

# Defense in Depth

You may have noticed a lot of "greeting cards" recently. I hope you didn't open any of them. Most of these come from a "neighbor," "friend," "classmate," "secret admirer," "parent," or someone else without a name. You see, most of



Randy Abrams

these are being spammed out by computers infected with bots. Bots are programs that allow a remote attacker to take control of your computer and automate all kinds of activities, including sending spam.

If you opened one of these eCards then the link to the card really was a link to a worm. If you have a good antivirus program, like ESET's NOD32, the worm was probably detected. There are a variety of ways to defend against these eCard attacks. As in all areas of security, defense in depth is a very sound approach.

Your number one defense is thinking. Yes, I work for an antivirus company and I am telling you that thinking is number one. These eCards do not use the name of the person who is sending them because the computers sending them do not know who you are or who you know. The bad guys know that eCards are teaching people to open anything from anyone and then to trust it. I advise against opening any eCard at all. ECards defy all principals of safe computing. If you are going to open one, at least check with the person the card claims to be from to make sure they did send it. Opening eCards is often like opening the door when an unknown person knocks and says "let me in, I am a friend".

Anti-spam is a good layer of defense as well. Sometime malicious emails will contain a file for you to run. A large portion of these emails are blocked by anti-spam. We had a customer wondering why we detected so little malware in their email system. The reason was that their anti-spam was deleting it before the emails got to their antivirus. That's a good thing!

Antivirus is another layer of defense, but like a seatbelt, you don't want it to be needed. That doesn't mean you don't use it, but you try to avoid the "accidents" that would require it. You certainly don't close your eyes when you drive and expect your seatbelt to protect you from everything!

Thinking is your first level of defense. Anti-spam, like anti-lock brakes, can help you avoid a bunch of other accidents. Antivirus is your seatbelt. Antivirus is important to have, but you hope you don't ever actually need it.

**If you wish to submit questions or comments to "Ask the Expert" please feel free to send them to [askeset@eset.com](mailto:askeset@eset.com).**



Randy Abrams is Director of Technical Education for ESET

[AskESET@eset.com](mailto:AskESET@eset.com)

[www.eset.com](http://www.eset.com)

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.