Chapter 15

Keeping Secrets Safe with Outlook Security

In This Chapter

- ▶ Obtaining a digital ID
- ▶ Sending a signed message
- ▶ Encoding a message

In the movies, computer hackers know everything — your credit card balance, Social Security number, and what you ate for breakfast. There doesn't seem to be a single scrap of personal information that a computer hacker in a movie can't find out.

Are real-life computer hackers just as brilliant and dangerous? Not really. Most crimes involving theft of personal information don't come from hackers sneaking into personal computers. More often than not, these losers dig credit-card slips out of a restaurant dumpster, or they just make a phone call and trick some poor slob into revealing a password.

Even though there isn't some hacker out there who knows what you bought at the Piggly Wiggly (or cares, for that matter), it may be wise to think about security when it comes to your e-mail and personal information. If you work in a corporation, you may be required by law to maintain certain standards of security over the messages you send and receive.

Outlook includes a feature called a Digital ID that enables you to keep your secrets secret, to keep your identity secure, and to be sure that the messages you receive actually came from the people who seem to have sent them. In most cases, you'll need to add some small program to Outlook to enable these advanced security features, but after you've installed these features, you never have to fuss with them again.

If security is a really big deal to you (as it is to people in the finance, law-enforcement, and defense industries), you may want to look into the more sophisticated security systems that are starting to turn up. Several high-tech companies offer systems for confirming identity and ensuring message security using fingerprint readers, eye scanners, and even gizmos that can recognize your face. Although many such systems can hook right into Outlook to make short work of message security, most of them cost quite a bit more than the average person needs to spend.

Getting a Digital ID

You probably receive messages every day from people you've never met. And I'll bet you don't spend much time wondering whether the messages you receive actually come from the people they seem to be — but you might need to think about that from time to time. After all, sneaky hackers can send out e-mail messages that appear to come from someone else. So how can you tell whether the message actually came from the person who appears to have sent it? Of course, if you know the senders personally, you can simply phone them to verify that what you received is what they sent. But a quicker, high-tech approach is to use what's called a *digital signature* — a tiny piece of secret code mixed in with your message to prove three things:

- That the message really comes from the person who seems to have sent it.
- That the person who seems to have sent the message really is the person he claims to be.
- That the person who sent the message sent it intentionally. It's like putting your signature on a check; it shows that you really mean to send a specific message.

If you want to take advantage of Outlook's security features, the first step to take is to get yourself a digital ID. If you work in a large organization, your employer may have obtained that for you — and your local computer gurus may have installed all the software — in which case, you can skip these steps. If you want to get a digital ID for your own use, you can get one from one of the many companies that issue and maintain digital ID services by following these steps:

1. **Click the File tab in the Ribbon.**

   The Backstage view appears.

2. **Click the word *Options.***

   The Outlook Options screen appears.

3. **Click the words *Trust Center*.**

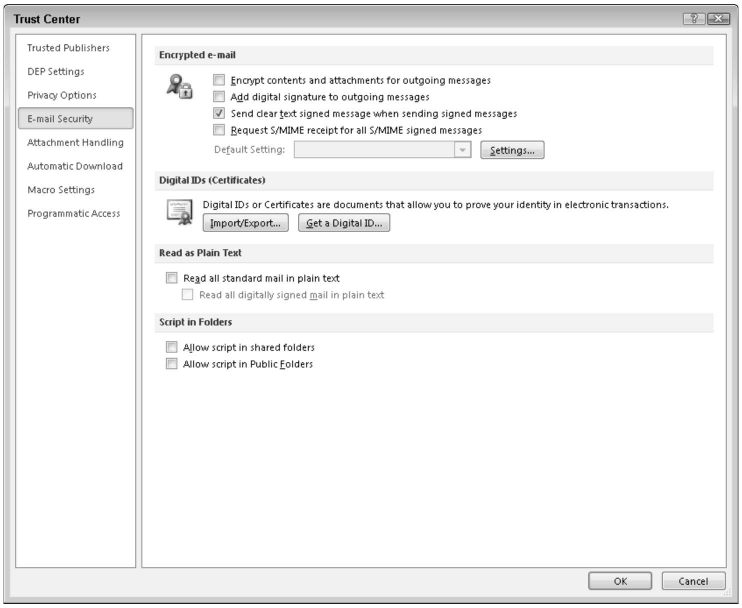
   The Outlook Options screen appears.

