SECURE E-MAIL COMMUNICATIONS PLAN

Updated August 25, 2011

Introduction

In October, 2008, the Division of Welfare and Supportive Services (DWSS) announced the introduction of secure e-mail through ASM 17-08. DWSS uses secure e-mail to ensure the protection of personal information (PI) being transmitted by electronic mail by using leading identity-based encryption technology.

What is Secure E-mail?

E-mail sent by DWSS staff becomes encrypted when sent to someone outside the state's e-mail system and our encryption tool detects the message contains personal information (PI) as defined by NRS 603A or other sensitive information. The message is received as an encrypted secure e-mail by the recipient.

Secure e-mail ensures that personal information (PI) and other sensitive information is protected and can only be read by the recipient by using the leading identity-based encryption technology. Secure e-mail is easy to use and enables you to receive, reply to, and forward secure e-mail.

Changes

At 7:00 P.M. on August 23, 2011, the Department of Information Technology (DoIT) migrated secure e-mail from the current encryption (Voltage) server to the new encryption (Proofpoint) server. DoIT estimated this migration to be complete by 10:00 P.M on August 23, 2011. During the migration DoIT held all outbound e-mail messages; once the migration was completed the messages were released. This delayed the delivery of the message but ensured secure delivery.

Secure e-mail messages received **prior** to August 23, 2011, at 7:00 P.M. will remain available to the secure e-mail recipient for approximately 90 days (November 23, 2011), at which time the encryption (Voltage) server will be retired. Secure e-mail recipients who need to retain a particular secure e-mail or open a particular secure e-mail received prior to August 23, 2011, at 7:00 P.M. will need to use their current credentials to open the secure e-mail and save the message prior to November 23, 2011. **PLEASE NOTE:** For a short period of time there may be a delay in the recipient accessing the secure e-mail messages received prior to August 23, 2011 at 7 PM. DoIT is currently working with Proofpoint engineers to resolve this issue timely. If a recipient continues to have difficulty accessing a particular e-mail after Monday August 29, 2011, the recipient will need to contact the DWSS Operations Helpdesk at nswdhelp@dwss.nv.gov or 775-684-0700.

Secure e-mail messages received **after** August 23, 2011, at 7:00 P.M. will require the secure e-mail recipient create a new account to decrypt and read the message. Any message that is sent after 7:00 PM on August 23, 2011, that meets the encryption criteria will be encrypted through the new Proofpoint encryption server

and the recipient will need to use their new credentials to decrypt and read the message.

How does Secure E-mail work?
When an e-mail is initiated or responded to by DWSS (identified by the extension dwss.nv.gov) the secure e-mail algorithm will determine if the e-mail needs to be encrypted based on predefined criteria. If it meets the predefined criteria the e-mail will be encrypted and sent to the recipient.

Why does DWSS need Secure E-mail?
Various state / federal laws and federal information exchange agreements require the use of encryption when transmitting PI or other sensitive data.

Nevada Revised Statute (NRS) 603A (Security of Personal Information) states:

A data collector doing business in this State shall not transfer any personal information through an electronic, non-voice transmission other than facsimile to a person outside of the secure system of the business of the data collector unless the data collector uses encryption to ensure the security of electronic transmission.

DHHS E-mail Acceptable Use policy states in part,

E-mail sent or received by an employee containing unencrypted personal information (PI), personally identifiable information (PII), protected health information (PHI), Social Security Administration data (SSA data), or federal tax information (FTI) data must not be stored by an employee on non-State approved systems. **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 e-mail system must be encrypted when being transmitted outside of the State e-mail system.**

What is Personal Information?
NRS 603A.040 defines personal information (PI) as follows:

"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:

1. Social security number.
2. Driver's license number or identification card number.
3. 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. The term does not include the last four digits of a

social security number or publicly available information that is lawfully made available to the general public."

Secure e-mail provides e-mail usage reports for administration. What gives my employer the right to view my e-mail usage?
The State of Nevada Information Security State Standard 4.65 regarding e-mail states in part,

Employees shall be informed that all e-mail sent on state systems can be recorded and stored along with the source and destination. Employees have no right to privacy with regard to e-mail usage on state systems. Management has the right to view employees' usage patterns and take action to assure that agency Internet and e-mail resources are devoted to maintaining the highest level of productivity. Recorded e-mail messages from state systems are the property of the agency.

DHHS E-mail Acceptable Use policy states in part,

Employees are advised e-mail sent and/or received is the property of the Department and employees have no right to privacy with regard to e-mail usage on State information systems. E-mail sent or received by an employee containing unencrypted personal information (PI), personally identifiable information (PII), protected health information (PHI), Social Security Administration data (SSA Data), or federal tax information (FTI) data must not be stored by an employee on non-state approved systems. E-mail 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 e-mail system must be encrypted when being transmitted outside of the State e-mail system.

Can I manually trigger secure e-mail to encrypt a message that does not contain PI or other sensitive information? Yes, by use of the word **tax** or **encrypt.**

Do I have to have Cookies turned on to read a secure e-mail?
Yes, Cookies must be enabled in order to access secure e-mail.

Will secure e-mail distinguish between a social security number (SSN) and a unique person identifier (UPI)? No. As a result, secure e-mail will encrypt both.

Will secure e-mail distinguish between a pseudo SSN and an actual SSN?
No. As a result, secure e-mail will encrypt both.

Will secure e-mail scan for PI captured within a scanned document, snap shot, or

screen shot? NO. Secure e-mail only scans text and views a scanned document, screen shot or snap shot as a graphic. Screen shots or snap shots that contain PI should be sent as a password protected attachment.

Example: A snap shot of a NOMADS production screen with client PI is pasted into a Word document and attached to an e-mail or is pasted directly into the body of an e-mail.

As an external entity with the ability to support Transport Layer Security (TLS), can we choose to use TLS so DWSS' use of secure e-mail will have zero impact to our e-mail users?

