Privacy through encryption

Don't leave your computer an open book. *by Russell Shaw*

Imagine a stranger secretly listening in on your telephone conversations. What would you do if that creepy snoop learned sensitive details about you, everything from the credit-card number you use for catalog shopping to your confessions about what you really think of your family, friends, and significant other?

You'd be embarrassed, angry, *outraged*. And you'd take steps to ensure the eavesdropping stopped.

In fact, most of us take preemptive measures to ensure that such private telephone conversations are just that—private. We assume no one's tapping our phone line, but we don't reveal sensitive information over the phone if there's a chance someone within earshot might overhear.

But what about our online conversations and transactions? Are there precautions we can take to ensure that our email, our instant messages, and our shopping activities remain private? You bet there are. You'll find them filed under the heading "encryption."

ENCRYPTION BASICS

Encryption describes a process through which the data you send from your computer to a Website, an email correspondent, or an instant-messenger service is translated into a secret code before it's transmitted over the Internet. When the encrypted data arrives at its destination, the recipient uses a secret "key" to decrypt—or translate—the information back into readable form. In the meantime, anyone who manages to intercept the message encounters only meaningless gibberish.

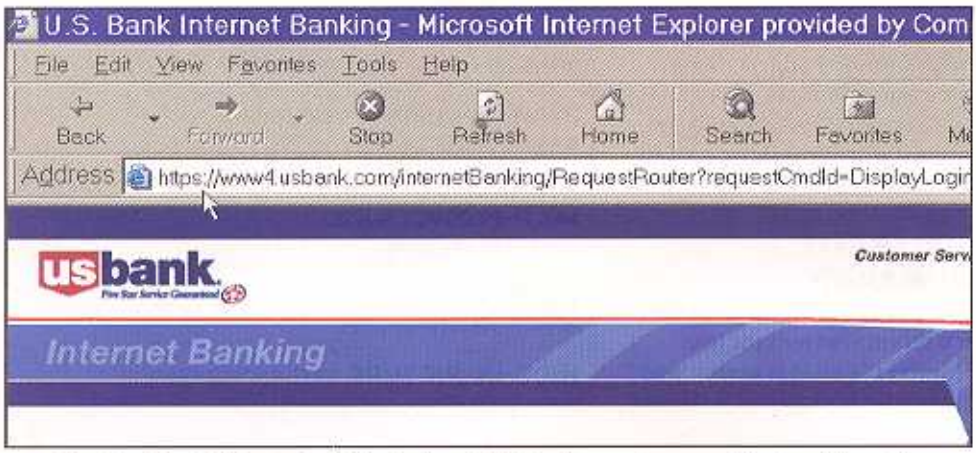
If you're thinking this is the stuff of wars, spies, and espionage, you're exactly right. What we're talking about is the science of cryptography: Using mathematics to encrypt and decrypt information. And if you know your history, you'll remember that cryptographers changed the course of World War II when they succeeded in breaking the German military's super-secret Enigma code.

Enigma would be child's play for today's powerful computers, but you'll find a variety of encryption solutions that guarantee you can send and receive secure communications over an insecure network, such as the Internet. Let's take a look at some of them.

SECURITY FOR WEB TRANSACTIONS

When you provide your credit-card number to a reputable online merchant, conduct an online banking session, or perform any transaction where you're sending and/or receiving sensitive information, the Website will use a communication protocol known as Secure Sockets Layer (SSL) to encrypt the data.

You can verify that the Website you're visiting is protected by the SSL protocol by looking at the URL (Universal Resource Link) that appears in your Web browser's

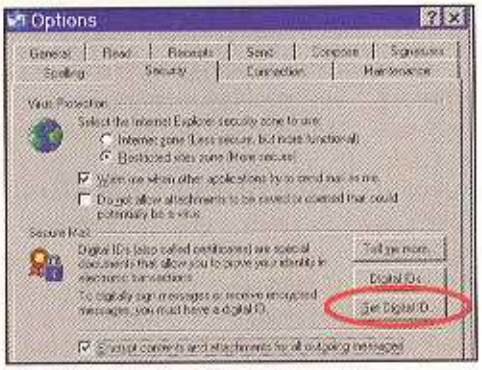


If the URL of the Website you're visiting begins with "https" you can be assured that any information you submit to the site is encrypted as it's being sent.

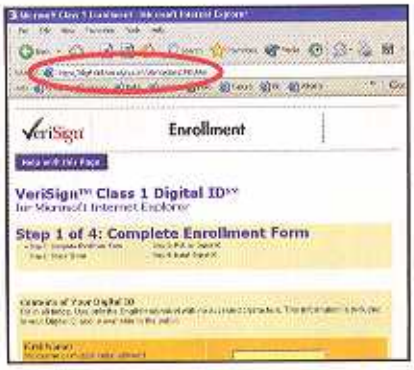
OBTAIN A DIGITAL ID The Easy Way

You can obtain a digital ID from a number of bona fide organizations. Since digital IDs are used most commonly for email, we'll show you the process of configuring Outlook Express with a digital ID issued by VeriSign, Inc.

