Securing your Printer

With ever increasing sophistication, printers are becoming more computer-like every day. High-end printers effectively contain computers; with processors, lots of memory, and even disk drives. These printers need to be secured in a manner similar to typical computers, especially since they're generally connected to the campus network for sharing.

The degree to which a non-secured printer may be vulnerable depends somewhat on the sophistication of the printer. On less sophisticated printers, a compromised printer may be simply an annoyance as someone else may be able to take control of your printer and block anyone else (including you!) from using it or may waste resources (i.e., make the printer print blank pages or, worse yet, waste ink or toner by printing solid pages). With more sophisticated printers, we've had instances at Lehigh where printers have been hacked. In these instances someone broke into the computer within the printer and used it for unscrupulous purposes such as sending SPAM or distributing copyrighted files.

The degree to which a printer can be secured also depends on the sophistication of the printer. For printers plugged directly into desktop computers, security is typically more of a function of the computer into which the computer is plugged. If the computer doesn't allow print sharing, the printer is most likely secure; if it does allow print sharing, that sharing should be limited through a password or limited to known computer systems.

LTS recommends working with your Computing Consultant to reserve an IP address and network name for any networked printer, and documenting a local password for it, as well as properly configuring any services it's providing. It's a very good reason to submit a request for LTS Help.

Check the documentation which came with the printer for any initial security settings. Register and periodically check with the printer manufacturer's web page for any security patches and upgrades which may become available for that printer and, once they become available, protect your printer by applying any additional security in a timely manner.