

# Life Skills

Only a portion of computer security is learning how it works. The larger issue is learning how to live in a society altered by the social dynamics introduced by computing and the Internet.



*Randy Abrams*

Once upon a time there were no cars. As cars became ubiquitous, elementary schools started teaching traffic safety to young children. We had crossing guards, and slogans about looking both ways before crossing the street. In high school we had courses teaching us how to drive, while some insurance companies gave reduced rates to driving course graduates. The automobile fundamentally changed our society, and our own expectations about what we needed to safely exist.

Many of the Internet attacks we see today are effective only because people can be easily tricked. We call it "Social Engineering." One of the best definitions of social engineering I have seen is "the art and science of getting people to comply with your wishes."

In other words, if I want you to run a very bad program, and then I trick you into doing so, this exemplifies the art and science of social engineering. With the advent of computers and the Internet, these types of attacks have dramatically escalated.

There are three primary reasons for the increased attacks. First, the attacker no longer confronts the victim. This often removes conscience as a factor, because when people "see" their victims it generally acts as a crime deterrent. This is akin to people who will say things in email they wouldn't say to another person's face—even if their physical safety isn't a factor. Secondly, computers and the Internet make the cost of attacking very inexpensive. For mail-based scams there was the cost of postage. For person-to-person scams there was transportation and no economy of scale. Email is virtually free and costs very little to attack 100,000 people. Finally, the Internet removes much of the risk of getting caught. When a thief faced his victim there was somebody who could identify the criminal. With the Internet, not only is there a fair degree of anonymity, but the international nature of the Web means even if the act qualifies as a crime, local law enforcement may lack the will and resources to do anything about it.

Bottom line: there are new social dynamics at work. The skills required to identify and protect against social engineering attacks need to be taught NOW - starting with elementary school. Changes in society require changes in social education.

If you wish to submit questions or comments to "Ask the Expert" 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.*