PGP TrustCenter
## A DIVISION OF PGP CORPORATION

Outlook Express

Using PGP TrustCenter Digital Certificates with Microsoft Outlook Express v6

To use any of the security features in Outlook Express, you must first configure the program to use your digital ID (certificate). If you do not already have a digital certificate, please visit PGP TrustCenter's website at http://www.pgptrustcenter.com/digital-certificate-solutions to obtain a "TC Personal ID" or "TC Business ID".
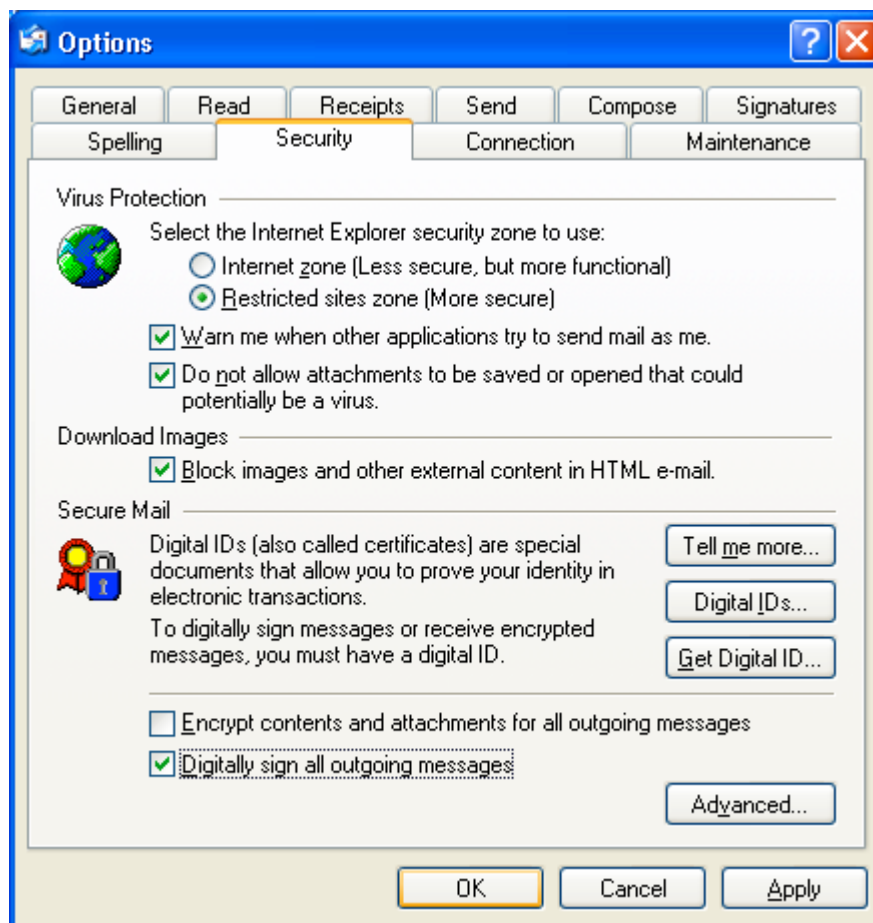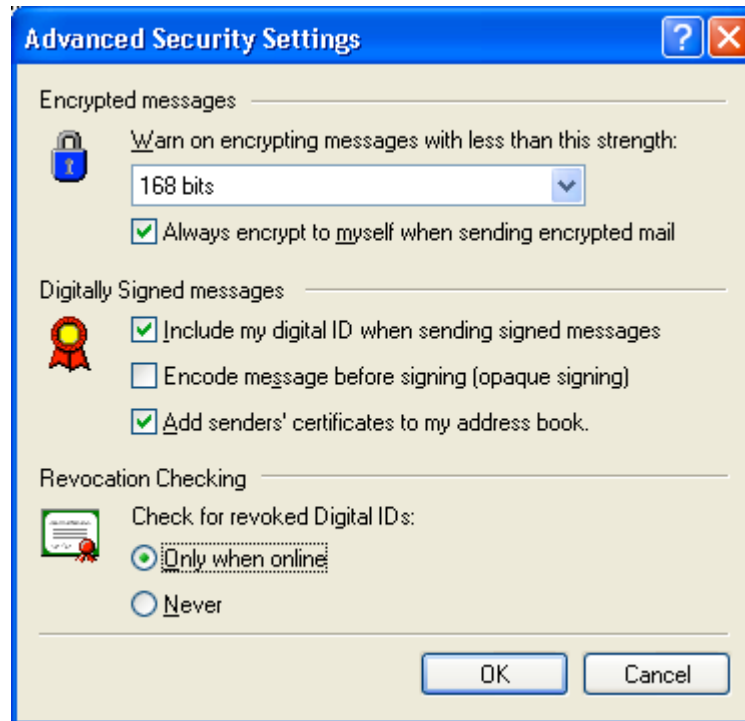
Configuring Outlook Express