4. **Click the Trust Center Settings button.**

   The Trust Center screen appears.

5. **Click the E-Mail Security button.**

   The E-Mail Security page appears (as shown in Figure 15-1).



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

Figure 15-1: The E-Mail Security page is where you can start looking for your digital ID.

6. **Click the Get a Digital ID button.**

   A Web site opens, offering a range of choices for obtaining a digital ID.

Quite a few companies offer digital IDs — some for free, but most of them charge a small fee. The range of companies that offer this service varies over time; your best bet is to check the Web sites to see which you prefer. The two best-known vendors of Digital IDs are Thawte (`www.thawte.com`) and VeriSign (`www.verisign.com`). After you pick a provider for your digital ID, you fill out a number of forms and pick a password for the ID. You'll also need to exchange several e-mails with a provider of the digital ID; that's how you prove that your e-mail address is really yours.

Sending Digitally Signed Messages

After you have a digital ID, the simplest thing you can do is to send someone a message that contains your digital signature. A digitally signed message does more than simply assure your recipient that you are really yourself — who else would you want to be, after all? Suppose that you want to send an encrypted message that only your recipient can read. To do so, you have to send at least one digitally signed message first so that Outlook can capture details about your digital ID.

After you've obtained a digital ID, you can send a message with a digital signature by following these steps:

1. **While creating a message, click the Options tab at the top of the message screen.**

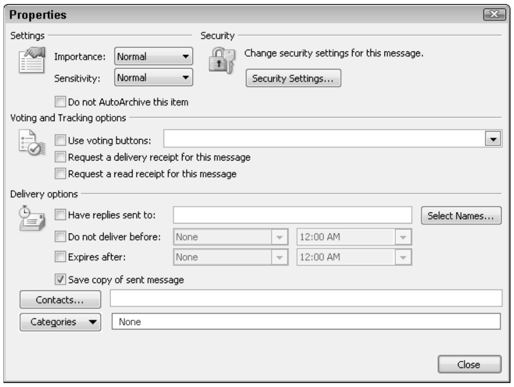
   The Options Ribbon appears.

2. **Click the icon to the right of the words *More Options*.**

   The Properties dialog box appears (as shown in Figure 15-2).

3. **Click the Security Settings button.**

   The Security Properties dialog box appears.



Properties

Settings

Importance: Normal

Sensitivity: Normal

□ Do not AutoArchive this item

Security

Change security settings for this message.

Voting and Tracking options

□ Use voting buttons:

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

□ Have replies sent to:

□ Do not deliver before: None 12:00 AM

□ Expires after: None 12:00 AM

☑ Save copy of sent message

Categories: None

Figure 15-2: To sign messages one at a time, click the Security Settings button in the Properties dialog box.

4. **Select the Add Digital Signature to This Message check box.**

5. **Click the OK button.**

   The Security Properties dialog box closes.

6. **Click the Close button.**

   Your message is now secure.

Adding a digital signature slows the process of sending a message somewhat because your computer has to check with the computer that issued your digital ID to verify your signature. But because Outlook checks your digital ID, your recipient can be sure that your message really came from you, and that's the whole point of digital signatures.

TIP

You can also set up Microsoft Outlook to attach a digital signature to every message you send, if you like. Just go back to the Trust Center, click the E-Mail Security button, and then select the Add Digital Signature to Outgoing Messages check box. In some industries, you may be required to add digital signatures to every outgoing message — but for most people, that's probably overkill.

Receiving Digitally Signed Messages

When you receive a message that contains a digital signature, you see a little icon in the upper-right corner of the message that looks like a little red prize ribbon that you'd win at the county fair for the best peach preserves.

You don't really need to do anything when you get a message like that; the icon itself verifies that the message really came from the person it claims to have come from. But if you're unusually curious, you can find out more about the person who signed the message by clicking the icon and reading the dialog box that appears. What you see should simply confirm what you already know: The person who sent the message is exactly who he says he is — the genuine article, the Real McCoy.