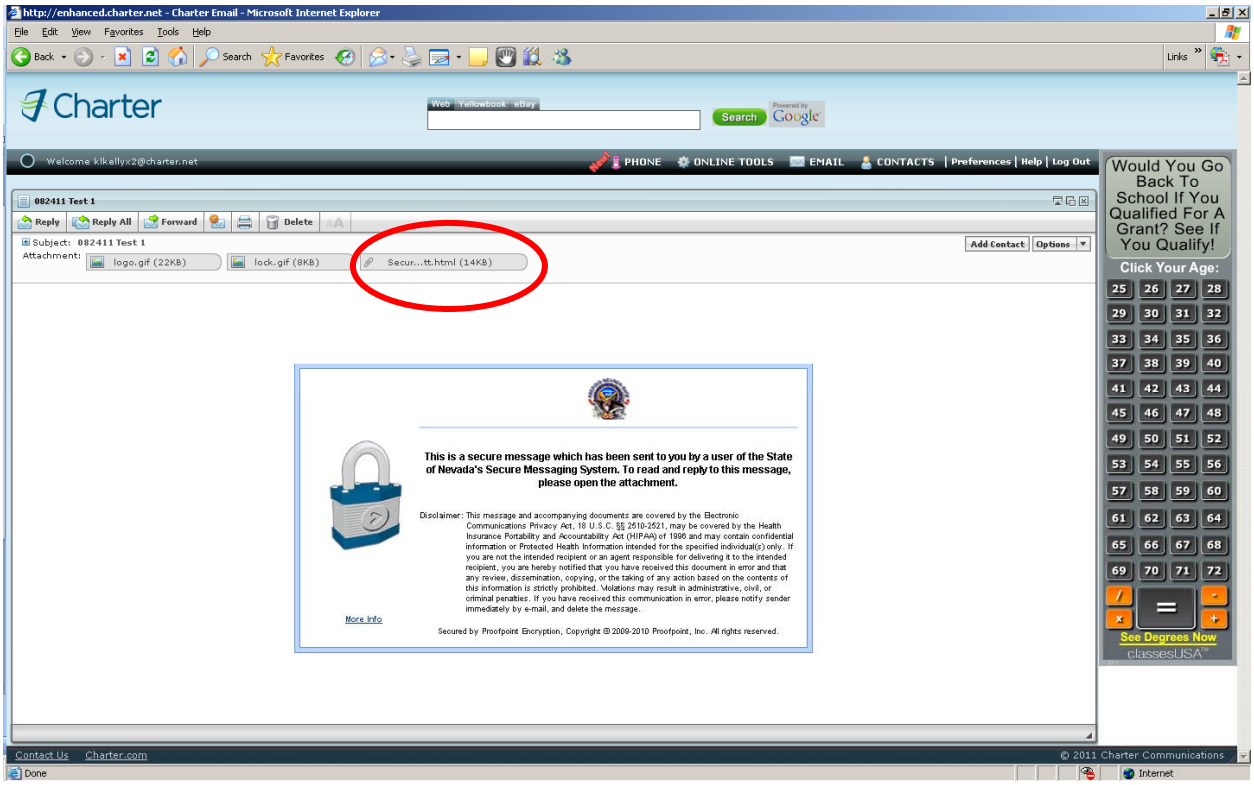
Yes, we highly encourage the use of TLS for those external entities that routinely receive DWSS e-mail that may contain PI or sensitive information. **Please have your technical support staff contact the DWSS Operations Manager to initiate the use of TLS**:

Larry Smolyansky
775-684-0512
775-671-5314
lsmolyansky@dwss.nv.gov

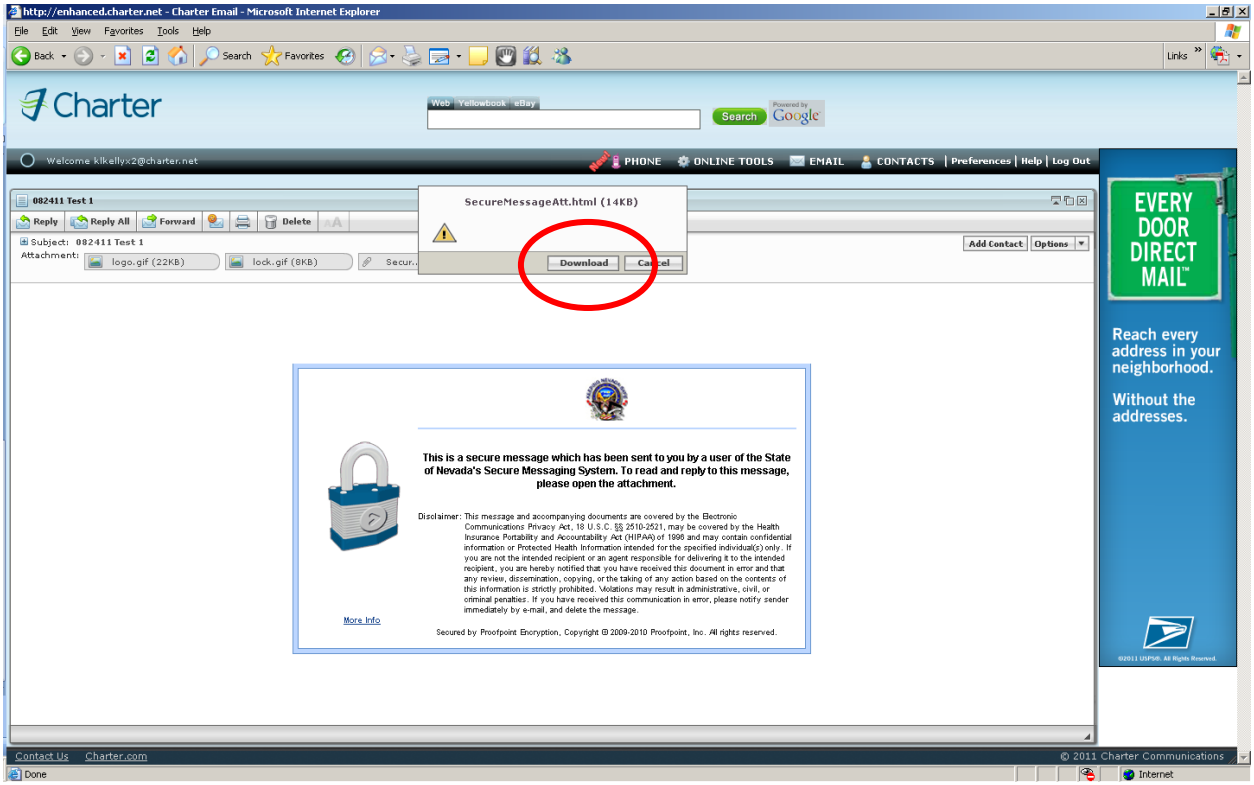
Do external entities have to support TLS to read a secure e-mail? No.

Will the 8/23/11 server migration impact entities using TLS? No, there is no impact to entities we send e-mail to via TLS connections.

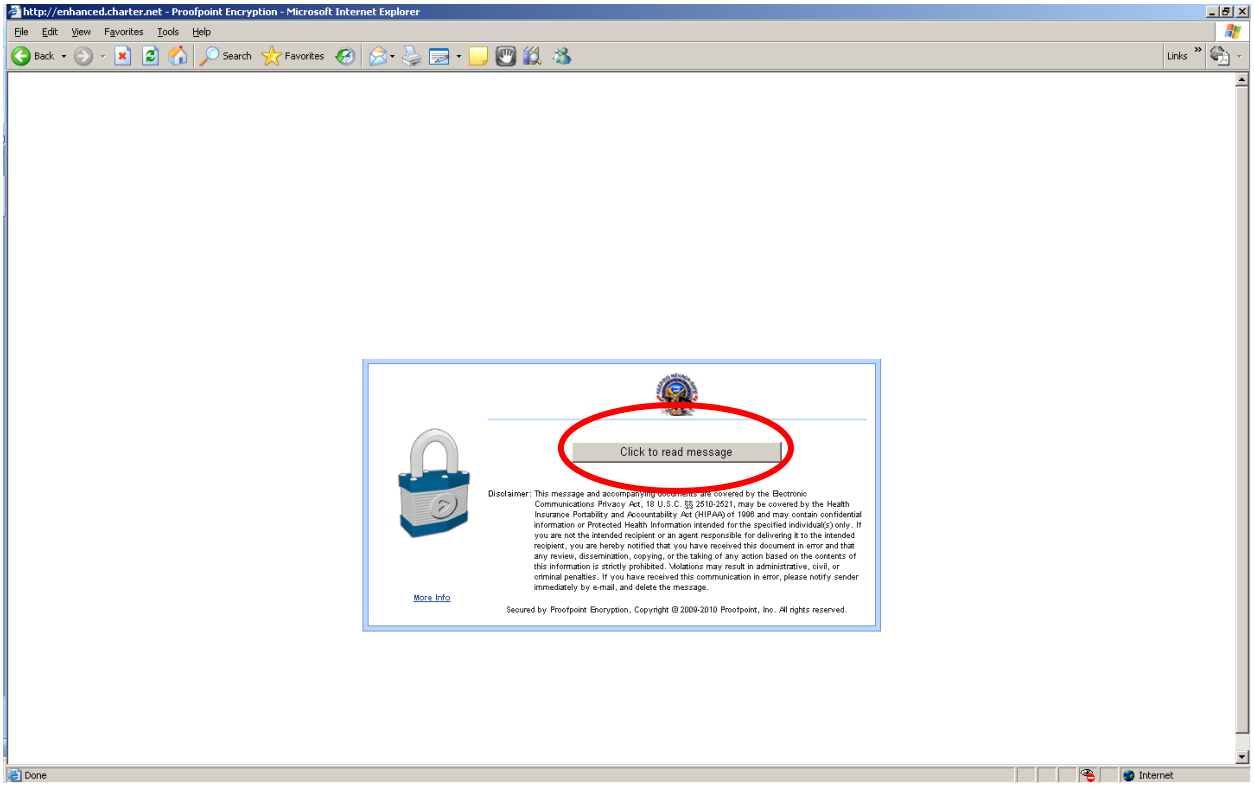
How do I as the recipient read a secure e-mail message?
The end user presentation may differ pending on which web browser is being used by the recipient. This document uses Charter to illustrate the end user presentation. Here is what a secure e-mail looks like when it appears in the "inbox" for a Charter webmail account:



