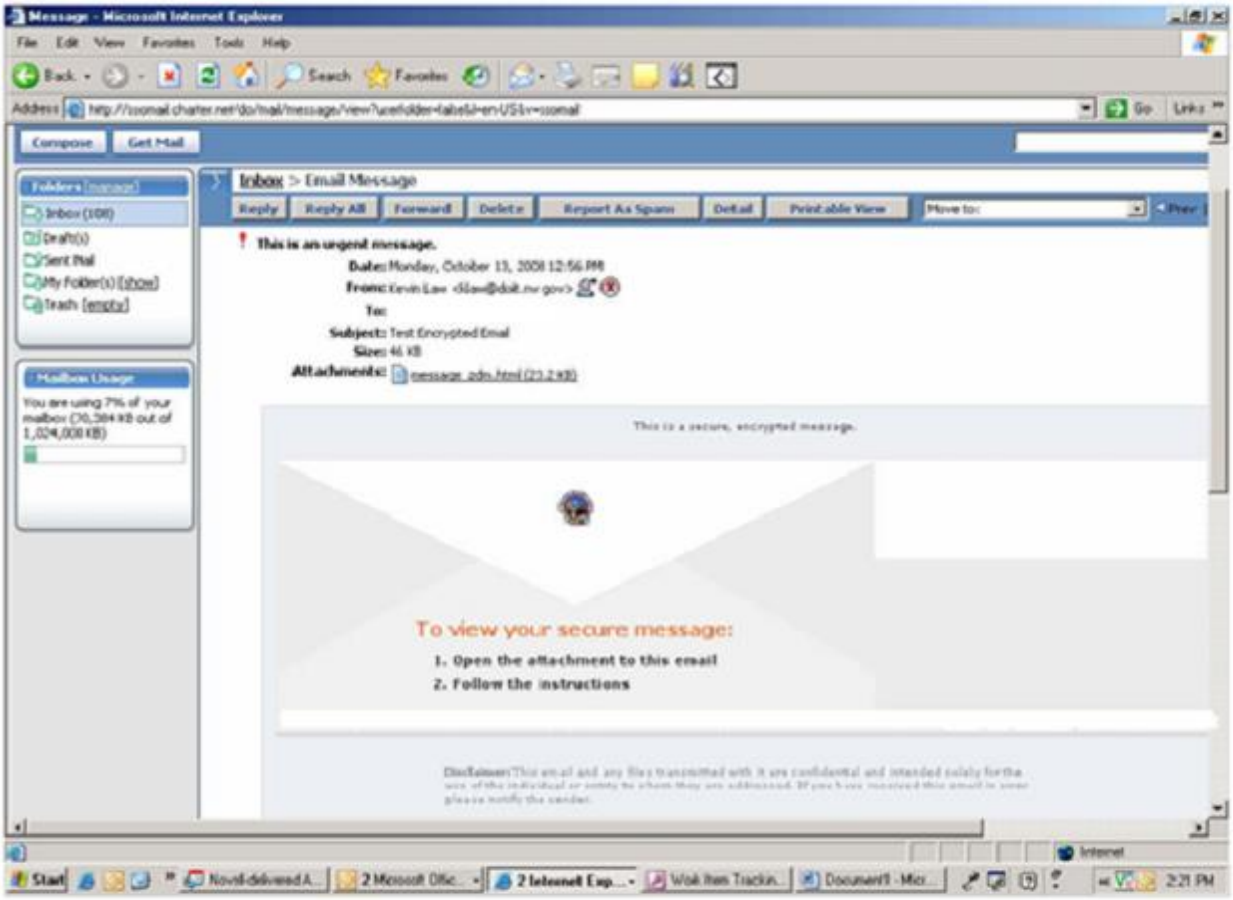
Here is how a secure email looks when it appears in the "Inbox" for a Yahoo webmail account:



When following the instructions to open the message and clicking on the attachment, Yahoo webmail does an antivirus scan on the attachment.

