There is an "I" in Security

Oh sure, you have received one. A rather innocuous e-mail that typically starts out something like:

"URGENT - HELP ME DISTRIBUTE MY $15 MILLION TO CHARITY

IN SUMMARY: I have $15 million USD and I want you to assist me in distributing the money to charity organizations. I agree to reward you with 10% of the money for your assistance, kindness, and participation in this Godly project. This e-mail might come to you as a surprise and the temptation to ignore it as unserious could come into your mind, but please consider it a divine wish and accept it with a deep sense of humility."

I mean, after all, you are a savvy Internet user and you just KNOW that nobody is going to give you 10% of $15 million, right? I teach Enterprise Security here at Stephen F. Austin State University. Last month, right before class, I received the following e-mail (copied verbatim):

"How are you? I do hope that you receive this e-mail in good health. I am presently in Madrid, Spain to be with my ill cousin (Chloe). She is suffering from a critical medical condition and must undergo surgery to save her life. I am deeply sorry for not writing or calling you before leaving, the news of her illness arrived to me as an emergency and that she needs family support to keep her going. I hope you understand my plight and pardon me.

I want to transfer her back home to have the surgery implemented there because surgery is very expensive here. I am wondering if you can be of any assistance to me. I need about ($2,500) to make the necessary arrangement; I traveled with little money due to the short time I had to prepare for this trip and never expected things to be the way it is right now. I will surely pay you back once I get back home. I need to get her home ASAP because she is going through a lot of pain at the moment and the doctor have advised it necessary that the tumor is operated on soon to avoid anything from going wrong. I will reimburse you at my return.

Anticipating your reply at the earliest to my request! Thank you for all of your assistance."

For those of you who have not been spammed this way, it appeared to come from a Facebook friend. Seems my friend's Facebook page had been compromised—he had responded to the following e-mail:

"HELLO, your Facebook account has been suspended due to suspected compromise. Please reset your account password with the link below to reactivate your account."

My friend's compromised account let the spammer target all of his friends (using spoofed e-mail) trying to get some money from them. The fun part for me was sharing this with my class, and, over the space of a full week, playing this scammer along. First I offered to send the money direct to his wife (by the way, I knew he was not married). After a return e-mail explaining that ONLY a money order to Spain would suffice, I then offered to send the money as a direct deposit to his bank account. Over the next week, his cousin Chloe mysteriously progressed from a tumor to cancer, then to emergency abdominal surgery. I was expecting either malaria or the Black Plague next. I sent him on a wild goose chase towards the end, saying the money order was returned due to a wrong address. After about five e-mail exchanges, I finally told the scammer than he/she had provided entertainment and education for my security class. The spammer, in turn, had the class to say "good luck" on the final e-mail.

Seriously, how many scams do we get via e-mail and the Internet? I am not really the 1,000,000th visitor to the web site. I have not won a free iPad for participating in a survey. There is no magic sweepstakes that you are automatically entered in based on having an e-mail account. The IRS is not trying to send me a refund using an .aol address. FedEx did not send an executable file to me explaining why they did not complete my delivery. The Better Business Bureau is not trying to redirect me to a page to explain a "suspicious complaint" against me.

Yet, every day somebody "clicks before thinking." We often forget that our e-mail address and our Internet connections serve as a huge "ATTACK ME HERE" target to those with no scruples. No matter how good your firewall, spam filter, or antivirus software is, nothing in the world that will protect you from momentary stupidity on the part of the user. You need to have frequent education and training on how to keep yourself safe. There are SO many ways that security can be compromised by literally inviting malware or viruses onto your computer. Do not think that a quick, "I will take the online test, and get an 80% without studying," is enough. You have to be prepared and educated every time you sit down at a computer. You have to think. Indeed, you might be the "Weakest Link". You do not need an unsecured USB drive to compromise security. You have to think "E-mail and Internet Security" ALL the time, no matter where you are …

… he says, as he sits with his MacBook at Starbucks, sipping on a venti coffee with extra cream, answering e-mails, paying off a few bills, and sending this column off to the wonderful and humble staff at CrossTalk …

… using an open, unencrypted, unsecure Internet connection with at least 10 people nearby on their own computers, potentially monitoring and copying every keystroke and piece of data going into and coming out of my computer.

Go figure. It is easier to preach than to actually follow my own good advice.

But that is another column.

David A. Cook Ph.D.
Stephen F. Austin State University
E-mail: cookda@sfasu.edu