



# The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: [www.longwood.edu/infosec](http://www.longwood.edu/infosec)

February 2009



## What is e-mail harvesting ?

E-mail harvesting is an act committed by spammers to find active e-mail addresses to send their messages to. Common tactics include:

- Searching the web for posted addresses
- Asking users to "subscribe" to receive a type of message or service

## Did you participate in our first ever review of IITS policies in Blackboard?

To see what changes were made to the policies based on the comments we received:

- 1.) Log back into the course; or
- 2.) Visit [www.longwood.edu/infosec/policyreview](http://www.longwood.edu/infosec/policyreview) for more information about our IITS policy review process.

## Friends Don't Let Friends Forward Chain Letters

*Help a sick child. Search for a missing kid. Watch out for the latest computer virus. Make money by forwarding an e-mail.*

Do you ever receive chain letters in your e-mail from friends or family that make statements or claims like those above? Do you ever forward such messages on just in case they are true? While your motives in looking out for others are admirable, you should always delete chain messages as the messages generally do more harm than good.

### Chain letters often spread inaccurate information.

False warnings of new and more destructive computer viruses often circulate through these messages. While some of these messages may have a basis in reality, the details are often distorted or fabricated to create a false sense of worry. Many of the false virus warnings circulating today originated several years ago, some of them over a decade ago, and were not true then and remain untrue today. Similarly missing children warnings that may start out as true often circulate for years with details (including the name of the supposed missing child) changing over time. While the occasional chain letter may be true, the majority of these messages are false and misleading and as a result no chain letter can be trusted.

### Chain letters put your privacy at risk.

Because you have no control over where the message may go after you forward it your name and e-mail address and any other personal information you included in the forward may now be seen by others you do not know. Also, with the long lists of e-mail addresses that are circulated within chain e-mails these chains can become a target for **e-mail harvesting**.

### Chain letters often hurt those they are intended to help.

Forwarded chain mails distract attention away from real threats, needs and problems and require organizations like the American Cancer Society or Make-A-Wish Foundation to divert some of their resources to addressing these bogus chains. In addition, false missing child chain letters may desensitize us to the real AMBER Alerts that help locate missing children. Chain letters are never reliable sources of information and you should always get the facts from a trusted source.



*The Security Minute* is a monthly publication aimed at raising awareness of information security related issues and concerns. If you have any questions regarding the newsletter, please contact Melissa Short at 434-395-2034 or [shortmj@longwood.edu](mailto:shortmj@longwood.edu).