After you have your private key (digital ID) installed, you need to configure Outlook Express to use the certificate by following these steps:

1. On the Tools menu, click Accounts.
2. Click the Mail tab, click the mail account in which you want to use a digital ID, and then click Properties.
3. On the Security tab, click Select under the Signing Certificate section.
4. Click the appropriate certificate and click OK.
5. To allow for your encryption details to be included when signing emails, click Select under the Encrypting Preferences and choose the appropriate certificate. Click OK.
6. Click OK to then Close.
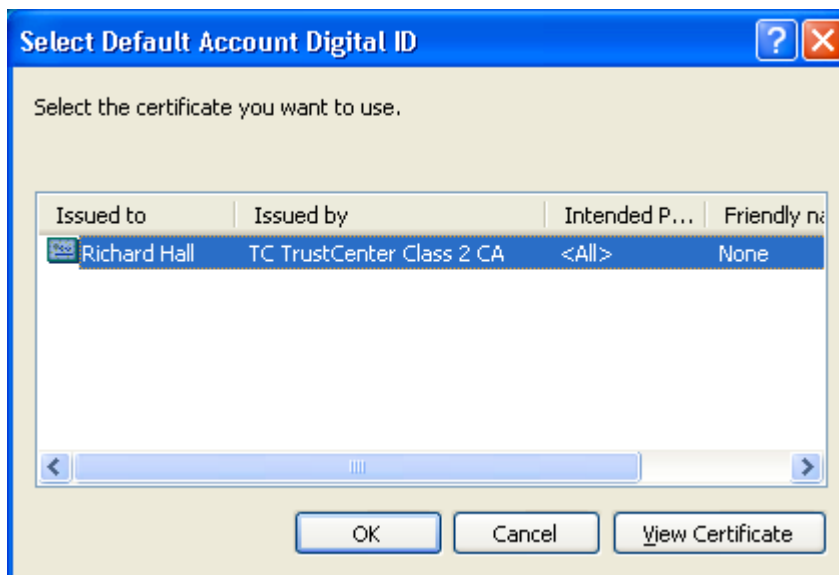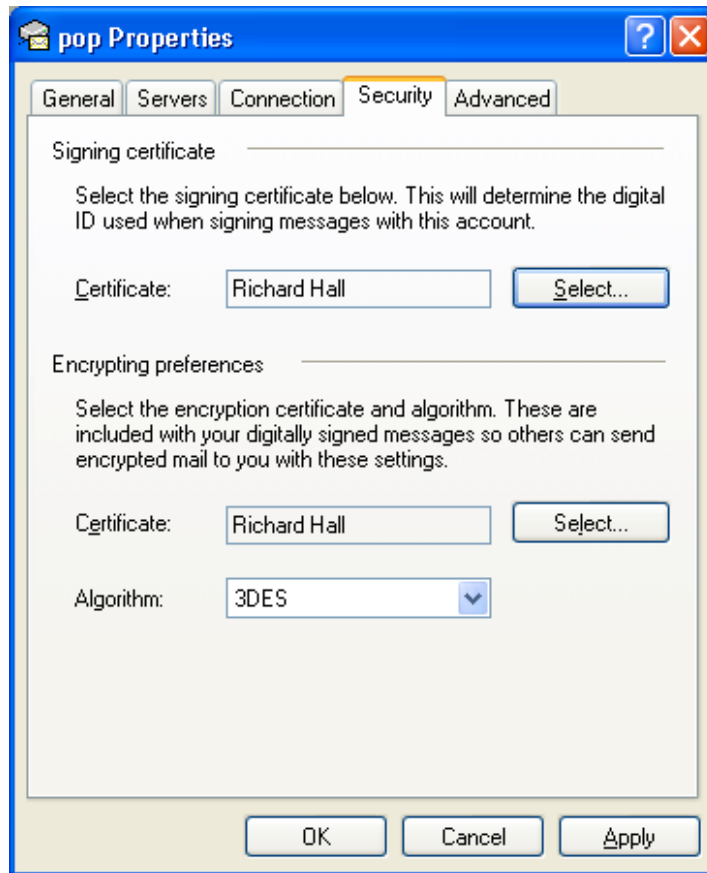
7. On the Tools menu, click Options.
8. On the Security tab, click Advanced Settings.
9. Click the option to "Include my digital ID when sending signed messages". This allows the recipients of your messages to easily verify your message with your public key.
10. To automatically save all recipients' certificates, click the "Add senders' certificates to my address book". This allows for the use of these certificates to be used for encrypted emails.
11. Under Revocation Checking, click the "Only when online" option to check for revoked IDs.
12. Click OK.
13. If you want to automatically digitally sign all outgoing messages, click the "Digitally sign all outgoing messages" check box to select it.
14. If you want to automatically encrypt all outgoing messages, click the "Encrypt contents and attachments for all outgoing messages" check box to select it.
15. Click OK.