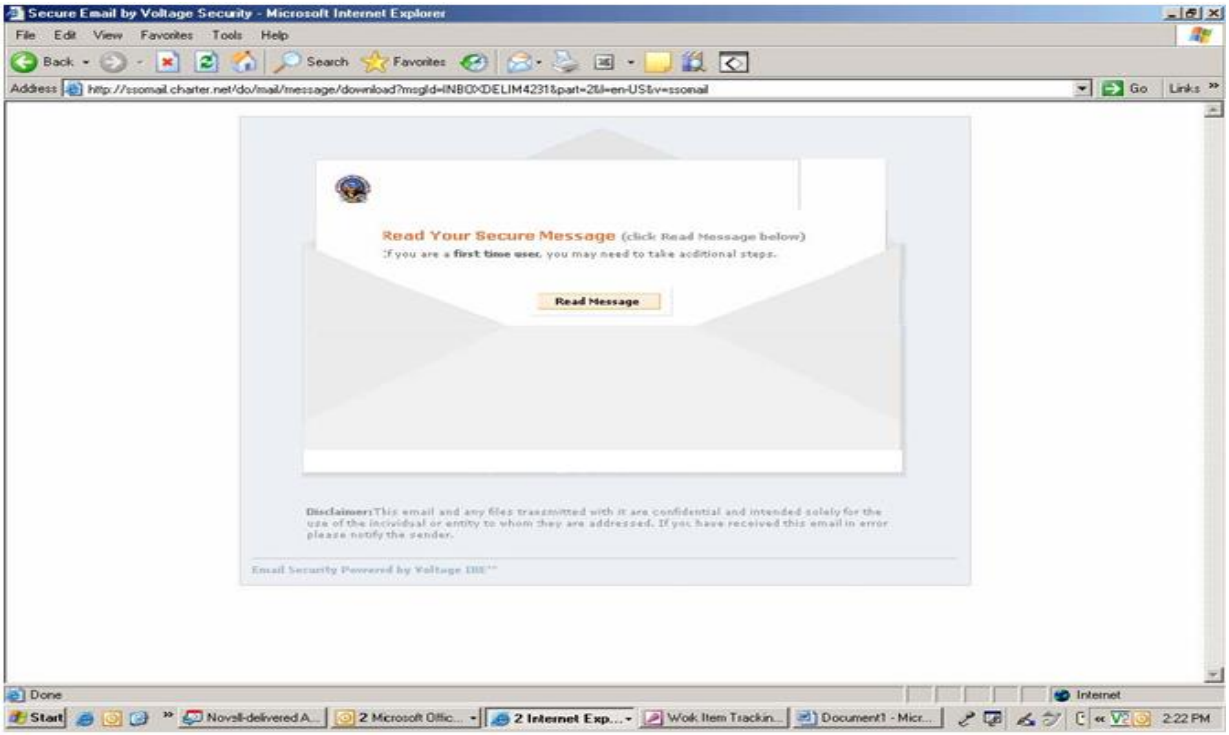


Here is what a secure email looks like when it appears in the "Inbox" for a Charter webmail account:

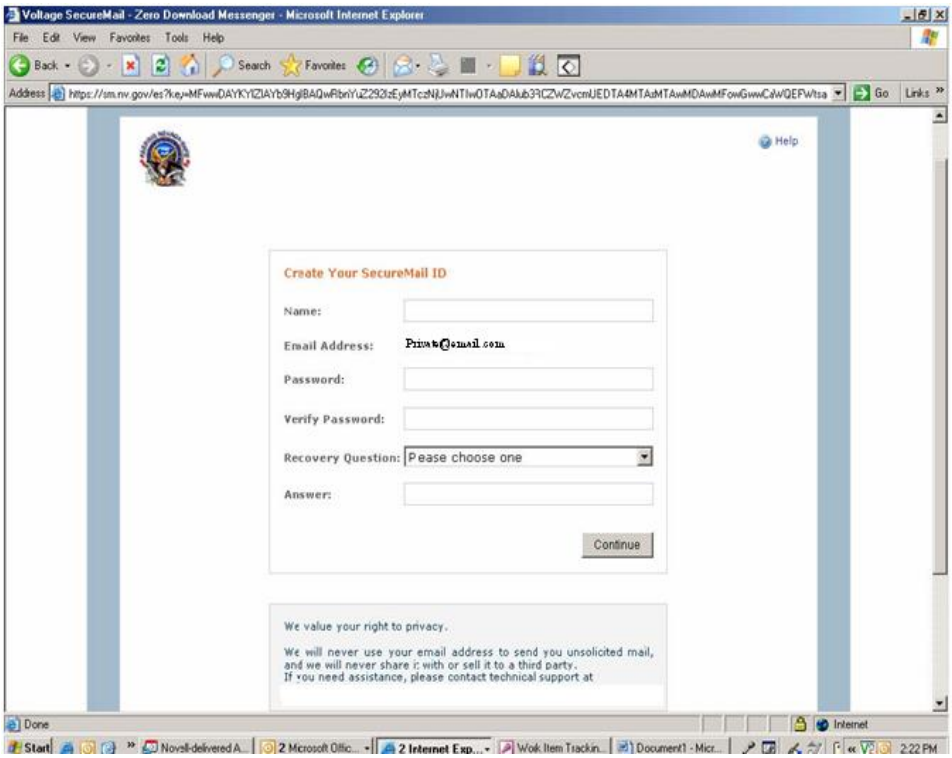


The secure e-mail recipient must click on the “message_zdm.html” attachment.

