

## **Important Security Alert To Anyone Using Instant Messaging**

According to the Radicati Group, 85% of businesses— both large and small— are now using instant messaging (IM) as a communication tool.

Unfortunately, hackers are rapidly developing ways to use IM to spread viruses and gain access to computers and networks. Instant-messaging security vendors FaceTime Communications and IMLogic Inc. have both reported an exceptionally high spike in attacks over recent months.

IM attacks work similar to e-mail viruses; the sender tries to get the user to click on a link that takes them to a website where they'll be infected with a virus, or it tries to get the user to download a file. Many of these attacks appear to be from legitimate sources or people on a "buddy" list.

Just recently, FaceTime discovered a threat on AOL's instant messenger system. They quickly contacted AOL but tens of thousands of computers had already been infected with a peer-to-peer file sharing program called BitTorrent. Hackers then used this program to upload movies to the victim's hard drive and use their computer as a vehicle for sharing it with others.

These attacks are also getting more complex. Savvy IM users will often reply to an IM and ask their buddy if the link or file sent was safe. However, hackers have now developed an intelligent bot that will actually automatically respond to the message confirming the file or link is safe. One bot actually had 6 different responses depending on the question that was asked by the user.

Just like viruses, worms, and other security threats, businesses need to put measures in place to protect themselves from these new threats. The first step is educating your employees about these threats through your employee's acceptable user policy. However, since there is always a chance someone will click on a link or download a file, education is not enough.

If you currently use IM, we urge you to contact our office about installing the proper software and security measures to make sure you don't fall victim to these growing attacks.