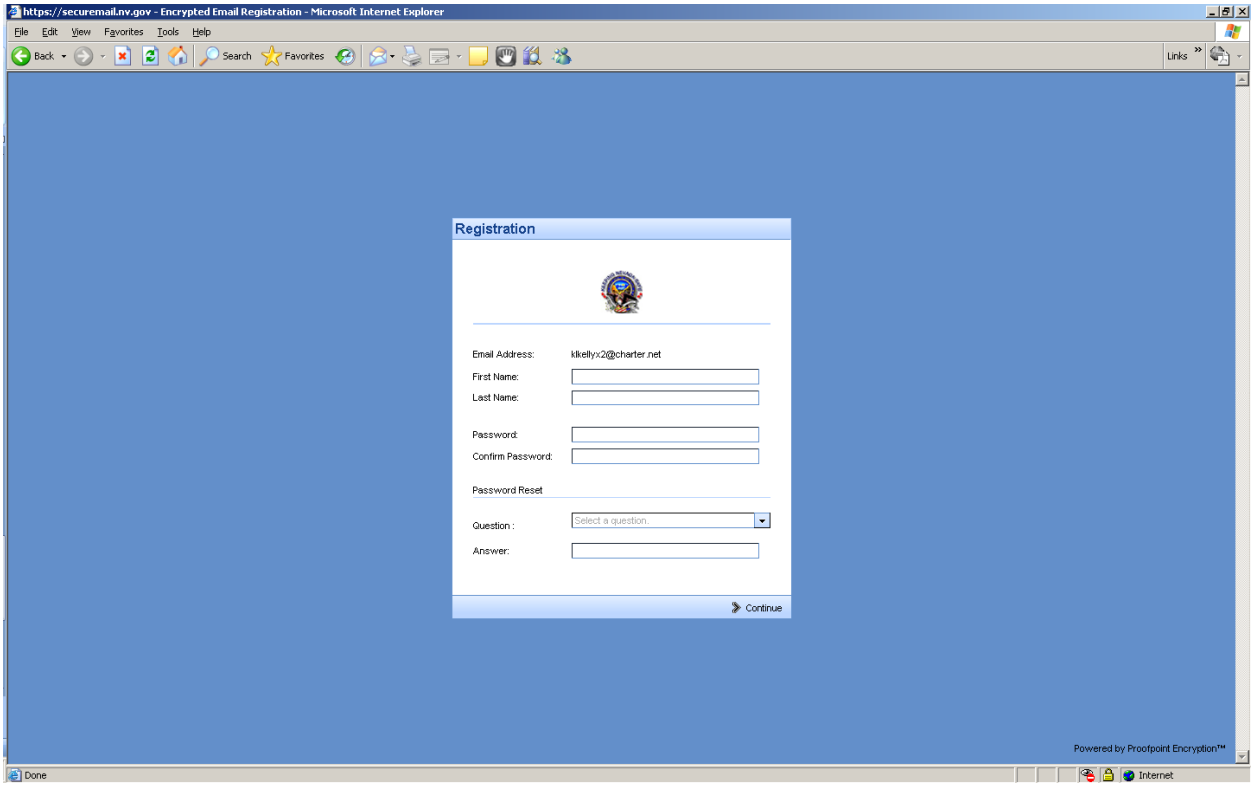
The secure e-mail recipient must click on the Secure Message Attachment button. After clicking on the Secure Message Attachment button, click on the Download button as illustrated below:



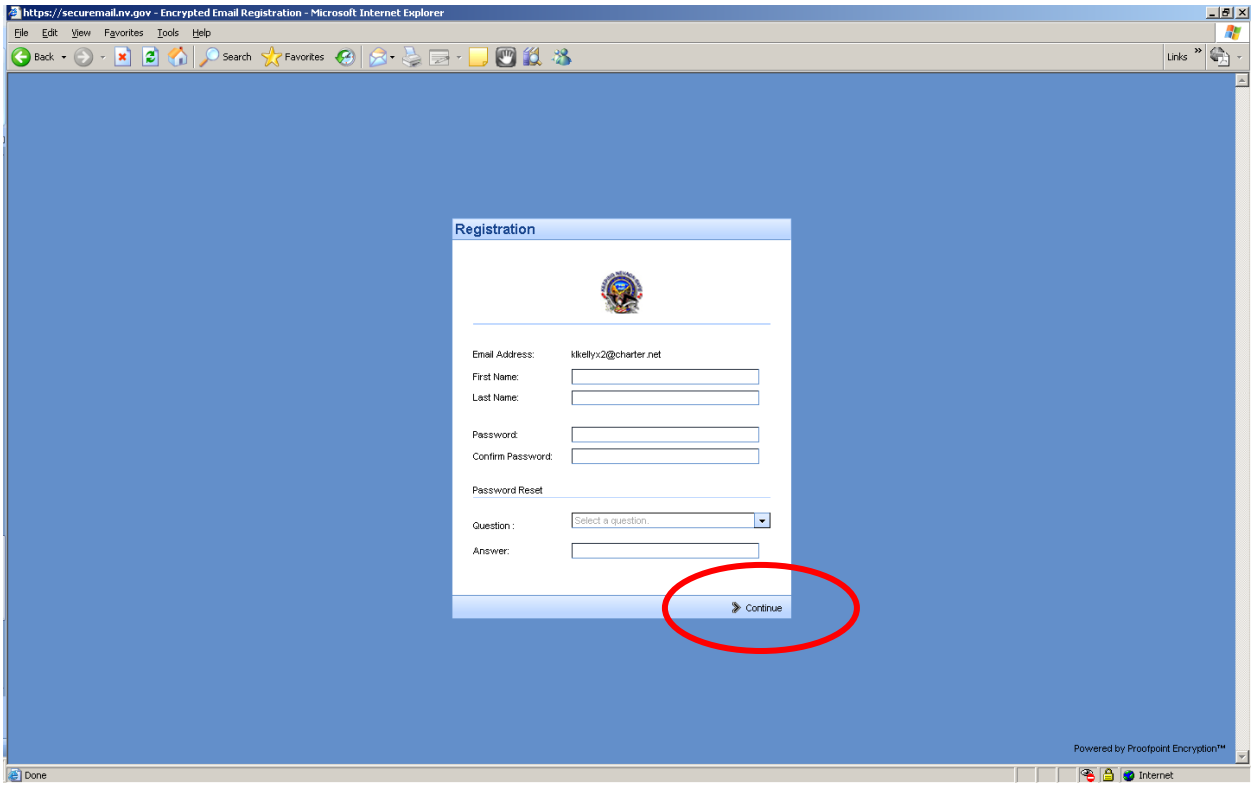
After clicking the download button you may be asked, “Do you want to open or save this file?” Click Open. Click the, Click to read message button as shown below:



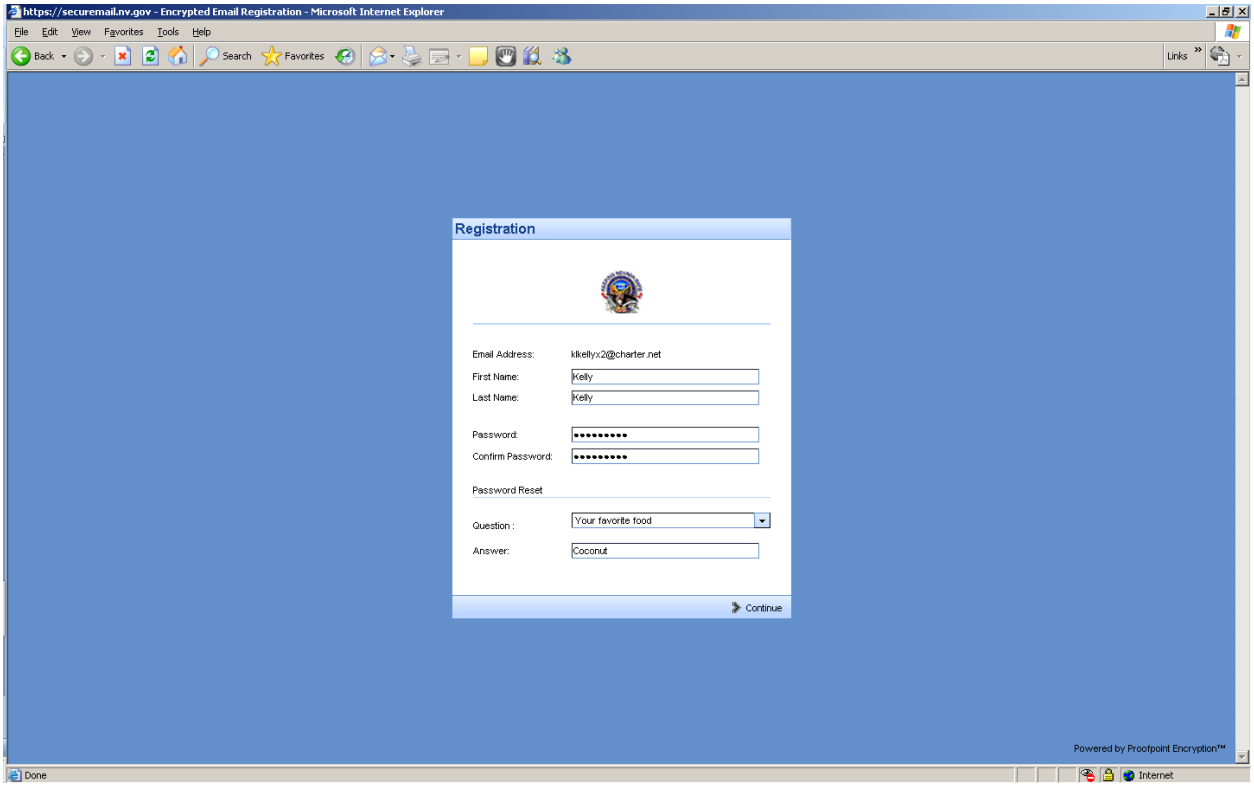
The first time a secure e-mail recipient attempts to read a secure e-mail they will need to complete the one time registration information.



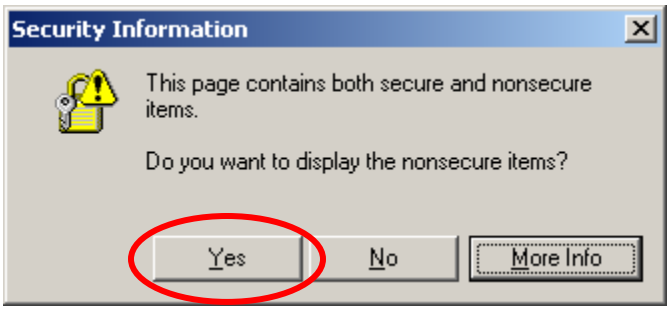
When you click in the Password field you will see the password policy requirements to assist you in creating a sufficiently complex password. The password must be 8-36 characters long, have at least one digit (0-9), have at least one symbol character and uppercase and lowercase characters are required.



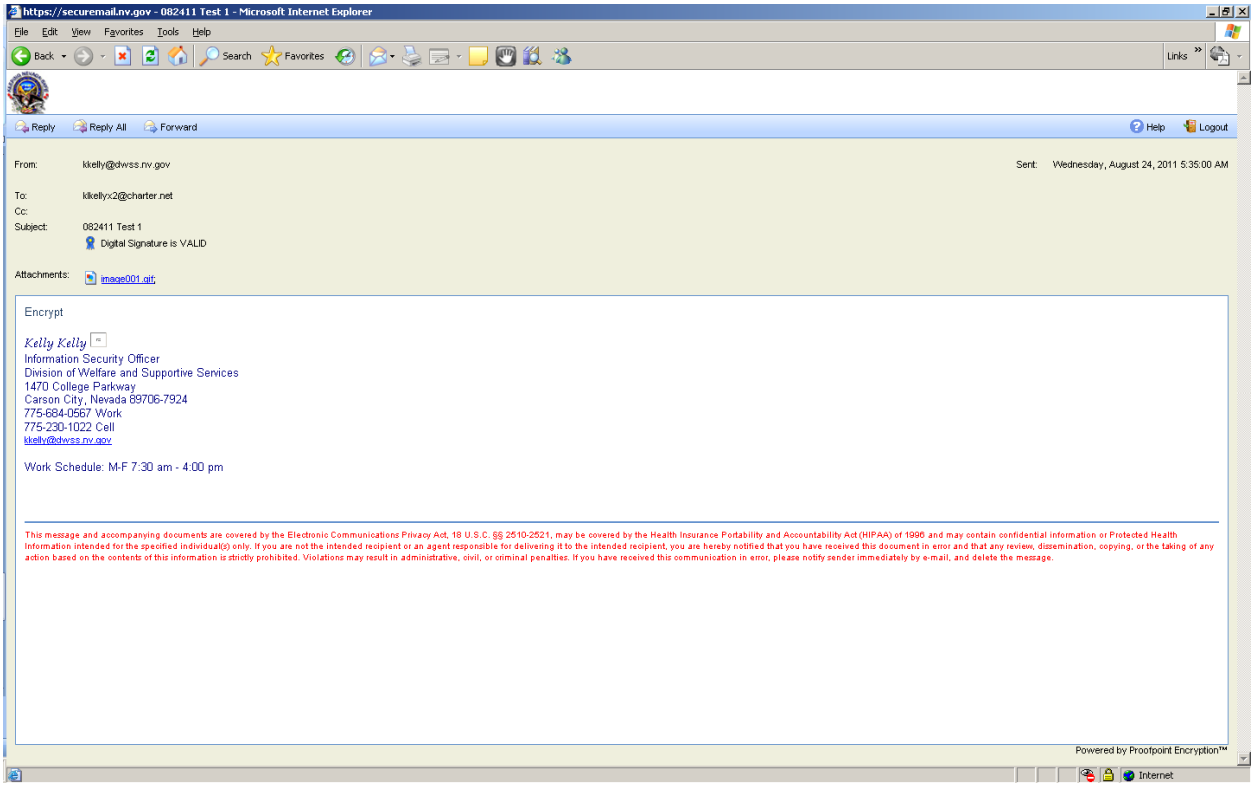
To complete the registration process, enter the password, confirm the password, select the Password Reset Question from the dropdown, answer the question you selected then click on the > Continue button at the bottom right corner of the registration page.



