

Why Avril Lavigne is bad for business

... and other computer security advice

By **Kyle Marnoch**

Just when you thought Canadian pop-punk princess Avril Lavigne couldn't get any more exposure, a dangerous computer virus is spreading the name of the five-time Grammy nominee.

The malicious file typically comes in an e-mail carrying the subject line "FW: Avril Lavigne--CHART ATTACK!" Open the attachment, which is usually labelled AvrilLavigne.exe, and you're transported to Lavigne's website. (Pray that your PC's volume is turned down.) The program then tries to disable your anti-virus and firewall software and send itself to everyone in your e-mail address book.

While the virus isn't known to delete files on infected systems, it can cause embarrassment by spamming your clients and colleagues, says Warren Fine of Toronto-based Complete Systems Inc. And if it disables your anti-virus and firewall protection, your systems will be open to other potentially damaging attacks.

How can you protect yourself against Avril and her ilk? Here are some quick tips from security experts contacted by PROFIT:

1. **Run anti-virus software on all PCs and/or servers** to catch viruses before they're downloaded and to find any infected files already residing in your system. Fine says that popular desktop anti-virus software packages cost around \$70, but that price drops if you're licensing for several computers.
2. **Update your anti-virus software frequently.** "New viruses come out all the time," says Fine. "Information that will protect your computer from specific viruses is updated on a regular basis, and you need to download these updates from your software provider." Packages from leading anti-virus providers such as Norton and McAfee go online and update themselves automatically. If you're updating manually, Fine recommends doing this every five days.
3. **Have a security policy in place.** Because viruses can arrive through text-messaging and file-sharing programs such as ICQ or KaZaA, you should ban such non-corporate applications from office use, advises John Dempsey, support manager at Ottawa-based Sensible Security Solutions Inc. Dempsey adds that Web- based e-mail programs should be restricted because file attachments will elude your server-based anti-virus software (although properly configured software running on desktop PCs should catch viruses coming through any e-mail client.)
4. **Don't open what you don't know.** Warn your staff against opening e-mail attachments with unfamiliar names or that come from an unrecognized source. "A lot of people say, 'Hmm, I want to know what that is,' and just open it and by then it's too late'," says Dempsey. He cautions executable files (those with an .exe suffix) are the most common virus carriers.

© 2003 Kyle Marnoch