VeriSign charges $14.95 for their service, and your digital ID must be renewed annually. Note: you'll need an active connection to the Internet during this exercise.

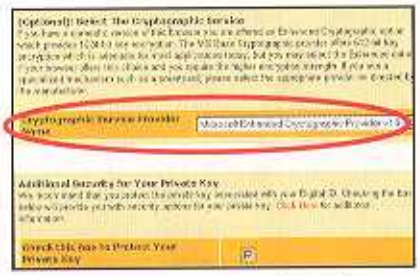


1 Launch Outlook Express. Click on the Tools menu and choose Options from the drop-down menu. When the Options box opens, click on the Security Tab and then click the Get Digital ID button. From here, you can either choose to follow the links to arrive at VeriSign's enrollment page, or you can proceed directly there via the URL in step 2.

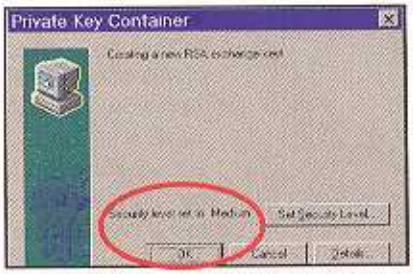


2 Open Internet Explorer. In the address box at the top of the page, enter this URL (note: the address must be typed exactly as follows, including using uppercase letters where indicated): https://digitalid.verisign.com/client/class1MS.htm

3 Complete the enrollment form by supplying your name, email address, and a "challenge phrase." This will protect your digital ID should someone try to revoke or change it. Scroll further down the page and enter your credit-card information.

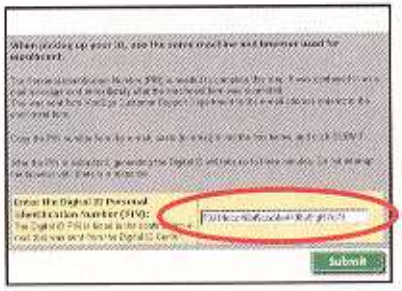


4 Scroll down and you'll be given the option of adding Enhanced Cryptographic protection to your browser. Choose Microsoft Enhanced Cryptographic Provider from the drop-down menu and place a checkmark next to "Additional Security for Your Private Key." Scroll down and click Accept.



5 A dialog box titled "Private Key Container" will appear. Leave the security setting at its default setting of Medium and click OK.

6 A second dialog box, titled "Signing Data With Your Private Exchange Key" will appear. Click OK.



7 You'll receive your Digital ID PIN via email. Point your browser to https://digitalid.verisign.com/enrollment/mspickup.htm, paste your PIN into the box, and click Submit.

8 You'll be taken to the Install Digital ID page. Click on the Install button, and your digital ID will be installed on your computer.

address window. If the address begins "https:" instead of the usual "http:" you'll know the page is encrypted (the "s" in this example stands for "secure").

If you'd like to verify that Internet Explorer is configured to use SSL, open the program and click on the Tools menu, scroll down, and choose Internet Options. When the window pops up, click on the Advanced tab and scroll down to the bottom of this box and you'll find a series of checkboxes under the heading of Security. Make sure both SSL-related boxes have checkmarks next to them.

Most email programs, including Microsoft's Outlook and Outlook Express programs, also support SSL. Refer to the sidebar "Securing Outlook Express" and we'll show you how to configure that program for SSL.

Web-based email services, such as Microsoft's Hotmail or Yahoo Mail, use SSL by default; in fact, your Web browser must be configured for SSL in order to use these services to begin with. However, they use SSL only to prevent your username and password from being intercepted when you send this information to their Website. While this makes it impossible for anyone to capture your username and password in transit, it does nothing to encrypt your actual email correspondence. We'll look at how to do that next.

ENCRYPTING YOUR EMAIL

Encrypting email is more involved than encrypting other types of information—usernames, passwords, and credit-card information—you might send over the Internet. You should, however, encrypt your email whenever you're sending sensitive information to your email correspondents. In fact, you should encrypt any email correspondence you wouldn't want just anyone reading.

Intercepting email correspondence in transit isn't a trivial matter, but neither is it impossible for a determined hacker or other criminal. A more common concern would be the security of your correspondence while it's being stored on your correspondent's computer. If other people have access to that machine, they might be able to gain access to unencrypted emails. If you encrypt your email, you can guarantee that only the intended recipient can read it.

