

Printers Gone Wild

News Story by Robert L. Scheier

JANUARY 23, 2006 ([COMPUTERWORLD](#)) - That innocent-looking printer in the corner might be gunning for you.

Because many printers and copiers have a processor, storage, an operating system and a network connection, they're as capable as a PC of launching an attack, says Mike Hawkins, associate director of networking at the University of North Carolina at Chapel Hill. Hawkins says he has seen "many, many" printers on campus used to store and download files or "used to launch attacks against other computers."

"We've found almost countless examples of where the compromise of an office productivity system, such as a printer or copier or fax, [is] used for illicit purposes," says John Roese, chief technology officer at network security vendor Enterasys Networks in Andover, Mass.

Preventing such attacks requires the same controls and monitoring as are used for PCs or servers. While copiers have inherently weak authentication, says Rose, strict policies limiting the bandwidth they can access and the network protocols they can use make them operate a less like PCs and thus a less attractive target. Other options include "placing them in a protected [virtual LAN] or behind a network gateway," says Burton Group analyst Diana Kelley.

Whatever you do, don't assume that a good printer can't go bad.