Advanced Security Settings

Encrypted messages

Warn on encrypting messages with less than this strength:

168 bits

☑ Always encrypt to myself when sending encrypted mail

Digitally Signed messages

☑ Include my digital ID when sending signed messages

☐ Encode message before signing (opaque signing)

☑ Add senders' certificates to my address book.

Revocation Checking

Check for revoked Digital IDs:

◉ Only when online

○ Never

OK   Cancel

Options

General | Read | Receipts | Send | Compose | Signatures

Spelling | Security | Connection | Maintenance

Virus Protection

Select the Internet Explorer security zone to use:

○ Internet zone (Less secure, but more functional)

◉ Restricted sites zone (More secure)

☑ Warn me when other applications try to send mail as me.

☑ Do not allow attachments to be saved or opened that could potentially be a virus.

Download Images

☑ Block images and other external content in HTML e-mail.

Secure Mail

Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.

To digitally sign messages or receive encrypted messages, you must have a digital ID.

Tell me more...

Digital IDs...

Get Digital ID...

☐ Encrypt contents and attachments for all outgoing messages

☑ Digitally sign all outgoing messages

Advanced...

OK   Cancel   Apply

Digitally Signing a Message

To digitally sign a message, you can use either of the following methods:

- Have Outlook Express automatically sign all messages each time you compose, reply to, or forward a message (see step 12 in the section titled "Configuring Outlook Express").
- Click the Digitally Sign Message button. This button displays an envelope with a red ribbon. You can also click Digitally Sign on the Tools menu.

