Rebecca Avery, e-Safety Officer, August 2012

Hoax and Chain Messages

What is a Hoax or Chain Messages?

A hoax or chain message is any message (received via email, text or social networking website etc) that, either through overt instruction or through compelling content, encourages the reader to pass it on to other people. Chain messages can range from promises of money (such as lottery wins or pyramid schemes), hoax stories promising luck, answering questionnaires, donations to charities, threats to personal safety, to hoax virus alerts.

Chain/hoax messages are started and sent for many reasons. The most common reasons are for generating money, harvesting personal data (email addresses), virus attacks, clogging up computer networks or programmes or for collecting email addresses/personal information to use to send people junk and unwanted (spam) messages.

Once you forward a chain/hoax message, even to people you know, your email address or personal information can be circulated and shared amongst potentially millions of people. By forwarding chain messages on, you may also share any content such as workplaces and email address of any recipients (e.g. your friends and family).

These chain/hoax messages can easily drop into the "wrong hands", and can provide criminals, spammer or conman with valuable information - these messages can then identify people who are likely to fall for scams, and their email addresses and accounts etc can then become a target for scams and spam messages which could include illegal or inappropriate content.

Chain/hoax messages can be annoying, persuasive or offensive and sometimes threaten people and they can be very frightening to the recipient. .Some chain/hoax messages even contain illegal content and therefore by forwarding some messages you could even be committing a criminal offence.

NEVER forward anything you suspect to be a chain/hoax message. Make sure you delete the message and if it was received via email or a website then do not click on any links or open any attachments in the message as they could contain viruses or malicious software which could harm your computer.

What does a chain or hoax message look like?

Common signs to spot a message could be a hoax or chain message is:

- The message states “this is a completely true story," or “it's perfectly legal." If the author feels he or she has to make it clear, then it's probably not.
- It relates an account of events that supposedly happened to an unidentified third person (i.e., "the dear son of the neighbour of someone my friend knows.")
- It mentions well-known companies or individuals that could be logically connected to the subject matter, without providing validation that they are connected e.g. Local Police
- It offers a reward (luck, money, love etc) for simply forwarding a message, or warns of dire consequences if you don't.
- It warns of some bizarre way to contract diseases or illness, or a way to die or become seriously injured.
- It contains references to "yesterday" or "last week” or “in the area” but doesn't say exactly when or where that was. Chain/hoax messages often arrive in our inboxes looking exactly as they did months or even years ago.
- It warns that if you don’t forward the message within a certain time frame that something unpleasant will happen such as bad luck, a problem with your computer or even death. People are often motivated by extremes and we respond faster when we believe the consequences of our inaction could be swift and severe.

- After reading it, you feel angry, scared, worried, or distrustful and want to do something about it. Emotions are a strong motivator, and hoaxers know this and will do everything they can to keep you from thinking critically.
- Most importantly a hoax or chain message **asks, begs or bullies you to forward it and share with everyone you know.**

What can I do if I or someone I know receives a chain or hoax message?

The simple and most effective solution is to delete the message, but all too often people don't do that. These steps can help to keep you safe:

- Don't send anyone any money, ever who contacts you online.
- Don't forward the message to friends and family. They won't thank you for it, however good the cause purports to be, and whatever riches it promises.
- If you are send the hoax/chain message via a social networking site then ensure you report the content.
- If you are still unsure what to do you can call or report the scam/fraud to Action Fraud www.actionfraud.police.uk/report_fraud

How can I prevent Hoax or Chain Messages?

Unfortunately there are no guarantees that you or someone you know won't receive a chain or hoax message, but there are steps you can take to limit this from happening.

- **Choose an email address that is difficult for other people to guess** and don't include any identifying information such as full names, ages, or locations.
- **Don't put your email address or contact details anywhere on the Internet**, in a profile or on a personal website for example as this could be used by hoaxers or spammers.
- **Use a separate email account** to your personal/work account and when entering competitions or registering online.
- **Only give out your personal email address to family and friends**
- **Only add real life friends as contacts online**.
- **Never reply to spam, hoax or chain messages**. Even if it says 'unsubscribe' or 'Be removed from the list' do not reply, as it may just confirm your email address to the sender and may mean you get even more spam!
- **Spam filters or junk mail filters can offer some protection** by diverting suspected spam into a junk mail folder – ask your email provider about this.
- **The more replies you send to chain/hoax messages then the more you will get sent them**. Sending liking, sharing or forwarding chain or hoax messages increases your exposure to spam, scams and other unwanted contact or content.
- **If you really must forward a message on to friends and family then delete all other information from the email or message**, such as headers that contain other email addresses or footers that could identify where it has come from. Most importantly **use the BCC (Blind Carbon Copy)** option on your email system when selected the recipients as this means that the email distribution list is not public to anyone who receives the message in the future.

For more advice and information visit

- www.getsafeonline.org
- www.actionfraud.police.uk
- www.adviceguide.org.uk/england.htm
- www.truthorfiction.com www.hoax-slayer.com or www.snopes.com list common online hoaxes or urban legends which can be used to check if an email or message is genuine.