

Biztech

INFORMATION TECHNOLOGY SOLUTIONS TO GROW YOUR BUSINESS

You make the work great. (Color will get it noticed.)

Lexmark C510N

Small workgroup color laser printer for price-sensitive business users.

Offer subject to CDW's standard terms and conditions of sale, available at CDW.com



Now just **\$699.99**

[More Info](#)



[[ROI](#)] [[wireless](#)] [[finance](#)] [[IT investment](#)] [[profiles](#)] [[security](#)] [[networking](#)] [[telecommuting](#)] [[regulatory](#)] [[management](#)]

:: current issue



[» Subscribe Now!](#)

contents

Features

Hiring Trends Report

Take A Lesson On SOX

Preparing For The Worst

Ten High-End Technologies You

Can Afford

Letter from the Editor

Dashboard

Out-of-the-Box ROI

Security, Part I

Security, Part II

Money Matters

How To

Growing Pains

Tech Trends

Best Practices I

Best Practices II

The Lowdown

Your CIO

Harry's Corner

Takeaways

[[Security - November 2005](#)]

Who Wants to Know?

Anyone with a bit of curiosity can read e-mail as it travels the Internet. Here's how to keep it private.

By Debby Young

Sending e-mail over the Internet is comparable to sending postcards through the U.S. mail—anyone can take a peek along the way.

But if companies don't want their electronic communications to be an open book, there is encryption available that can be set according to the privacy needed.

The most basic step requires integrating encryption into the Simple Mail Transfer Protocol (SMTP) used to send e-mail over the Internet. Some level of encryption makes sense because experts agree that SMTP is inherently insecure.

Given that businesses generally use one of the three big e-mail packages—Microsoft Exchange, IBM Lotus Domino or Novell GroupWise—the encryption feature comes standard. But how and when a business uses it is the question, says Phil Karren, senior product manager for GroupWise at Novell.



Eric Tucker / Getty Images



Looking to get more work done? (Find a way to work in more places.)

ThinkPad T42

Making the power of a workstation mobile.

- 1.6GHz Intel Pentium M

Starting at **\$1349***

*After \$200 trade-in

[More Info](#)



ThinkPad

Offer subject to CDW's standard terms and conditions of sale, available at CDW.com

Looking to get more work done?
(Find a way to work in more places.)



Panasonic TB 51
Full-featured desktop
alternative.

Starting at **\$1299***

*After trade-in

[More Info](#)

Panasonic.
Offer subject to CDW's standard terms and conditions of sale, available at CDW.com



"If you're managing landscaping supplies, then you probably don't care, but if you're dealing with the Health Insurance Portability and Accountability Act, then you have to use" full encryption, Karren says.

Most e-mail systems support Secure Multipurpose Internet Mail Extension (S/MIME), so it's relatively simple for one company to send encrypted e-mail to another as long as both have enabled the S/MIME feature on their mail servers, explains Kevin Lynch, Domino security development manager at IBM.

Complexity Factor

The various levels of encryption on some e-mail systems are more complicated to configure than on others, Lynch notes, a factor that small businesses will want to consider when choosing their e-mail systems.

According to Stefan Dietrich, software architect and former chief operating officer for e-Vantage Solutions of New York, small businesses need to be smart about data exchanges via e-mail and those with whom they are messaging. "Once you send e-mail over the Internet, you have to use SMTP, and when you do that, a lot of the information you're sending goes out in clear text format that can be intercepted," Dietrich says.

Internet service providers will provide encryption as part of their messaging service, based on each client's request. DSLExtreme in Los Angeles, for example, offers three levels of progressively more secure encryption.

The percentage of small businesses using the most secure level of encryption is small, says Jim Murphy, DSLExtreme's president. But he's noticed a rise in Level 1 encryption.

Murphy detailed the three encryption levels his company provides. "Level 1 is simple authentication encryption, encryption of the password when you're connecting to the mail server," he explains. "But the messages between the server and the Internet are not encrypted at all."

About 20 percent of DSLExtreme's small-business customers take advantage of this service, which the company offers for free. IT

managers can enable authentication encryption for their e-mail clients using a simple checkbox when setting up employee e-mail accounts.

Level 2 encryption supports both authentication encryption and encryption of messages going to and from the mail server.

"If you send something from your desktop to the server, it's encrypted," Murphy says. "But as soon as it leaves the server and goes to the Internet, it's not encrypted anymore."

DSLExtreme stores encrypted messages on its host servers using S/MIME. About 5 percent of the company's small-business clients use the Level 2 S/MIME option, he says.