When a message is digitally signed, a red ribbon appears to the right of the "To:" line. When you click send, Outlook Express signs the message using your private key and sends the message.
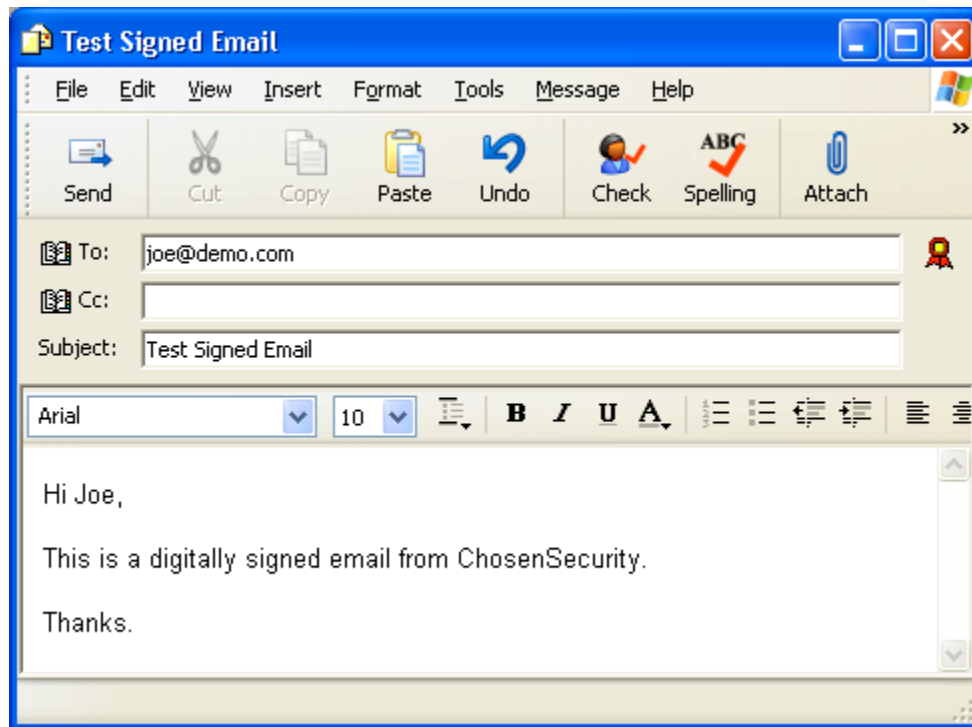
If you do not have your private key installed on your computer, Outlook Express displays the following message:

The message could not be sent.
You cannot send digitally signed messages because you do not have any certificates. (OK)

The recipient must have your public key to verify that the digital signature on your message is trustworthy. Others cannot use your public key to send messages with your digital signature.

You can include your public key with the message (see step 9 in the section titled "Configuring Outlook Express") or you can send your certificate files as an attachment. If the recipient's e-mail client is not S/MIME aware, the public key certificate appears as a file attachment with a .p7s extension. If the e-mail client is S/MIME aware, there is no visible enclosure.

