KEEP YOUR SECRETS FROM FALLING INTO THE WRONG HANDS WITH THESE PRACTICAL COUNTERINTELLIGENCE MEASURES

FOR YOUR EYES ONLY

by Ben Patterson

The next time you visit your local coffeehouse and blithely surf the Web over its public Wi-Fi connection, consider this: Every website you browse, every unencrypted form you submit, and every e-mail you send is fair game for the hacker sipping a double mocha at the table next to you. Using network "sniffing" programs that are easily found on the Web, Wi-Fi snoopers can track your every move through cyberspace. They might even lift a password or two, giving them unfettered access to your amorous e-mail correspondence with Trudy the Zamboni driver and exposing your membership in the Hair Club for Men.

Pretty scary, right? But don't pack up your gear and head home just yet. There are plenty of online services and software available that can cloak your surfing and your messages with state-of-the-art encryption that even the wiliest of hackers can't crack. Better yet, you don't have to be an expert to use the latest security software: It works quietly behind the scenes to keep your information and surfing habits safe.

Read on for some of the best, easiest-to-use security and encryption software for surfing from public hotspots. Not only will you be able to surf and communicate behind a veil of secrecy, you'll even keep your information safe from the more traditional thieves who might snatch your notebook while you're ordering another latte.

CRYPTO 101

How encryption software wraps your secrets in a mystery inside an enigma

If you've ever tried to fool your kid brother by saying "I'm oing-gay to the ovies-may," you're an amateur cryptographer. The cipher used in pig latin is painfully simple, but the basic principle of garbling a message in a predictable way is similar to the techniques used by the most powerful encryption software.

Of course, today's cryptographers have moved well past such simple ciphers. Modern encryption methods, such as DES (data encryption standard) and AES (advanced encryption standard, now the method of choice for the U.S. military), use extremely complex mathematical algorithms to create "keys" that lock up sensitive data. These cryptographic keys are strings of letters and numbers of various lengths, and the longer they are, the harder it is to crack a message coded using the key. The encryption used for most secure webpages (such as those in which you submit a credit card number) use 128-bit keys and AES encryption, while some security programs go even further with 256-bit key AES.

Can AES encryption be cracked? For the time being, no way. You'd have more luck creating life from a box of Legos than making sense out of an AES-encrypted message. While a specialized device was developed a few years ago that can crack DES encryption within a matter of hours, that same hardware would take 149 trillion years to unlock a 128-bit AES key. Cryptography experts believe it will take at least 20 years before someone discovers a technique to crack AES.

So now that you have an encryption key that is — for now — impossible to crack, how do you use it to protect your files and messages? When it comes to protecting files on your hard drive, you can use a process known as symmetrical, or single key, encryption. That means you use the same key (itself protected by a password) to encrypt and decrypt your files. Symmetrical encryption is a perfectly secure system if you just want to keep your data in a virtual lockbox.

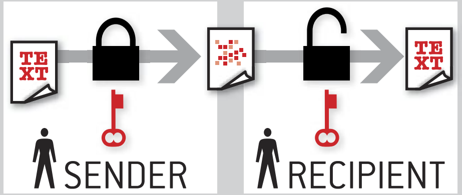
Securely transmitting data to another party is a bit more complicated. Sure, you could encrypt a message, send it to a colleague, and give her the key. But how do you get the key to her securely? What's more, you may not want to trust the recipient with your password. Would you hand out your house key to just anyone, even that creepy guy in the mail room? We didn't think so.

That's where asymmetrical, or public key, encryption comes in. Public-key encryption, which was developed in the 1970s, works on the principle of creating a pair of keys instead of just one. One key is your private key, which you use to decode messages, while the other is your public key, which your correspondents use for encoding messages to you. For example, if your boss wants to send you a private message, she encodes it with your public key; when you get the message in your inbox, you decrypt it with your private key. To reply, you take her public key, encrypt the message, and send it. She'll then decrypt the message with her own private key.

The beauty of public-key encryption is that anyone — even a stranger — can send you encrypted messages, as long as he has your public key, and you can encrypt your replies back to him. No passwords or keys are ever exchanged.

SYMMETRICAL ENCRYPTION

The same key is used to encrypt and decrypt files and messages.

