Safeguard Your Instant Messenger

Symantec Internet Threat Meter
Instant Messaging

LOW
RISK
Use Basic Caution

No significant malicious activity
Currently there are no widespread outbreaks of malicious code circulating via instant messaging. In the past, however, some malicious code did take advantage of IM. Always use normal security precautions whenever you use IM.

How They Attack	How You Know	What To Do
Malware	• IM attachments, just like email attachments, can carry destructive viruses, Trojan horses, and worms • Some new worms use IM software to send themselves to every member of your buddy list	• Don't open attachments or click on Web links sent by someone you don't know • Don't send files over IM • If a person on your Buddy list is sending strange messages, files, or web site links, terminate your IM session • Remove viruses from IM with Norton AntiVirus
Spam	• Some Spam can contain offensive language or links to Web sites with inappropriate content	• Reject all Instant Messages from persons who are not on your Buddy list • Do not click on URL links within IM unless from a known source and expected
Vulnerabilities	• Most instant messages still travel unencrypted across the Internet, exposing private conversations to anyone who can find a way to listen in	• Never send personal information through an IM • Keep your IM software up to date • Keep your operating system and security software up to date with Norton Internet Security