

## Get a Valentine's Package From Your Sweetheart?

It's time for those mushy emails. Some have poems, some have jokes, and some have attachments. We've all been told not to open attachments from suspicious sources, but nobody ever talks about what truly makes an attachment or source suspicious. Security professionals may as well tell you not to run bad programs — it's about as helpful.

Email from unknown sources is easy. . . don't open any attachments, but this is just the tip of the iceberg. I happen to be the mayor of San Diego. Ok, I'm not really, but you see how easy it is to get it in print that I am? It is even easier to send an email that says it came from someone else's address. If I want to send an email that looks like it came from george.bush@whitehouse.gov it is a very easy thing to do. Viruses, spammers, and scammers alike do this all of the time. What this means to you is that you don't know who sent the email by looking at the email address it says it came from — it might not really have been sent by that person. This also means that if you are not expecting an attachment, it is suspicious no matter who sent it to you. Many viruses will scour a computer looking for email addresses and randomly substitute them in the "to" and "from" fields.

Does this mean that you can never trust an attachment? No, what this means is that **generally it is a very good idea to ask the sender if they meant to send you an attachment before you open it.** You can pick up the phone, send a text message, or email the sender, but verify the source before you open it.

If you don't verify the source you must be very certain that the attachment was deliberately sent by the person who you believe sent it. The trick to this is context and specifics. **Does it make sense that the person is sending the specific email with the specific attachment at the time it is sent?** Additionally, and at least equally important, is there anything that would indicate the message could not have been sent by someone who does not even know you?

An old worm called "ExploreZip" used a WinZip icon and would delete files when it was executed. The worm responded to unread emails in your inbox with a message that read "Hi I have received your email and I shall send you a reply ASAP. Till then take a look at the attached zipped docs." A file called ZIPPED\_FILES.EXE was attached, and was the worm which deleted files.

I knew a programmer who was expecting some files from his boss. When his boss got infected the



Randy Abrams

programmer received the worm — email message and all. The context was correct, but obviously it takes no personal knowledge to say "Hi I have received your email and I shall send you a reply ASAP. Till then take a look at the attached zipped docs." If the message had said, Please take a look at these proposals for the Hercules project and he was working on such a project, then there is a high degree of confidence that his boss actually sent the message.

**When you read an email ask yourself if the exact same email could be sent to somebody else and make equal sense?** To prove the point I once sent out an email titled "About the meeting. . ." with an attachment titled "Details.txt.vbs" and the text indicated that there was more information about the meeting in the attachment.

If a user opened the attachment it simply advised them to attend a training session I was giving. The message could easily have pertained to a few hundred million people who attend meetings every day. If I had said something like "I hope you can attend the anti-virus training session on Tuesday, Feb. 13th at 8 AM in the Orca conference room" then this is a pretty specific message. One would have a high degree of certainty that I actually did compose and send the email. It still might be considered suspicious that I would put the details in a file instead of just writing them in the body of the email though.

Close cousins to attachments are emails with links to web sites. I cringe when I get "eCards". Unless you have your browser configured for much higher than normal security, following a web link is about the same as opening an attachment. If you know people who send eCards, always insist that they include a very personalized message that makes it clear the message was generated by someone who actually knows you. You should do the same if you send these greetings.

**When you get that email from your loved one this Valentines Day, make sure it isn't from an impostor before you open the attachment or click on the link.**

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.