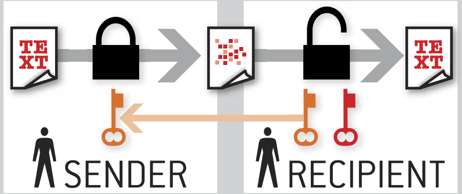


1. The sender uses a digital key to encrypt data before sending it.

2. The recipient uses an identical key to decrypt the data, restoring the original document.

ASYMMETRICAL ENCRYPTION

Others use your public key to encrypt messages before delivering them to you. You then use your private key to decrypt these messages.



1. The sender requests the recipient's public key, then uses it to encrypt data for delivery.

2. The data can then be decrypted only with the recipient's private key, which no one else has.

SECURE E-MAIL

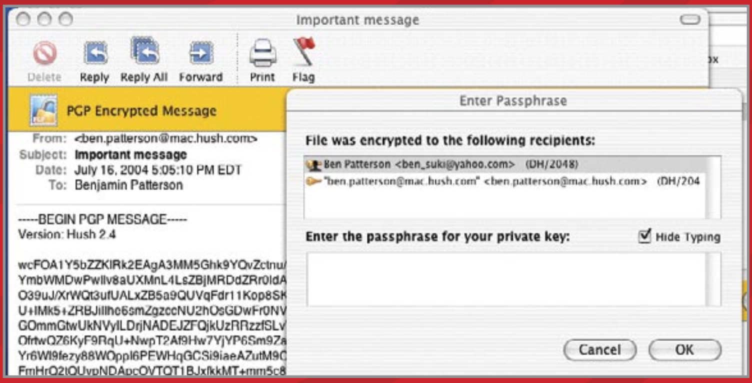
Purloined letters? Not any more, with these mail security tools

→ If you're using a public hotspot and you need to send a few sales figures via e-mail, think twice. More likely than not, your Web e-mail service (such as Hotmail or Yahoo Mail) or e-mail client (such as Outlook Express) uses an unencrypted protocol for transmitting messages. That means any 15-year-old hacker who knows what he's doing can read your messages word for word. He can even grab your e-mail password when you log on. Don't give hackers a free pass to peruse your e-mail; instead, cloak your communications with an encryption service.

PGP Personal Desktop

PGP Corporation	$60
www.pgp.com	

You probably won't lose sleep if a hacker intercepts your e-mail to the gang asking where they're meeting for drinks. But if you're sending a message that could bring Western civilization to a crashing halt if it fell into the wrong hands, consider using PGP Personal Desktop. Developed in 1991 by encryption guru Phil Zimmerman, the modestly named Pretty Good Privacy provides solid encryption for your files and e-mail. The current incarnation of PGP uses 256-bit AES public-key encryption to protect your messages and files from prying eyes. (See "Crypto 101" on page 83 for a brief primer on how it works.) PGP Personal Desktop seamlessly encrypts your e-mail messages, turning them into blocks of gibberish that are almost impossible to crack. The program steps you through the process of creating public and private PGP keys as well as setting a "strong" pass phrase (one that doesn't use your birthday or your dog's name, for instance). Plug-ins for Outlook and Apple Mail let you encrypt your e-mail with the click of a button. You can also encrypt any files you want to attach to your message, or encode e-mail with an encrypted "signature" that lets the recipient know with certainty that the message came from you intact and unaltered.



From: <ben.patterson@mac.hush.com>
Subject: **Important message**
Date: July 16, 2004 5:05:10 PM EDT
To: Benjamin Patterson

```
-----BEGIN PGP MESSAGE-----
Version: Hush 2.4

wcFOA1Y5bZZKIRk2EAgA3MM5Ghk9YQvZctnu/
YmbWMDwPwllv8aUXMnL4LsZBjMRDdZRr0IdA
O39uJ/XrWQt3ufUALxZB5a9QUVqFdr11Kop8SK
U+IMk5+ZRBJillhe6smZgzccNU2hOsGDwFr0NV
GOmmGtwUkNVylLDrjNADEJZFQjkUzRRzzfSLv
OfrtwQZ6KyF9RqU+NwpT2Af9Hw7YjYP6Sm9Za
Yr6Wl9fezy88WOppl6PEWHqGCSi9iaeAZutM9C
FmHrQ2tQUvpNDApcOVTQT1BJxfkkMT+mm5c8
```