Verifying a Digitally Signed Message

The recipient must have your public key to verify that the digital signature on your message is trustworthy. This will not be an issue if you have included the certificate with your message as was instructed in step 9 in the section entitled "Configuring Outlook Express". Digital Signatures are done with your private keys, and therefore others cannot use your public key to send messages with your digital signature.
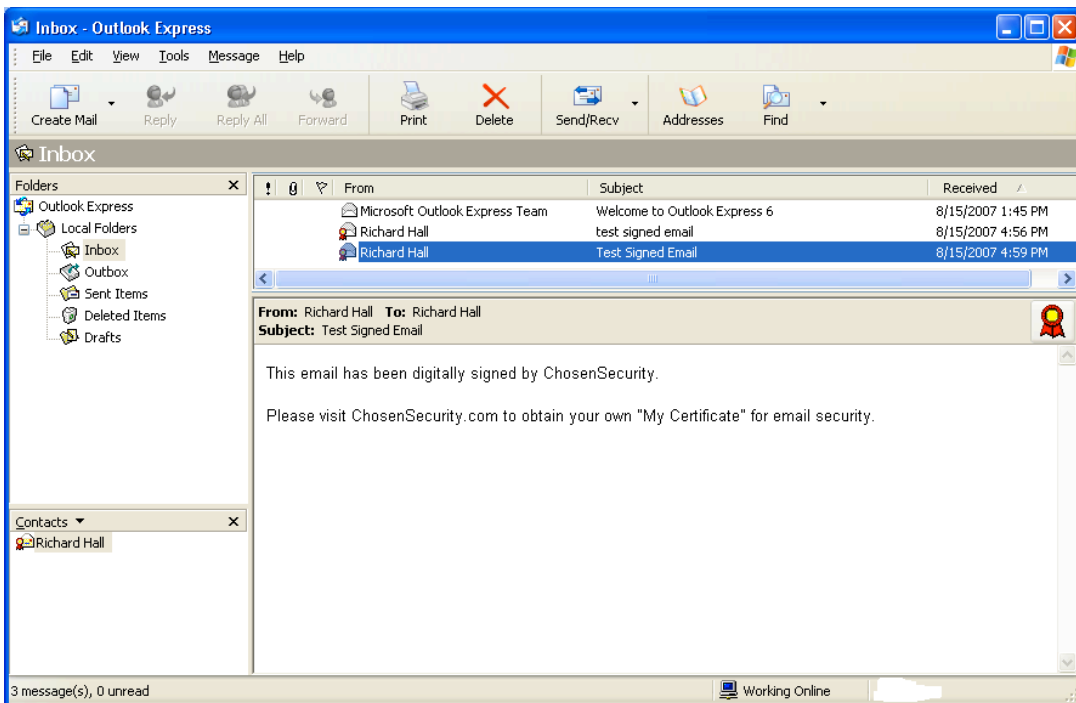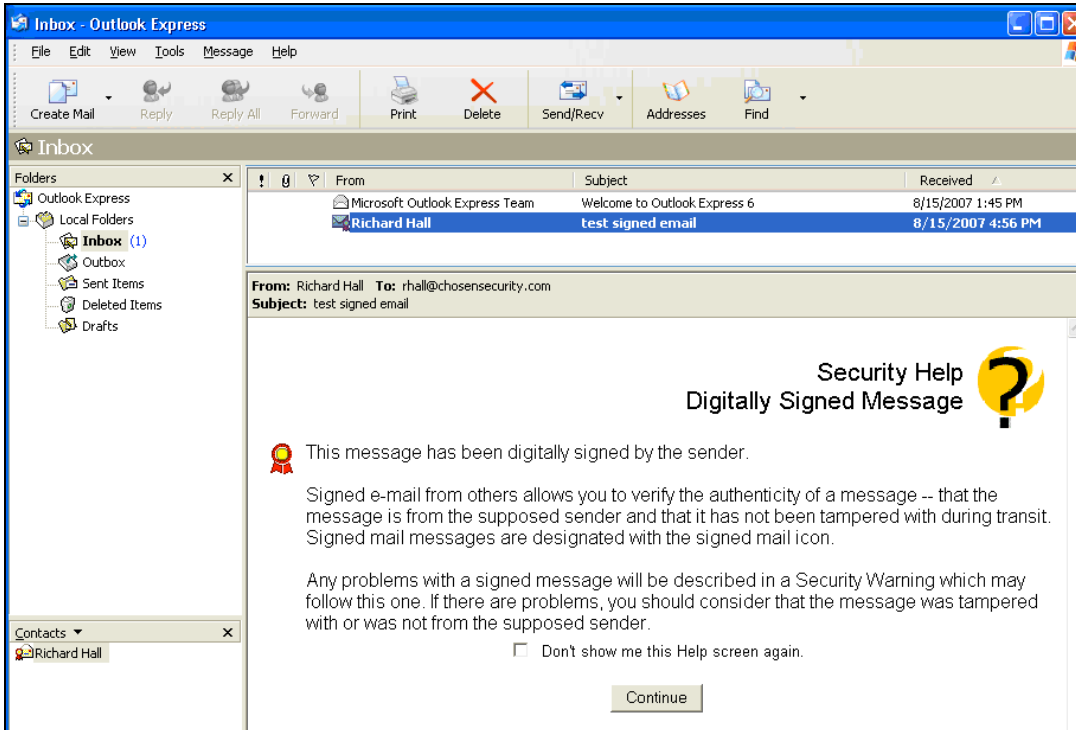
Adding a Certificate to the Address Book

To be able to verify a sender's digital signature or to send encrypted mail, you must obtain the other person's certificate (public key) and import it into your address book.

There are two ways to obtain a public key:

- Look up the other person's public key by visiting PGP TrustCenter's Web site, searching for the correct person under the Certificate Services section within the Resource Center, and installing the certificate.
- You receive a digitally signed message that includes the sender's certificate (public key).

To automatically add all recipient's certificates to your address book from a signed message you receive (method 2), see step 10 under "Configuring Outlook Express".

To manually add a person's certificate to your address book from a signed message you receive (method 2), follow these steps:

1. Click the message to select it.
2. On the File menu, click Properties, and then click the Security tab.
3. Click "View Certificates"
4. Click "Add to Address Book."
5. Click OK, and then OK again.

Encrypting a Message

To encrypt a message so that only the recipient can decrypt the message, you need the recipient's certificate (public key) in your address book. See the section titled "Adding a Certificate to the Address Book" for information on how to do this.