Encrypting Messages

Back in the days of radio, millions of children loved to exchange "secret" messages that they encoded with Little Orphan Annie's Secret Decoder Ring. Outlook does something similar, using a feature called Encryption. Unfortunately, you don't get a colorful plastic ring with Outlook. On the other hand, you don't have to save your box tops to get one — the decoder is built right into Outlook. When you encrypt a message, your system scrambles the contents of your outgoing message so that only your intended recipient can read your message.

Before you can send someone an encrypted message using Outlook's Encryption feature, both you and the person to whom you're sending your encrypted message need to have obtained a digital certificate, as I describe earlier in this chapter. Also, your intended recipient needs to have sent you at least one message with a digital signature, which I also describe earlier, so that Outlook recognizes that person as someone you can trust. Outlook can be pretty suspicious; even your mother can't send you an encrypted message unless you've sent her your digital signature first. Can you imagine? Your own mother! But I digress.

To send an encrypted message to someone who meets all the requirements, follow these steps:

1. **While creating a message, click the Options tab at the top of the message screen.**

   The Options Ribbon appears.

2. **Click the icon to the right of the words *More Options*.**

   The Properties dialog box appears.

3. **Click the Security Settings button.**

   The Security Properties dialog box appears.

4. **Select the Encrypt Message Contents and Attachments check box.**

5. **Click the OK button.**

   The Signing Data with Your Private Exchange Key dialog box appears.

6. **Click the Close button.**

   Your message is encrypted.

When you receive an encrypted message, the contents of the message don't appear in the Reading pane; you have to double-click the message to open it. In fact, if you work in a big organization, your network may deliver the message to you as an attachment to a serious-sounding message warning you that encrypted messages can't be scanned for viruses.

Antivirus Software

One of the biggest risks for every computer owner is a virus infection. You've probably heard news reports about computer viruses that spread across the Internet faster than a wildfire and to much worse effect. Every day new viruses seem to appear, and each new virus gets sneakier about how it wheedles its way into your system. Many viruses come to you through e-mail, often appearing as e-mail messages that seem to come from people you know. Others sneak in through your browser when you're surfing the Web. In most cases viruses only create a mild annoyance, but some are so destructive that they can render your computer permanently useless and destroy all the work you've created and left on that machine, then move on to all your friends' computers and do the same to them.

There's no substitute for effective anti-virus software if you use your computer the way most people do today. Most antivirus programs automatically connect to Outlook, scan incoming message for viruses, and automatically block any message that might be infected.

The tricky thing about antivirus software is that there are fake antivirus programs out there that pretend to protect you, but actually act as viruses themselves, inflicting your machine with alarms and annoyances and forcing you to purchase "updates" that only make the problem worse.

If you don't keep up with the latest developments in antivirus software, your best bet is to buy a well-known brand of antivirus software at your favorite computer store and install it as soon as you can. Some computers come with antivirus software preinstalled, but those packages sometimes want you to buy annual updates. If the software is Norton Antivirus from Symantec, McAfee VirusScan, or Kaspersky Internet Security, you know they're legitimate and you'll do well to buy the updates. You can also go to an antivirus software manufacturer's Web site and buy a downloadable version. The sites for the products I just mentioned are:

- Norton Antivirus at `www.symantec.com`
- McAfee VirusScan at `www.mcafee.com`
- Kaspersky Internet Security at `www.kaspersky.com`

There are also legitimate antivirus titles that you can get for free. Microsoft now offers a free antivirus program called Microsoft Security Essentials (`www.microsoft.com/security_essentials`), which I haven't yet tested extensively, but it looks good and Heaven knows the price is right. I've relied on a free antivirus program called AVG (`http://free.avg.com`) for many years, and I've found it to be effective. Bear in mind, however, that if you rely on free antivirus software, you'll have nobody to call when something goes wrong, and antivirus software matters most when something goes wrong, so if you're not comfortable dealing with geeky details yourself, the for-fee antivirus programs are worth what you pay.