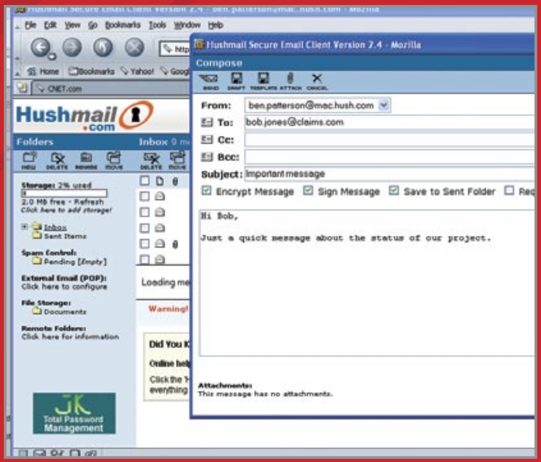
File was encrypted to the following recipients:
Ben Patterson <ben_suki@yahoo.com> (DH/2048)
"ben.patterson@mac.hush.com" <ben.patterson@mac.hush.com> (DH/204

Enter the passphrase for your private key: ☑ Hide Typing

Hushmail

Hush Communications	Free; $14 per year for IMAP access
www.hushmail.com	

PGP Personal Desktop is a great way to encrypt e-mail from your notebook. However, if you're logging in from an Internet café during a hurried stopover in the Rio de Janeiro airport, you'll need another way to send your extortion demands securely. Hushmail is a Web e-mail client that lets you send AES-encrypted messages from almost anywhere, using just a Web browser. The free version lets you set up a new e-mail account and create public and private encryption keys, which are stored on Hushmail's key server. (You should also send your Hushmail public key to your correspondents and upload their public keys to the Hushmail key server.) Once your account is set up, you can send encrypted Hushmail messages from any Internet-connected PC or notebook. The site's webpages are secured with an SSL (secure sockets layer) link to protect your login password, although even if a network snoop were to grab one of your e-mails, all he would get is a block of seemingly random text. For $14 a year, you can retrieve messages from Hushmail using any e-mail client with IMAP support.


File Edit View Go Bookmarks Tools Window Help
Home
Bookmarks
Yahoo!
CNET.com
Hushmail.com
Folders
Inbox
NEW
DELETE
RENAME
MOVE
Hushmail Secure Email Client Version 2.4 - Mozilla
Compose
SEND
DRAFT
TEMPLATE
ATTACH
CANCEL
Total Password Management

Storage: 2% used
2.0 MB free - Refresh
Click here to add storage!
Inbox
Sent Items
Spam Control:
Pending [Empty]
External Email (POP):
Click here to configure
File Storage:
Documents
Remote Folders:
Click here for information

From: ben.patterson@mac.hush.com
To: bob.jones@claims.com
Cc:
Bcc:
Subject: Important message
☑ Encrypt Message ☑ Sign Message ☑ Save to Sent Folder ☐ Req

Hi Bob,

Just a quick message about the status of our project.

Attachments:
This message has no attachments.

FILE SECURITY

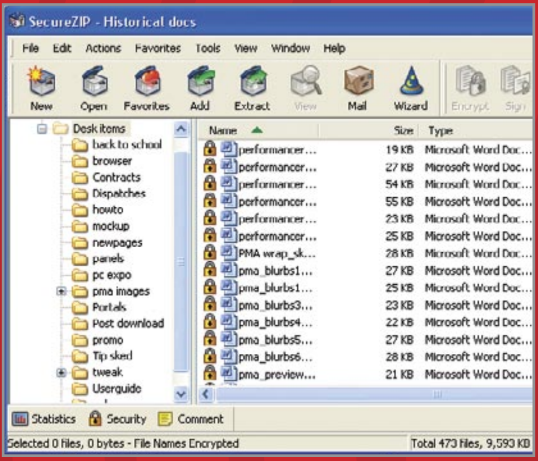
Your secrets will be safe, even if your notebook's not

→ Picture this: You're sitting in Starbucks working industriously at your notebook when you decide to get one more napkin. You get up, come back, and your notebook has vanished. First, you're mad that the ultralight you campaigned so hard for is gone, but then it hits you: Whoever took your precious computer now has all your customer data, spreadsheets, and diagrams of the top-secret Flubber manufacturing process you've been working on. While you may not be able to get your notebook back, at least you can make sure that your information stays under lock and key.