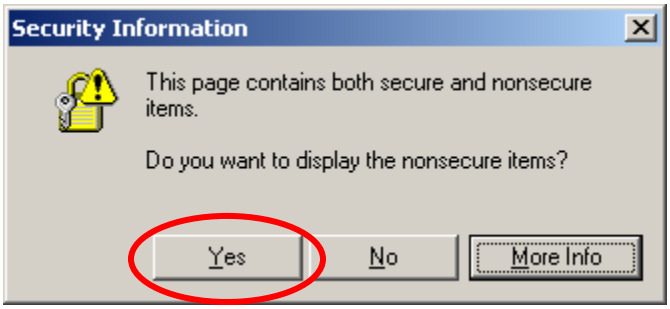
If you receive the following Security Information popup, click **Yes** to continue:

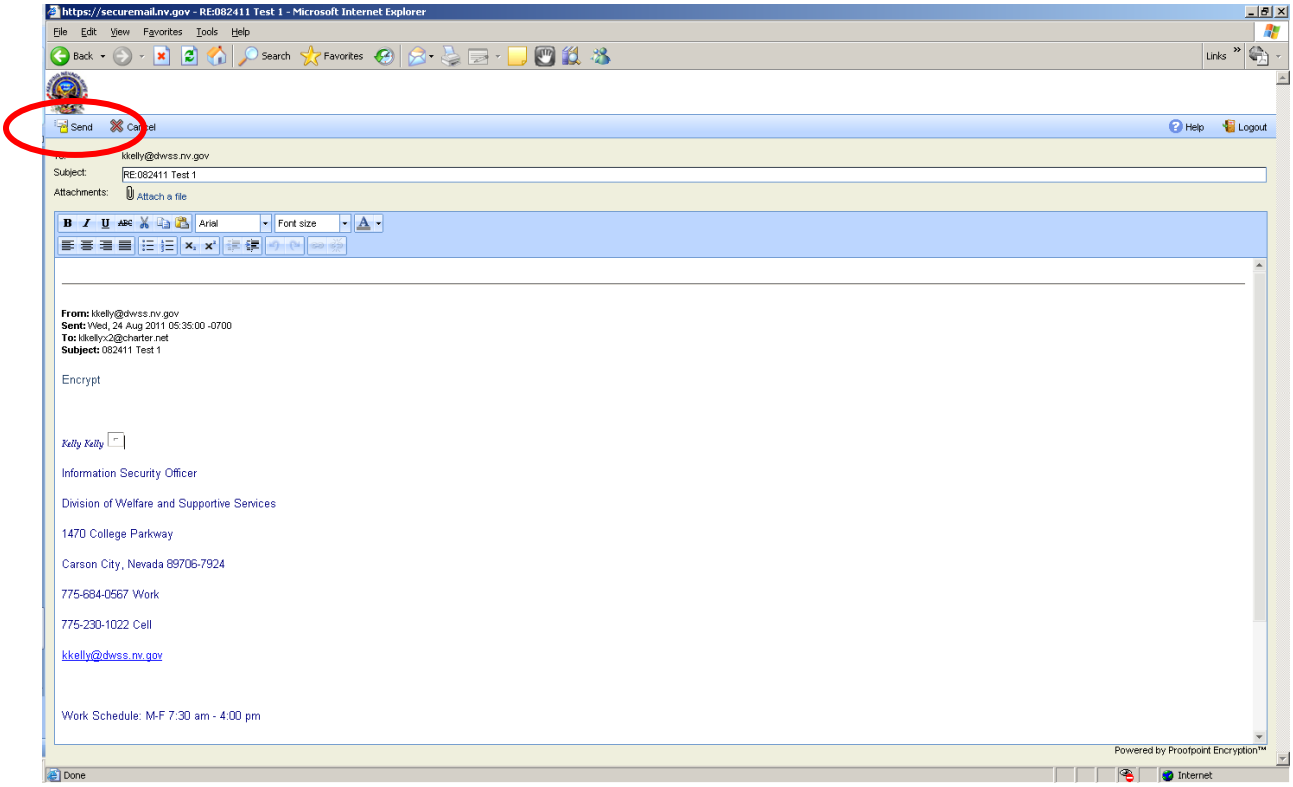


The secure e-mail message recipient will then be presented with the decrypted message:

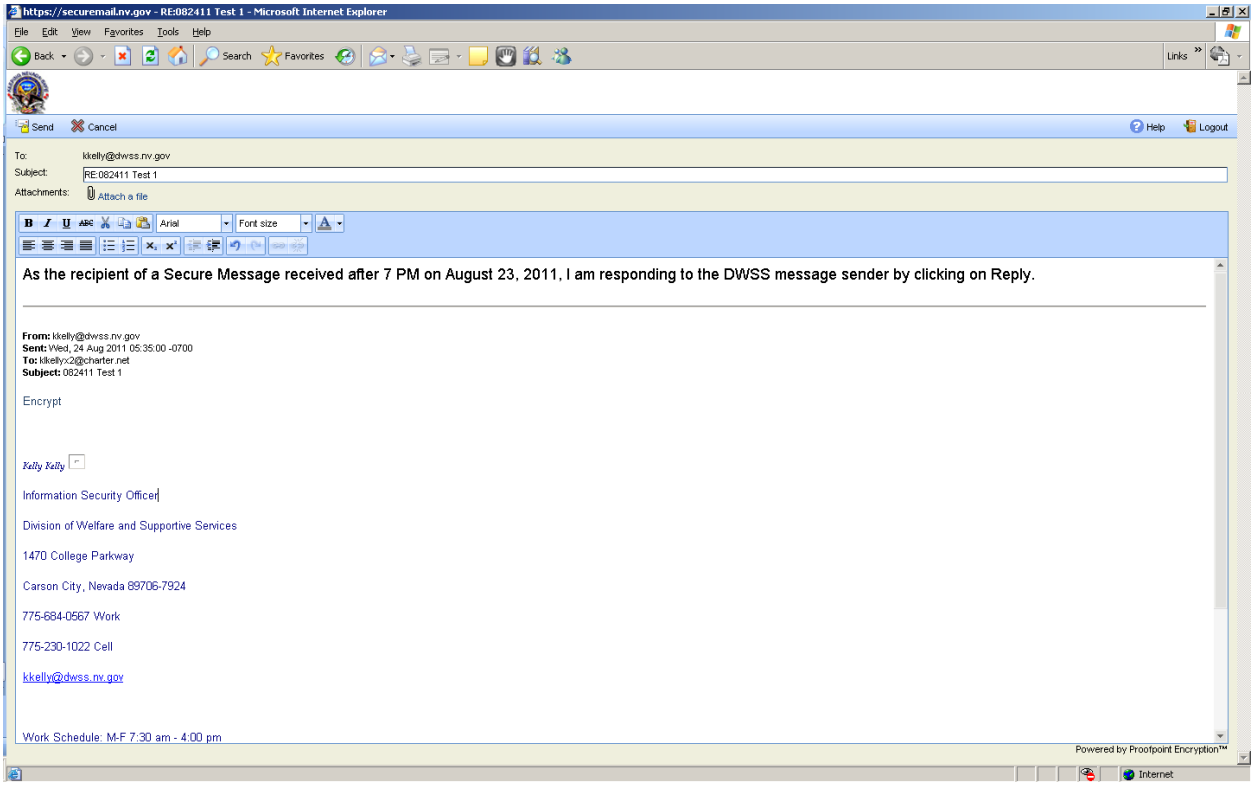


To Reply, Reply All, or Forward the message, click the appropriate corresponding button at the top left corner of the message. If you receive the following Security Information popup, click **Yes** to continue:

