

March 21, 2014 Release # 258

-- Begin Transmission --

"DO NOT IGNORE THIS LETTER... OR YOU WILL SUFFER..."

CHAIN LETTERS

Chain letters, like virus hoaxes, depend on you, rather than on computer code, to propagate themselves.

The main types are:

- Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth
- False claims that companies are offering free flights, free mobile phones or cash rewards if you forward the email
- Jokes and pranks (e.g., the claim that the Internet would be closed for maintenance on April 1)
- On social networks like Facebook, posts asking users to share links, such as a photo of a sick infant that needs a heart transplant, or phony scares such as children being targeted with strawberry flavored drugs



Chain letters don't threaten your security, but they can waste time, spread misinformation and distract users from genuine email.

They can also create unnecessary email traffic and slow down mail servers. In some cases, the chain letter encourages people to send email to certain addresses so that they are deluged with unsolicited mail.



The solution to the chain letter problem is simple: Don't forward these messages.

For comments or inquiries email infosec@pjlhuillier.com

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCES:

- Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats*.
- <http://www.last.fm/music/BruteForce+Attack/+images/35168135>