SecureZip

PKWare	$100
www.pkware.com	

If you've been keeping archives of your files on your notebook, consider how easy it would be for a thief to make off with your crown jewels. With SecureZip on the case, your files won't end up in the wrong hands. SecureZip takes your most sensitive files and packs them into an encrypted Zip archive. You can choose 128-bit to 256-bit AES encryption, which will make for a virtually impregnable archive, and you can even have SecureZip encrypt the names of the protected files. After your files are packed into the archive, SecureZip will go back and wipe the originals off your system, rendering them unrecoverable. (You can also leave the originals as is, if you prefer.) Once the archive is finished, anyone who tries to open the file will be prompted for a password; if a snooper can't cough up the right pass phrase, he won't be able to open the archive or see the names of the files inside. SecureZip can also scan encrypted files for viruses, authenticate archives with certificates obtained from VeriSign or BT Trustwise, or send archives via e-mail using your default e-mail client.



Desk items
- back to school
- browser
- Contracts
- Dispatches
- howto
- mockup
- newpages
- panels
- pc expo
- pma images
- Portals
- Post download
- promo
- Tip sked
- tweak
- Userguide

Name	Size	Type
performancer...	19 KB	Microsoft Word Doc...
performancer...	27 KB	Microsoft Word Doc...
performancer...	54 KB	Microsoft Word Doc...
performancer...	55 KB	Microsoft Word Doc...
performancer...	23 KB	Microsoft Word Doc...
performancer...	25 KB	Microsoft Word Doc...
PMA wrap_sk...	28 KB	Microsoft Word Doc...
pma_blurbs1...	27 KB	Microsoft Word Doc...
pma_blurbs1...	25 KB	Microsoft Word Doc...
pma_blurbs3...	23 KB	Microsoft Word Doc...
pma_blurbs4...	22 KB	Microsoft Word Doc...
pma_blurbs5...	27 KB	Microsoft Word Doc...
pma_blurbs6...	28 KB	Microsoft Word Doc...
pma_preview...	21 KB	Microsoft Word Doc...

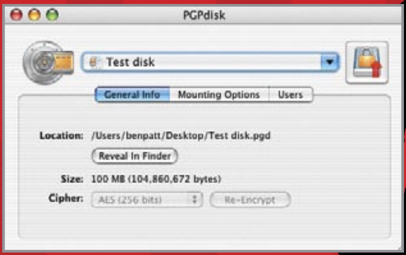
Selected 0 files, 0 bytes - File Names Encrypted

Total 473 files, 9,593 KB

PGPdisk

PGP Corporation	$60 (comes with PGP Personal Desktop)
www.pgp.com	

Chances are, your most sensitive documents are the ones you're using on a day-to-day basis. If that's the case, you're probably not going to bother creating a secure archive of your spreadsheet every half hour. An easier way of keeping your oft-used documents safe is with an encrypted disk image. PGPdisk, a component of PGP Personal Desktop (see page 84), creates an encrypted, password-protected disk volume on your hard drive. (Think of it as just another drive on your network.) You can create a disk image of any size that is protected by either 128- or 256-bit AES encryption. To mount the protected disk on your system, you click on the image and enter your pass phrase; you can then move your important files inside the drive and work on them as you would normally. When you're finished, you unmount the drive with the click of a button, and that's it — your files are encrypted. If you need to get back into your files, just mount the disk again and re-enter your password. You can set your PGPdisk to unmount after a specified time of inactivity, and you can also grant read-write or read-only privileges to other users.



Test disk

Location: /Users/benpatt/Desktop/Test disk.pgd

Size: 100 MB (104,860,672 bytes)

Cipher: AES (256 bits)

SECURE COMMUNICATIONS

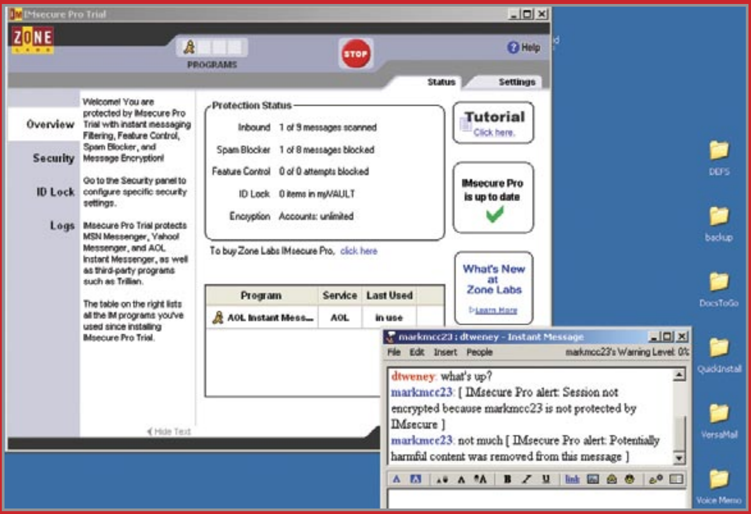
It's like having your own virtual war room