Murphy classifies Level 3 as full end-to-end encryption of the message and user password as data travel from a sender's desktop system across the Internet and into a recipient's mailbox. Murphy sees little use of this full-blown encryption among his customers—fewer than 1 percent.

"It involves dealing with digital certificates and public and private keys," he explains. "Most small businesses don't have the resources—dedicated IT staff or the budget—to manage this."

From Outbox to Inbox

For some companies, end-to-end e-mail encryption is essential. For instance, if your company works with health data and moves files via e-mail, you must comply with the security requirements of the Health Insurance Portability and Accountability Act (HIPAA) and ensure that data remain private.

In cases where legislation such as HIPAA would apply or if a lot of personal identifying information is moved via e-mail, companies should consider stringent encryption options:

How Small Businesses Guard Against E-mail Vulnerabilities

Scan for viruses	82%
Block or quarantine attachments	69%
Filter incoming mail for spam	68%
Institute acceptable-use policy	22%
Restrict Internet e-mail use	20%
Do nothing	5%
Don't know	2%

Total exceeds 100 percent because respondents could select multiple answers.

Source: *Small Business Technology Institute, July*

Transport Layer Security: TLS is an encryption and authentication protocol that encodes the entire message stream (sender and recipient information as well as the message itself) while it moves between client and server systems.

"With TLS enabled, all of your e-mail traffic from your company's SMTP mail server to external TLS-enabled SMTP mail servers will be encrypted from start to finish," says Joel Snyder, e-mail security expert and senior partner for Opus One of Tucson, Ariz.

Most mail servers come with a TLS feature. Once enabled, users will need to use digital certificates to prove the identity of clients and servers. Companies such as VeriSign of Mountain View, Calif., and

2005

RegisterFly.com of West Orange, N. J., offer certificate authority services

and sell digital certificates.

TLS isn't foolproof. "If you don't match the server certificate to the identity you think you're sending to, you're susceptible to a man-in-the-middle attack," Snyder says. "You could be sending encrypted traffic, but not to your intended recipient."

Because SMTP mail is forwarded through a number of relays, there's no assurance that the message will remain encrypted at each hop, giving hackers an opportunity to intervene and capture data.

Secure Multipurpose Internet Mail

Extension: S/MIME enhances encryption, authentication and data integrity checking. The sender encrypts and digitally signs each message before sending it. The recipient's e-mail program verifies the signature, checks that the message itself hasn't been tampered with and determines whether the digital signature matches the return address on the mail, thereby authenticating the sender.

Like TLS, S/MIME requires each user to have a digital certificate. When a certificate authority generates a certificate, it also creates two keys simultaneously: a public key stored in a public directory and a private key for the user. Senders use the public keys to encrypt messages intended for specific recipients. The receivers use the private keys to decrypt them.

There are some obvious drawbacks to S/MIME. If a recipient loses the private key, encrypted e-mail is unreadable. Plus, there's the chance of malware getting into a network if the e-mail system is not properly set to check the messages, Snyder points out. "Because the message is encrypted from end to end, virus scanners, message archivers and antispam tools aren't able to peer inside," so the entire e-mail system can be vulnerable to intrusions if a message contains malicious content.

Pretty Good Privacy: PGP, like TLS and S/MIME, uses digital certificates with private and public keys. Besides protecting and verifying mail during transit, some people use PGP to encrypt files being stored so that intruders or other users can't read them.

PGP is shareware that can be downloaded for free, although a low-cost commercial version is also available. The tool's user interface works with the client e-mail program, adding an encryption and verification button to the desktop tool bar.

In the End

There's really no good reason not to use encryption, says Mark Sunner, chief technology officer for MessageLabs, an e-mail security company in New York City. Beyond the need to cloak business information from prying eyes, there are the issues of basic security of your network from e-mail attacks, he says.

"With the plethora of Trojan horses and spyware out there, if you have to communicate sensitive data you don't want exposed, you have an obligation to encrypt at some level," Sunner says.

IT takeaway

Use digital signatures to protect users against spoofing (e-mail that appears to be coming from someone a user knows but is really from someone phishing for information), spyware or attempted hacks.

Educate users to guard their passwords and private keys. Send out weekly reminders, for example, cautioning them not to divulge this information to anyone. Ban Post-It notes with sensitive information from monitors.

Make security consciousness part of the corporate culture because complacency is the greatest security risk. Hold periodic meetings to review security policies and why they are so important.

Boost individual message security by making the content of each e-mail a separate encrypted attachment.

[e-mail](#)[print](#)