One way to encrypt a message is to have Outlook Express automatically encrypt all messages each time you compose, reply to, or forward a message (see step 14 in the section titled "Configuring Outlook Express").

Another way is to click the Encrypt Message button on the toolbar. This button displays an envelope with a blue padlock icon to the right of the email. You can also click Encrypt on the Tools menu.
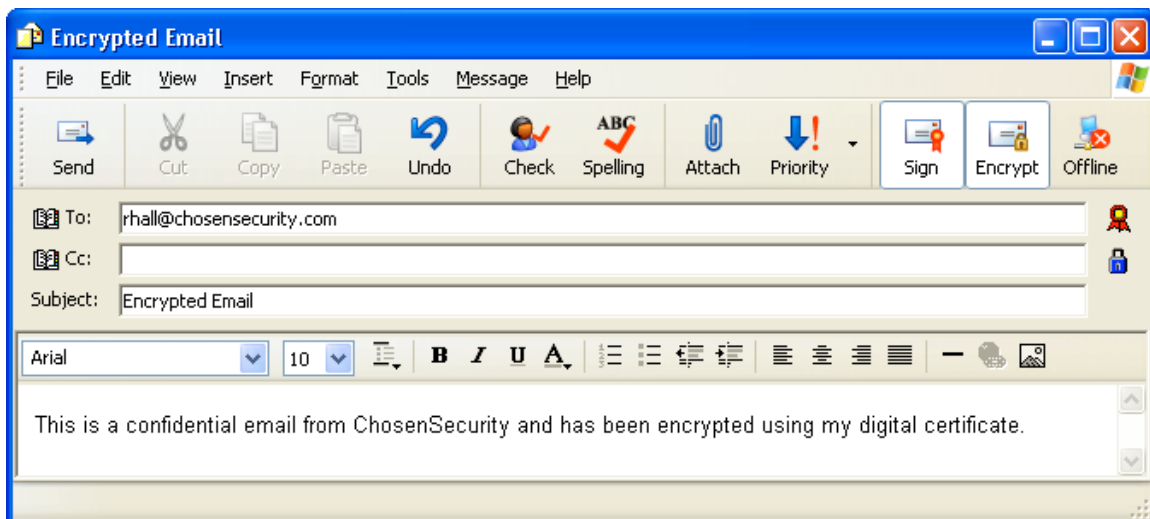
When you click send, Outlook Express encrypts the message using a secret key, encrypts that key with the recipient's public key, and sends the message.