Surfing at a public hotspot is a little like displaying your browser history on a JumboTron. And instant messaging? Forget about it. Anyone with a simple Wi-Fi sniffing utility can see where you're surfing, what you're typing, and whom you're chatting with. To protect your privacy while you're connecting wirelessly, use a virtual private network (VPN) or secure chat and collaboration tools, so you can get your work done without any unwanted flies on the wall.

IMsecure

Zone Labs	Free (protects one IM client); $20 (protects multiple IM accounts)
www.zonelabs.com	

If you're sending instant messages over a public hotspot, you may as well stand up and shout your conversations for all to hear. The majority of IM clients send messages as cleartext, meaning that wireless snoopers can read your every smiley. You can foil Wi-Fi sniffers with IMsecure, a program that encrypts IM traffic. IMsecure uses 56-bit DES security, which is strong enough to deter casual snoopers but not nearly as secure as 128-bit AES; if hard-core hackers are after your secrets, be careful what you say. Provided your friends have IMsecure installed on their systems as well, you can send IMs over AIM, ICQ, MSN Messenger, and Yahoo Messenger in relative security. IMsecure also blocks IM spam ("spim") and guards against Net attacks.



Welcome! You are protected by IMsecure Pro Trial with instant messaging Filtering, Feature Control, Spam Blocker, and Message Encryption!

Go to the Security panel to configure specific security settings.

IMsecure Pro Trial protects MSN Messenger, Yahoo! Messenger, and AOL Instant Messenger, as well as third-party programs such as Trillian.

The table on the right lists all the IM programs you've used since installing IMsecure Pro Trial.

Protection Status

Inbound	1 of 9 messages scanned
Spam Blocker	1 of 8 messages blocked
Feature Control	0 of 0 attempts blocked
ID Lock	0 items in myVAULT
Encryption	Accounts: unlimited

To buy Zone Labs IMsecure Pro, click here

Tutorial Click here.

IMsecure Pro is up to date ✓

What's New at Zone Labs ▷Learn More

Program	Service	Last Used
AOL Instant Mess...	AOL	in use

markmcc23 : dtweney - Instant Message

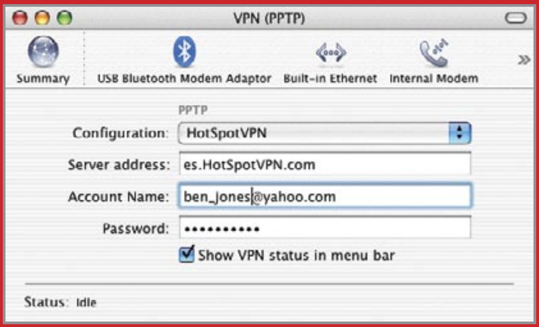
markmcc23's Warning Level: 0%

dtweney: what's up?
markmcc23: [IMsecure Pro alert: Session not encrypted because markmcc23 is not protected by IMsecure]
markmcc23: not much [IMsecure Pro alert: Potentially harmful content was removed from this message]

HotSpotVPN

WiFiConsulting	$8 per month
www.hotspotvpn.com	

If you work for a large company, chances are it can supply you with a VPN to connect to the office server so that you can access your work data with relative confidence that your information and passwords are protected. However, most of us don't have the luxury of a company VPN — and even if you do, you might not want to be checking ESPN or downloading Morrissey's new album on the company dime. Instead, give HotSpotVPN a whirl. HotSpotVPN uses PPTP (point-to-point tunneling protocol) to protect your data while it travels across public wired and wireless networks. Setup is simple: Once you sign up, HotSpotVPN sends you a server address, a login name, and password. Depending on your OS (the service works with Windows 98 and higher, Mac OS X, Pocket PC, and Linux), you can plug the server and login settings into your network preferences. The next time you connect to a public hotspot, just fire up your personal VPN and you're ready to surf in relative privacy. Because hackers have reportedly broken holes in PPTP, you shouldn't rely solely on HotSpotVPN for hotspot security. That said, most hackers probably will pass up your PPTP-protected connection for easier prey, like the ignorant sap swilling chai lattes two tables over.