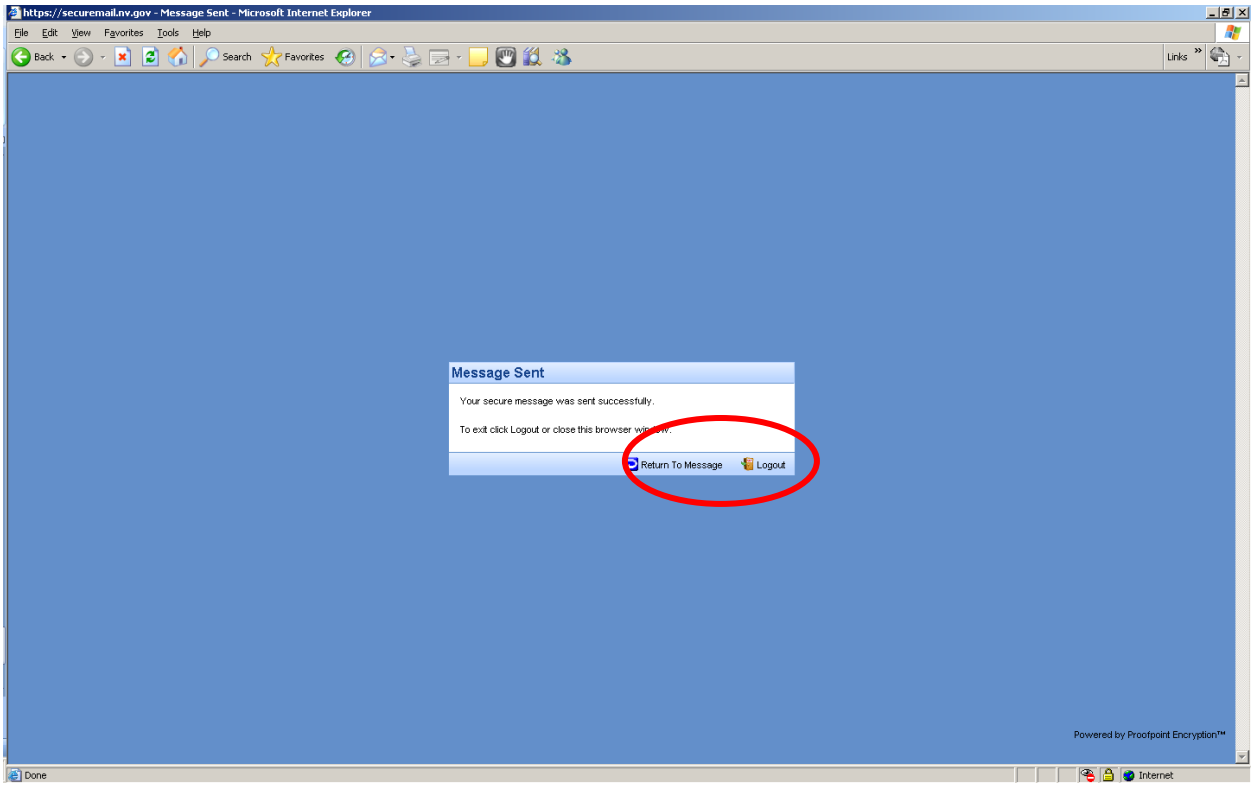




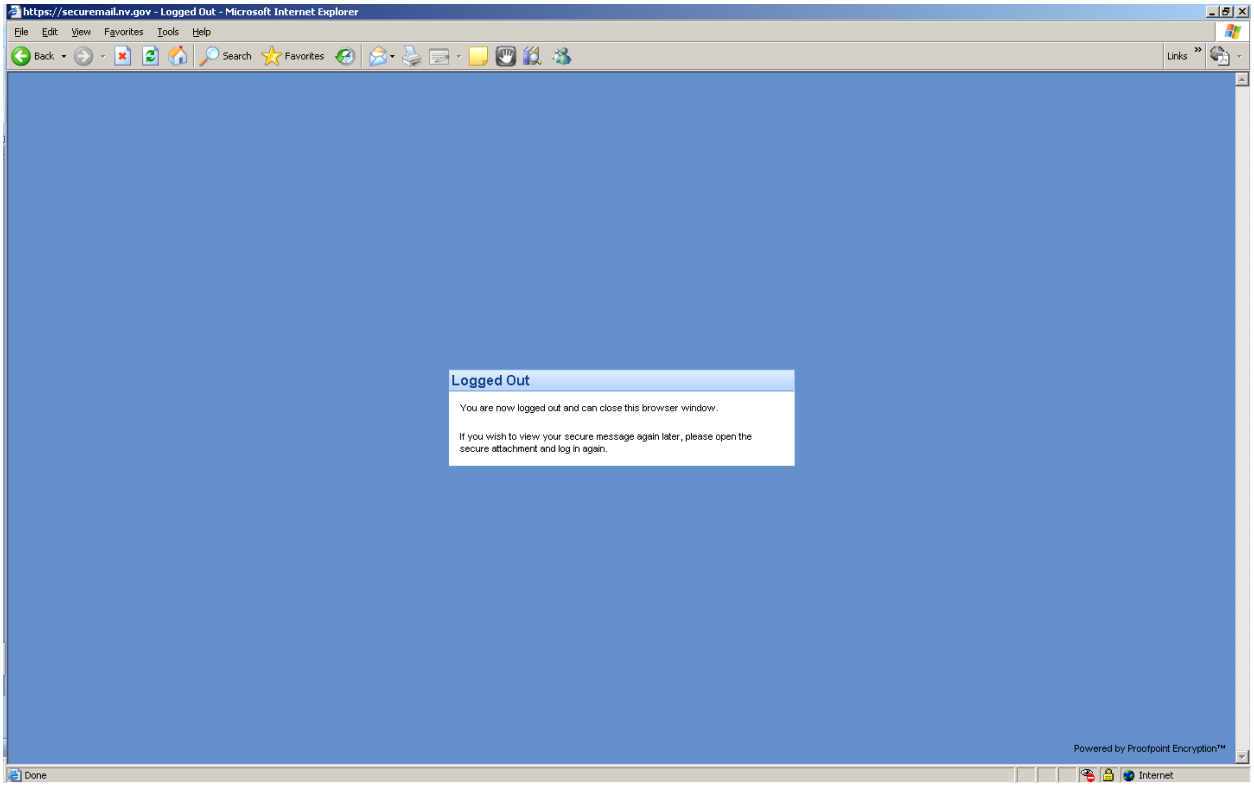
Example using the Reply feature:



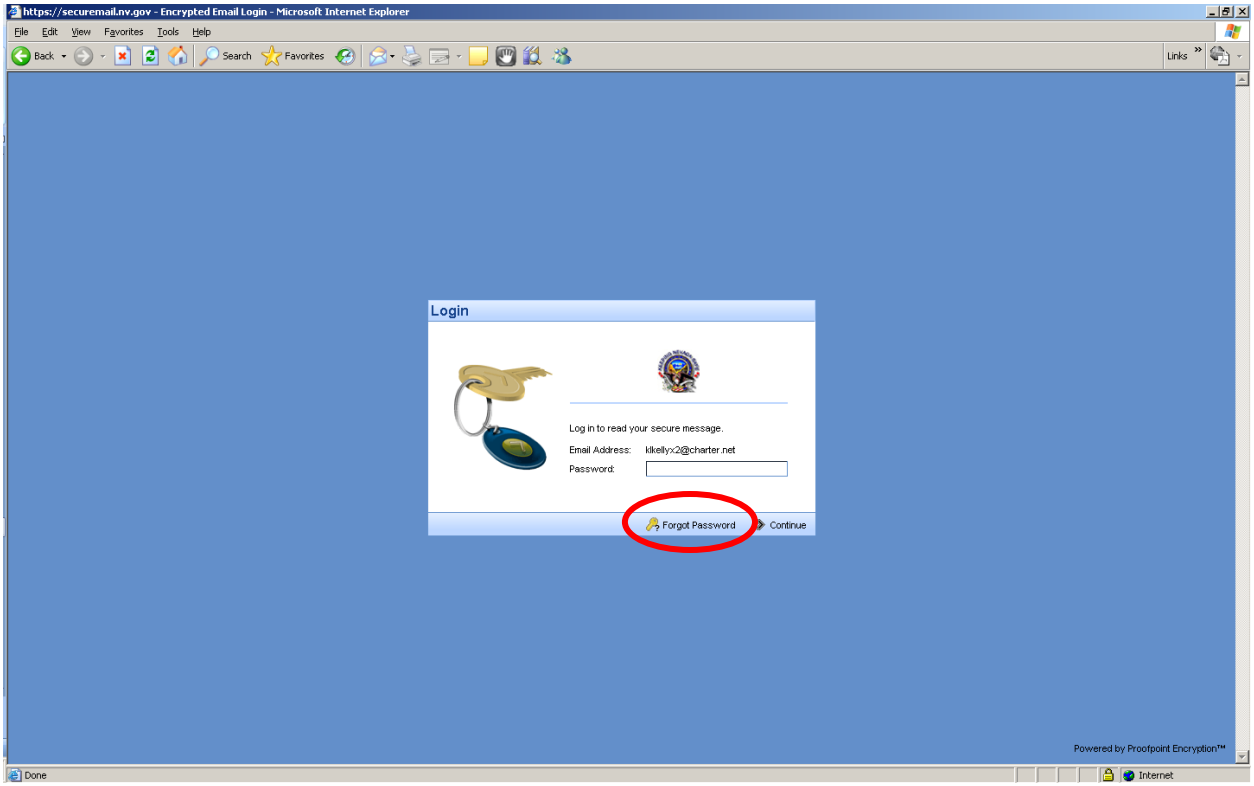
When you are ready to send your Reply, Reply All, or Forward, click the Send button at the top left corner. You will also have the option to cancel. Once you have clicked the Send button you will see Message Sent:



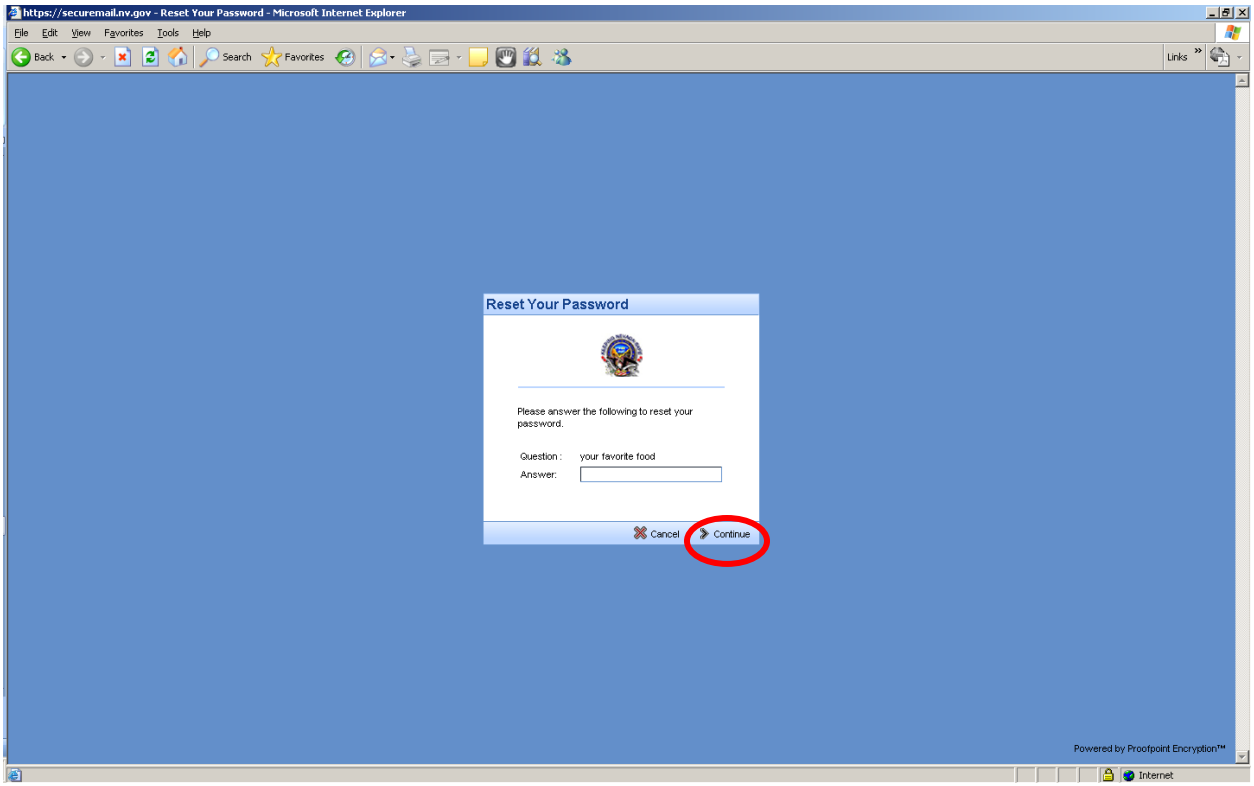
From the Message Sent page you have an option to Return to Message or Logout. To Logout, click on the Logout button on the lower right corner which will display the following message:



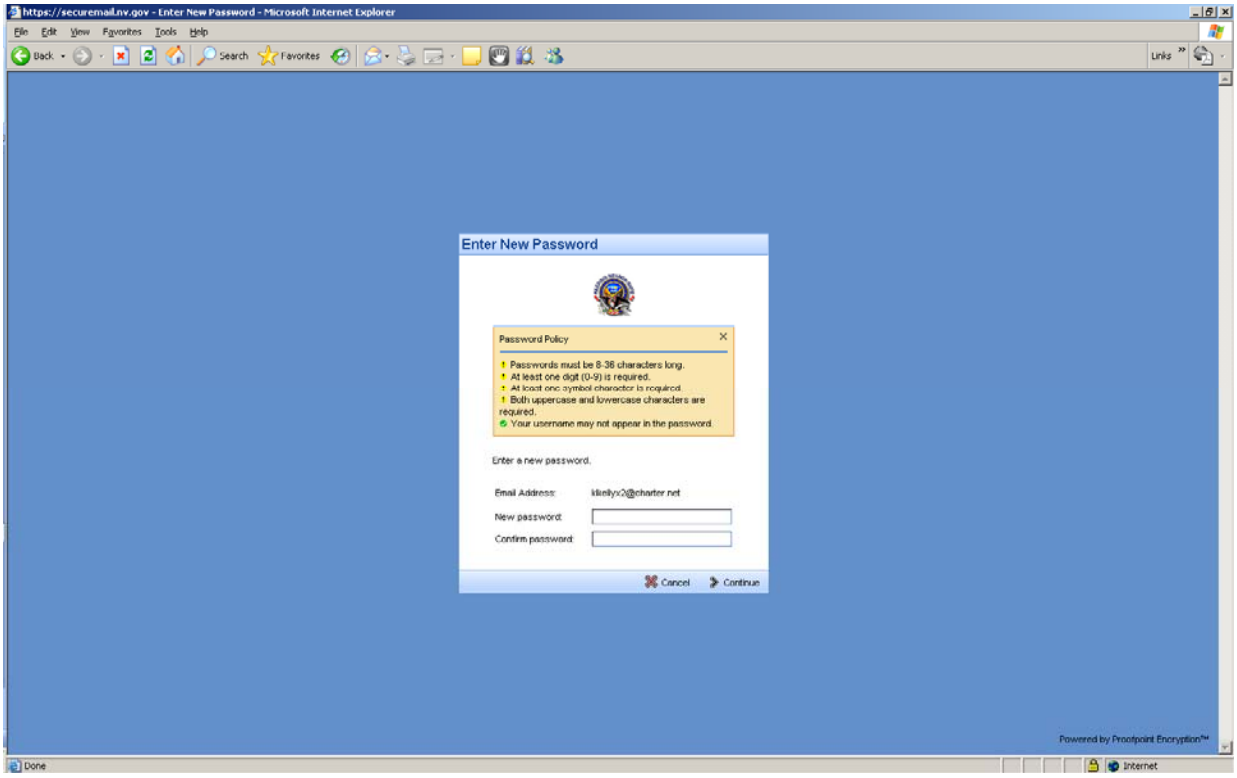
You are now logged out and can close this browser window. If you wish to view your secure message again later, open the secure attachment and log in again.



If you cannot remember your password, click on the Forgot Password button on the bottom portion of the Login page to Reset Your Password. Answer the passphrase question you established when initially creating your account and click > Continue.



Create a new password conforming to the password policy requirements, confirm your new password and click > Continue.



The secure e-mail message can now be read by the recipient.

Who do I contact if I have a problem with a secure e-mail received from a DWSS e-mail user? If you need assistance, please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

The secure e-mail help tool has valuable information and can be used at any point by clicking on HELP. The following information was copied directly from the new secure e-mail help tool to provide additional information. For purpose of this secure e-mail communications plan, where the help tool references contacting the e-mail administrator has been replaced with: "Please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700."

Receiving Encrypted Email

You have received a secure, encrypted message from the sender. Click the attachment in the message to launch a browser to authenticate so that you can decrypt and read the message.

Note: If you see red X icons in the browser, your email client is blocking images. These images are typically the logo or images of the sender's organization. You can display the images or ignore them without affecting your ability to read the message.

- If you have not registered for Proofpoint Encryption, you will be prompted to create an account and choose a password on the **Registration** page. Click **Continue** when you are done. In the future, you will not be prompted to register.

- If you have already registered, or if your account already exits, you will be prompted to sign in and provide your password to decrypt the message. Click **Continue**.

- If you sign in, and the Login screen returns with a field that you can edit for your user name, it means Proofpoint Encryption found a record for you, but the email address is different - perhaps an email alias. Enter a different address to sign in. For example, a record for jsmith@example.com exists, but you entered joe@example.com - your alias for jsmith.

Forgot your password?
If Proofpoint Encryption is configured to allow you to reset your password, click the Forgot Password link. You will be prompted for your security question. Create a new password for your account.

Locked out?
If you try to enter an incorrect password several times, you may be locked out of Proofpoint Encryption. If this happens, please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

Replying or Forwarding
Your ability to reply to or forward an encrypted message depends upon the sending organization's policies. If you do not see a **Reply**, **Reply All**, or **Forward link**, it is because the sender of the message cannot allow recipients to reply to or forward the message. When you reply to a message, your reply will be sent securely.

Adding Recipients
The ability to add or edit the recipient list when you reply to a message depends upon the sending organization's policies. The To and CC recipient fields will either be fixed so that you cannot change them, or you will be allowed to add or delete recipients from these fields. Separate multiple recipients with a comma.

When you forward a message, you can always edit the recipient list.

Note: The sender's organization has the option to restrict secure messages to specific domains. If this is the case, you will see an error message if you try to forward a secure message to a recipient that is not allowed to receive it.

Send Me a Copy

Proofpoint Encryption does not automatically place a copy of a secure message in your Sent folder. Click Send me a copy when you forward or reply to a secure message so that a copy will be sent to your address for your records.

Adding an Attachment to Encrypted Email
If you want to add an attachment to a message, click the Attach a file link. Navigate to the file you want to attach and then click the Add link. The name of the attached file displays in the dialog box. Click Upload when you are done adding attachments.

To delete an attachment from a message, click the X link to the right of the attachment.

Note: The (combined) attachments cannot exceed 15 MB in size.

Reading a Secure Message on a Smart Phone
Some Smart Phones cannot download files, and some Smart Phones modify HTML files. Since your secure message is sent to you as an HTML attachment, you may not be able to read it on your Smart Phone. If you have trouble reading your secure message, follow the instructions to forward the message to another server. You will then be able to download the message from the server to read it.

Troubleshooting
This section describes error messages and what they mean.

- **You authenticated successfully, but do not have permission to decrypt this message.** You do not have permission to decrypt this message. Or, the administrator has disabled your ability to decrypt the message. Please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

- **You authenticated successfully, but the decryption key for your message has been deleted.** The decryption key for this message has expired or has been deleted. Please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

- **There was a critical error processing your request. There may be a problem with the system or your request.** Proofpoint Encryption is temporarily unavailable. If this situation persists, please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

- **The message you are trying to read is corrupted and cannot be processed. Please contact the sender of the message.** The message is corrupted and cannot be decrypted. Contact the sender of the message.

- **The page you requested was not found. If you clicked a link to get here, click**

the Back button in your browser to return to the previous page.
The page you are trying to view in the browser is not available or does not exist. Click the Back button in your browser.

- **The username you requested has already been registered.**
  You have already authenticated with Proofpoint Encryption.

- **There was an error retrieving the key for your message. If this error persists, please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.** The key server is temporarily unavailable. Try again later, and if you still cannot decrypt the message, contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

- **Your account has been disabled.**
  Your email administrator has disabled your account.

Other Issues

Error with Large HTML Secure Messages:
If your HTML message contains more than 500 KB of content, you may encounter a "Large Message Warning" error message. This limitation applies to Firefox 3.X or Internet Explorer browsers when you reply to the message or forward it. This limitation does not apply to plain text.

Intermittent Problem with Replying to or Forwarding Secure Messages:
If Proofpoint Encryption hangs when you try to compose a message and click the Reply, Reply All, or Forward links, click Cancel and try again. If the original text of the secure message does not display in the browser, refresh the browser or close the browser and open it again. The behavior is infrequent, intermittent, and typically works the second time around.

If you use Outlook Web Access on Windows Vista:
Do not save the SecureMessageAtt.htm attachment to disk and then try to open it. Open it from the email message.