Receiving Encrypted Email

When an encrypted is received, a padlock icon appears on the email.
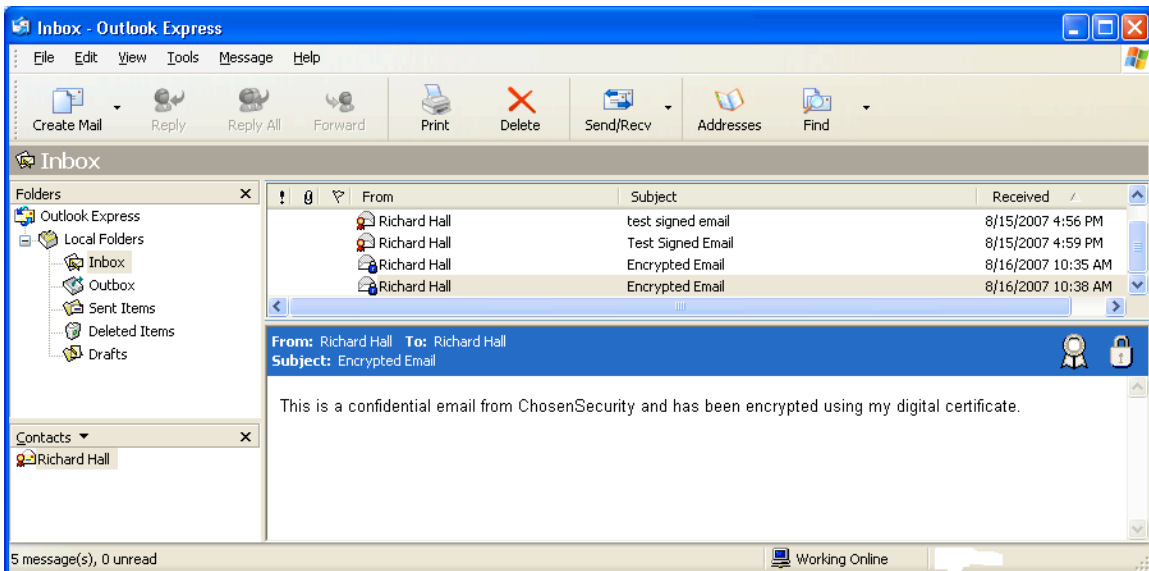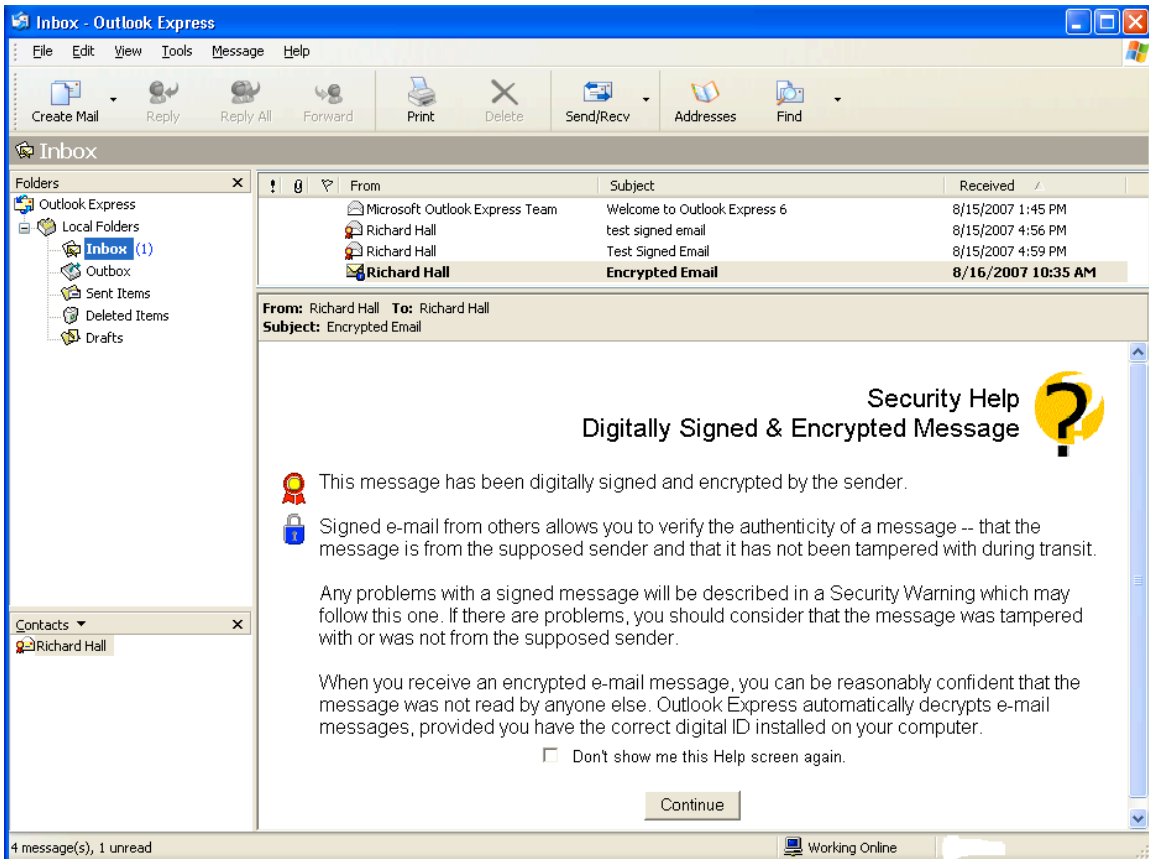
Errors Received When Sending Encrypted Emails

If you send an encrypted email and you do not have the public key for one or many of the recipients (including yourself, the sender), Outlook Express displays the following security warning message:

Outlook Express was unable to locate the digital IDs of the following recipients:

<list of recipients>

You can choose to send this message without encrypting it, or you can cancel sending this message.