Configuration: HotSpotVPN

Server address: es.HotSpotVPN.com

Account Name: ben_jones@yahoo.com

Password: ••••••••••

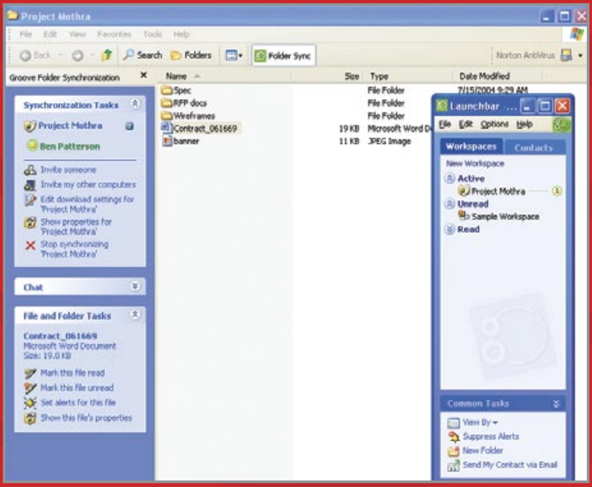
☑ Show VPN status in menu bar

Status: Idle

Groove Virtual Office

Groove Networks	$70 (File-sharing edition); $179 (Professional edition)
www.groove.net	

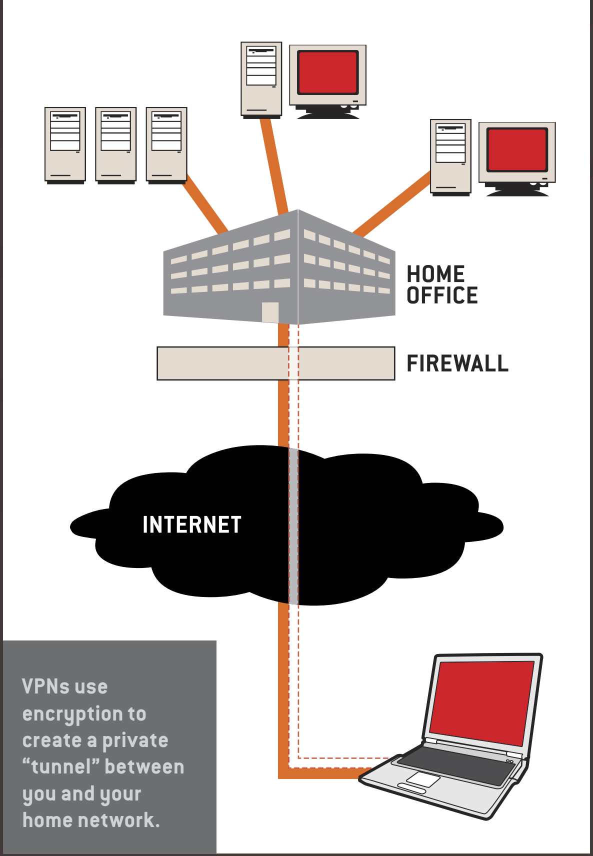
Encrypting a single file and sending it to a friend is easy enough, but when you're sharing and revising dozens of documents with a group of colleagues, the security logistics can become nightmarish. Get everyone on the same page with Groove Virtual Office, a Web collaboration app that lets you set up a secure, shared folder for your project. Once you create and name the folder, you can grant access to others and begin sharing and revising files. Virtual Office automatically downloads any changes in the shared folders to all members of the group, and you can broadcast a message to everyone or IM with individual group members. Behind the scenes, 192-bit AES encryption protects all the files, folders, and chatting from anyone who's sniffing around your public hotspot or network.



Name	Size	Type	Date Modified
Spec		File Folder	7/15/2004 9:29 AM
RFP docs		File Folder	
Wireframes		File Folder	
Contract_061669	19 KB	Microsoft Word D	
banner	11 KB	JPEG Image	

What the Heck Is a VPN?

Working within your company's local area network is like being in a fortress: You and your data are safe inside, and hackers are outside (we hope!). But if you're holed up at a Motel 6, you'll need to dig a virtual tunnel between you and your home network. A virtual private network, or VPN, creates a secure, temporary network over the Internet by encrypting both the headers and contents of your data packets. That way, hackers can't read the data you're sending, and they can't even tell where the traffic is headed. VPNs can be created with a variety of different protocols, such as IPsec (IP security) and PPTP (point-to-point tunneling protocol).