After the attachment is opened you will see the following "Read Your Secure Message" screen. You must click the "Read Message" button.



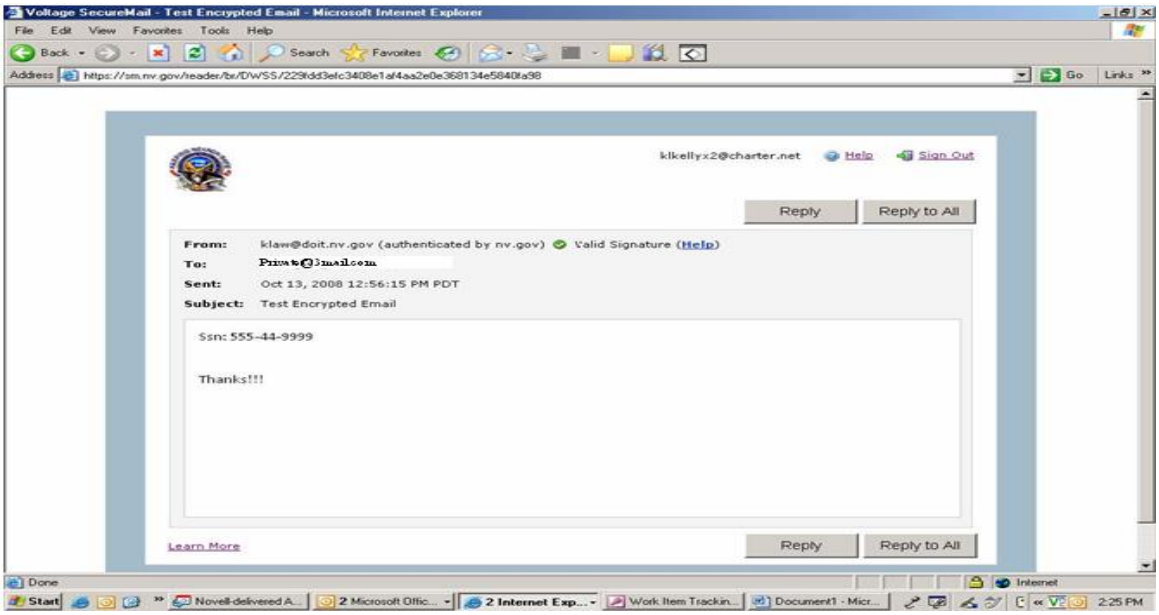
The **first time** a secure email recipient attempts to read a secure email they will need to create a Secure Mail ID.



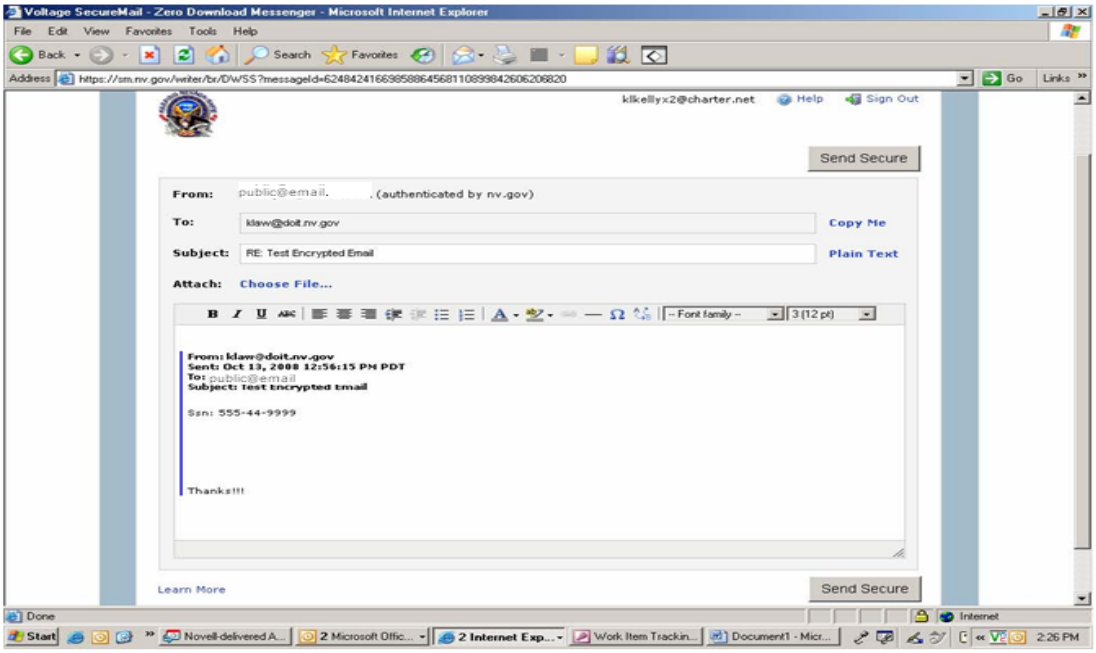
The secure email recipient enters the following information:

- Name
- Password
- Verify Password

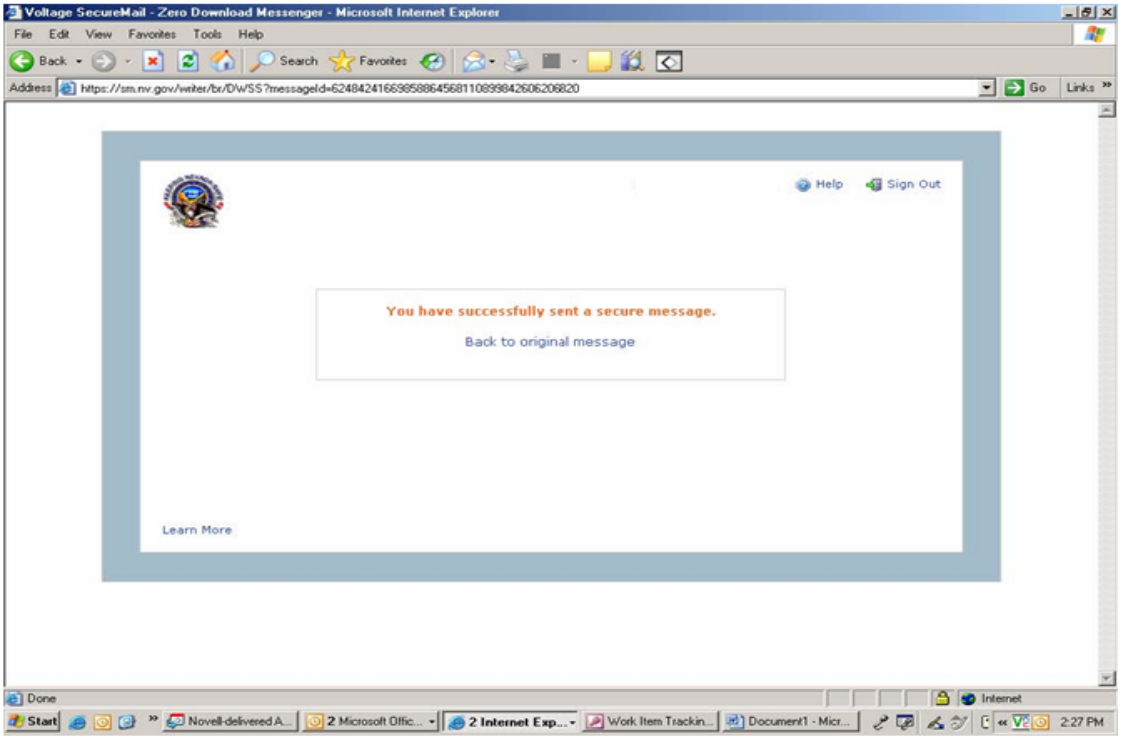
Select the Recovery Question and provide the response. Please note, the email password will expire in 90 days, as State policy requires. Should you on a subsequent login forget your password a recovery option will be provided. Click on "Continue" to display the secure email message as shown below.



When the secure email recipient clicks Reply or Reply to All they will see:



After clicking "Send Secure", the following displays:



The following information has been copied from the secure email help tool to provide additional information:

Enabling Cookies in Your Web Browser

Windows Internet Explorer:

1. Under the Tools menu, select "Internet Options".
2. In the Internet Options window, select the "Privacy" tab.
3. Click the "Advanced" button.
4. Check the box to "Override automatic cookie handling".
5. In Advanced Privacy Settings window, for First-party Cookies, select "Accept".
6. Click the "OK" button on the Advanced Privacy Settings window.
7. Click the "OK" button on the Internet Options window.

Firefox:

1. Under the Tools menu, select "Options".
2. In the Options window, select "Privacy".
3. In the Cookies section, ensure that the box next to "Accept cookies from sites" is checked.
4. Click the "OK" button.

If you have any questions please contact the OIT helpdesk at (775) 684-5906, (702) 486-3699 or email OITSupport@health.nv.gov.