But cryptography faces what you might call a chicken-or-the-egg problem (meaning, which came first, the chicken or the egg?). In order for encryption to work, the person receiving an encrypted message must possess the same key that was used to encrypt it. But if the key is sent unencrypted, it could be intercepted and surreptitiously copied by a third party, who would then be in a position to decrypt the supposedly secret message.

The modern solution is to use two mathematically related keys, one that is public and one that remains private. Anything that is encrypted with the public key can be decrypted only by using the private key.

Here's a simplified look at how this works: You provide your public key to the person with whom you wish to correspond, and they'll use it to encrypt the messages they send you. When you receive these messages, you use your related private key to decrypt them. In order for two-way encrypted

ENCRYPTING INSTANT MESSAGES

These days, a lot of correspondence happens via instant messages, using programs such as AOL Instant Messenger (AIM), MSN Messenger, ICQ, and others. Although none of these programs have built-in encryption features, you'll find a variety of third-party tools that will do the job.

If you use AIM for chatting online, take a look at the free program AIMEncrypt. This handy utility adds Secure Sockets Layer encryption to AOL Instant Messenger, so that if someone intercepts the chat session you're having with a friend, they'll see only gibberish. In order for the encryption to work, however, both you and the person you're chatting with must be using AIMEncrypt.

If you use other instant-messenger programs—or more than one IM program—take a look at JohnyTech's Encrypted Messenger 3 ($14.95). As with AIMEncrypt, both parties must install the software in order to encrypt their online conversation. To get around the problem of forcing someone else to buy the program, however, the full-price version comes with a free "lite" version that you can send to your friends. They'll be able to encrypt any conversation you initiate, but they won't be able to initiate an encrypted conversation with you.

Encryption Software's Top Secret Messenger can encrypt instant messages you send via ICQ or MSN Messenger.

correspondence to work, of course, the other person must also maintain a private key and provide you with their public key.

Now this is all fine and dandy, except that you have no way to prove that the person at the other end of the email is really who they say they are—or that someone masquerading as you doesn't initiate encrypted correspondence using their own public and private keys. The solution to this problem lies with a digital ID.

A digital ID consists of the aforementioned public and private keys, plus a digital signature. You purchase digital IDs from a certification authority, such as VeriSign. (Note: The certification authority will require you to prove your identity before they'll issue your digital ID.) Refer to the sidebar "Obtain a Digital ID" for details.

In order to send encrypted email, both parties must have digital IDs; otherwise, the recipient of your correspondence could decrypt the message and respond to you in the clear, defeating the purpose of your encrypting the message. If you're using Outlook or Outlook Express, your correspondents' digital IDs will be stored in your address book.

Once you have your own digital ID, you must configure your email software to encrypt your email. To encrypt individual messages in Outlook or Outlook Express, create a new message, click on Options in the message toolbar, and then click on the Security Settings button in the window that opens. Put a checkmark next to the item that reads "Encrypt contents and attachments." To enable encryption in all Outlook or Outlook Express email messages you send, click on the Tools menu, choose Options, and then click on the Security tab. Place a checkmark on the box that reads "Encrypt contents and attachments for outgoing messages." Click OK when you've finished. (Note: As long as Outlook or Outlook Express is configured this way, you won't be able to send any email until you've provided the software with your digital ID.)

Try and send encrypted email from Outlook or Outlook Express, and you'll get this message if you haven't already obtained a digital ID.

When you send and receive email containing digital IDs, you can be assured that not only is your correspondence encrypted, but that you know the person at the other end is who they claim to be—and *they* know that *you* are who you say you are.

PARANOIA OR COMMON SENSE?

It's easy to dismiss security measures such as encryption as paranoia. You're probably thinking "Who'd want to spy on little ol' me?" The problem is compounded by the fact that you can't have encrypted email correspondence unless *both* parties take the step of obtaining digital IDs and renewing them each year.

But the more comfortable you become with electronic correspondence such as email and instant messaging, the more likely you'll be to reveal sensitive and private information. And although it's not a trivial matter, neither is it all that difficult for someone to intercept unencrypted correspondence.

You should also remember that unlike a telephone call, email correspondence is a semi-permanent record—it exists until someone destroys it. And because of the nature of computers and the Internet, you don't have control over where copies of that record might end up or when they get destroyed.

It's simple, really: If your electronic correspondence and transactions are encrypted, you can control who reads them. If they're not, you can't. The good news is that you get to decide if it matters. ■

CONTACT INFO

Here's where you can get additional information about the encryption products mentioned in this story.

VERISIGN DIGITAL ID
CERTIFYING AUTHORITY
www.verisign.com

ENCRYPTED MESSENGER
INSTANT-MESSAGE ENCRYPTION
johnytech.com

TOP SECRET MESSENGER
INSTANT-MESSAGE ENCRYPTION
www.encrsoft.com