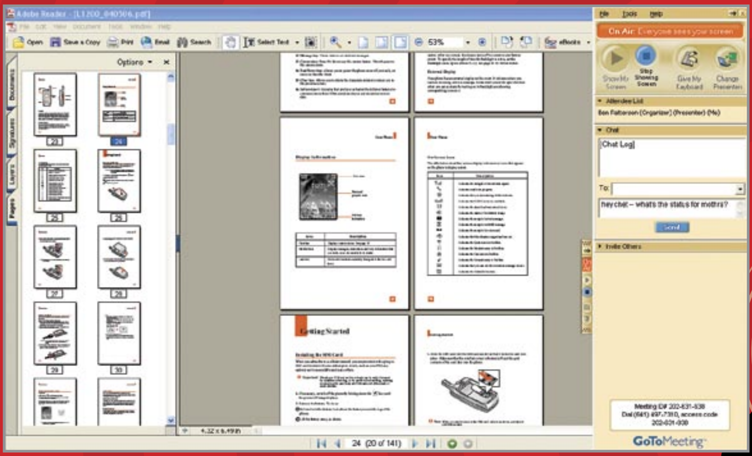


VPNs use encryption to create a private "tunnel" between you and your home network.

GoToMeeting

Citrix Online	$50 per month
www.gotomeeting.com	

Want to deliver your PowerPoint presentation to a bunch of New York analysts while sipping mai tais on the lanai of your Hawaiian hideaway? GoToMeeting (developed by the folks who made GoToMyPC) lets you invite others to a private viewing of your computer's desktop, complete with a chat interface and a list of attendees. Armed with ultrastrong 128-bit AES encryption, GoToMeeting broadcasts your keystrokes and mouse movements to everyone in the virtual meeting (but no one else), and you can even hand over temporary control of your keyboard to another presenter. The program provides a local, toll phone number and access code for conference calling, and you can send an IM to the whole group or "whisper" secrets to an individual. (We trust you enough not to use that feature for sharing insider stock tips.)



Ben Falterson (Organizer) (Presenter) (Me)

[Chat Log]

To:

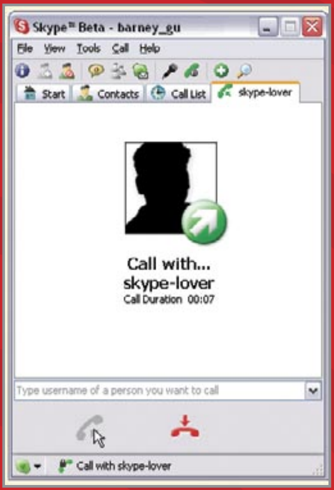
hey chet – what's the status for mothra?

Meeting ID# 202-631-638
Dial (641) 497-7310, access code 202-631-638

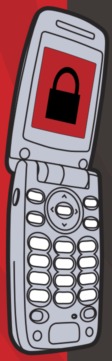
Skype

Skype Technologies	Free
www.skype.com	

Sometimes, the best way to get your point across is to just pick up the phone — a VOIP (voice over IP) phone, that is. Launched by the people who created peer-to-peer file sharing network Kazaa, Skype is a free download that lets you speak or exchange text messages with fellow Skype users. Using 256-bit AES encryption, you can chat with far-flung friends and colleagues with almost impregnable security. All you need is a headset for your notebook. (In a pinch, you can make an impromptu microphone by plugging a pair of headphones into your notebook's microphone jack, then listen through your notebook's speakers. Try it, it works!) ⊖



Call with...
skype-lover
Call Duration 00:07



Cell Phone Security

If hotspots and even wired public networks are so open to attack, how secure are cell phones and PDAs (such as BlackBerrys and Treos) that connect to corporate intranets? Older analog phones are frighteningly easy to crack — just about anyone with a police scanner can listen in. Luckily, it's much harder to eavesdrop on cell phones using digital networks, which scramble conversations across a wide range of frequencies. That said, a determined hacker with the right equipment could conceivably tap into your call, so consider using a landline if you're giving out credit card numbers or other sensitive info.

BlackBerry and Treo users with PDAs that connect to their corporate Exchange servers have much less to fear. Most networks that use BlackBerrys and Treos use either AES or triple-DES encryption for all e-mail transmissions, making for virtually uncrackable security. If you're still worried about sending private information using your PDA, ask your network administrator what kind of security your network uses.