

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



Malware



Spam



Vulnerabilities

How You Know

- 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
- Some Spam can contain offensive language or links to Web sites with inappropriate content
- Most instant messages still travel unencrypted across the Internet, exposing private conversations to anyone who can find a way to listen in

What To Do

- 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**
- 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
- 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**

Products

- Norton 360
- Norton Internet Security
- Norton AntiVirus
- Norton One
- Norton 360 Multi-Device
- Norton Ghost
- Norton Online Backup
- Norton Utilities
- Norton Family Premier
- Norton Mobile Security

Services

- NortonLive Services
- Ultimate Help Desk
- Spyware and Virus Removal
- Norton Safe Web

Support

- Norton Support
- Norton Update Center
- DNSChanger
- Windows 8 Security
- Windows 8 Apps

