Hoaxes and other electronic ephemera:
Taming the Beast (or at least managing it).

Martin Overton,* Chek*WARE

Email: *martin@chekware.com*
WWW: ***http://chekware.com***

Tel: ***+44 (0) 7092 256799 or +44 (0) 1403 241376***

51 Cook Road,
Horsham, West Sussex,
RH12 5GJ, United Kingdom.

Abstract:
When you are responsible for the security of 1,000 to 100,000 PCs, hoaxes, chain letters, urban legends, scams and other electronic ephemera are flooding your network and causing you more grief than *real virus* outbreaks, What do you do?

This appears to be the scenario in many large companies as well as many small and medium-sized companies.

Many security officers or support staff are given the onerous task of anti-virus strategy, policy, testing, implementation and support. Many of these people are also responsible for dealing with hoaxes and their kin, in many cases this is causing more work on an already over-stretched department or individual.

For many it's a catch-22 situation. If they ignore the problem, they are wrong. If they do something and it fails, they are also wrong! Management just wants results; they want their staff working and their network bandwidth back. Add to this the changes in viruses over the last 18 months, with e-mail (worms, Trojans and viruses) that can trigger payloads on preview or opening, it's no wonder many believe the hoax virus messages that circulate in many companies.

Hoaxes and their kin are at the very least a nuisance, and in many companies they are causing major problems with wasted bandwidth, e-mail services, and lost staff time. No matter how silly a hoax is, it still hits the corporate support and infrastructure budget. Magnify this by the number of different hoaxes, etc that are circulating within a company at any one time, now add the cost trying to counter it, and the problem becomes more focused and expensive.

This paper aims to supply solutions for the above scenario and answer the questions below that many companies are asking:

- *How do I get my staff to stop sending hoaxes, etc. around?*
- *How do I stop or minimise their penetration within my company and manage them when they do get in?*
- *How can virus hoaxes, other hoaxes, chain letters, etc. be successfully defused?*
- *What other resources, sites should I use?*

This paper was written for, and presented at the 2001 Virus Bulletin conference at the Prague Hilton, Prague, Czech Republic on September 27th – 28th 2001.
I would welcome any constructive feedback on this paper and it's content.
(Martin Overton 1st October 2001)

Introduction

"You can fool all of the people some of the time. You can fool some of the people all of the time. But you can't fool all of the people all of the time."

Who would you think was the original author of the above quotation?

How many of you would say**: P.T. Barnum**? I bet a fair percentage of you did?

It appears, though, that he was not the 'originating source'. This quote has been attributed to none other than Abraham Lincoln (1809-1865)[1]. This is just a small example of how many of us take things at face value, without questioning the validity or the credentials of the person/company or other source.

"In the province of the mind, what one believes to be true either is true or becomes true." - John Lilly

I don't know about you but I used to spend more time debunking and dealing with hoaxes than dealing with real viruses. Please note the past tense, as this is not the case now, how this state of affairs was turned around is revealed in this paper.

"A rumour without a leg to stand on will get around some other way." - John Tudor

However, it seems that it is true that many companies and organisations are suffering far more from hoaxes, scams and other EE than real virus outbreaks. The quote below seems to sum up the current sate of affairs:

"At CIAC, we find that we spend much more time de-bunking hoaxes than handling real virus and Trojan incidents."

The problem has got somewhat worse over the last eighteen months or so, as we have started to see malware that does what we always told our end-users couldn't be done, and now they are starting to doubt both the Anti-Virus software and your companies own internal security staff.

So, realistically, what can we do to try and reverse this trend, or to at least manage it in a more streamlined way?

Most of (if not all) the classes covered below are considered to be 'meme viruses', that is roughly translated as 'viruses of the mind'. EE's rely on suggesting, fooling, or programming the recipient to get them pass the EE on to others, who do the same, ad nauseum!

Why call them 'viruses of the mind' or meme viruses? When the Good Times hoax first erupted on to the internet Clay Shirky stated:

'It's for real. It's an opportunistic self-replicating e-mail, which tricks its host into replicating it. Sometimes adding as many as 20,000 copies at a go. It works by finding hosts with defective parsing apparatus which prevents them from understanding that a piece of e-mail which says there is an e-mail virus and then asking them to re-mail the message to all their friends is the virus itself' *[JK97]*.

Which I think you will agree sums the problem up rather well, as does the quote below:

"Once created, a virus of the mind gains a life independent of its creator and evolves quickly to infect as many people as possible. – Richard Brodie" *[RB]*

[1] See Bartlett's http://www.bartleby.com/100/448.16.html for evidence.

Definitions

Before I outline the some of the things you can do to help yourselves, I think that it would be a good idea to look at the different classes of EE and see how they work. Let's look at the definitions first.

Ephemera

Things of short-lived relevance, transitory, fleeting, temporary nature.

Electronic Ephemera

The group (Genus) name for the all the distinct classes of EE, such as Hoax, Urban Legend, Scam, Spoof, Chain Mail, etc. All of these are only considered species of EE if they are sent/received electronically.

Meme

Pronunciation: 'mEm[2]
: an idea, behavior, style, or usage that spreads from person to person within a culture[3]

Memes (pronounced Meem) are the basic building blocks of our minds and culture, in the same way that genes are the basic building blocks of biological life. Richard Dawkins[RD] (an Oxford zoologist) has been credited with first publication of the concept of meme in his 1976 book *The Selfish Gene*.

Memes are contagious ideas, all competing for a share of our mind in a kind of Darwinian selection. As memes evolve, they become better and better at distracting and diverting us from whatever we'd really like to be doing with our lives. They are a kind of Drug of the Mind.

Memetics is the study of Memes, which is described as:

"Memetics is extending Darwinian evolution to include culture. There are several exciting conclusions from doing this, one of which is the ability to predict that ideas will spread not because they are "good ideas", but because they contain "good memes" such as danger, food and sex that push our evolutionary buttons and force us to pay attention to them"[4]

Hoaxes

[Hoaxfaq]Here's the entries from various dictionaries:

Hoax \Hoax\, n. [Prob. contr. fr. hocus, in hocus-pocus.] A deception for mockery or mischief; a deceptive trick or story; a practical joke. --Macaulay.

OR

Hoax \Hoax\, v. t. [imp. & p. p. Hoaxed; p. pr. & vb. n. Hoaxing.] To deceive by a story or a trick, for sport or mischief; to impose upon sportively. --Lamb.

OR

hoax n : deliberate trickery intended to gain an advantage [syn: fraud, fraudulence, dupery, put-on] v : subject to a hoax [syn: play a joke on]

So now you know!

---

[2] From the Merriam Webster Dictionary http://www.m-w.com/dictionary.htm
[3] Fom the Merriam Webster Dictionary http://www.m-w.com/dictionary.htm
[4] From www.memecentral.com

Hybrid Virus Hoax

This is a more unusual class, which includes Virus Hoaxes that contain some genuine information amongst the usual dire warnings. An example of this class of EE would be the SULFNBK.EXE virus hoax that appeared early in 2001.

Chain Letters/E-Mail

The following description is from the CIAC web site:

Chain letters and most hoax messages all have a similar pattern. From the older printed letters to the newer electronic kind, they all have three recognisable parts:

- ***A hook.***
- ***A threat.***
- ***A request.***

The Hook
First, there is a hook, to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl Is Dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.

The Threat
When you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. However, others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.

The Request
Finally, the request. Some older chain letters ask you to mail a dollar to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the Internet or the fact that the message is a fake, they only want you to pass it on to others.

Urban Legends

[AFU1]An urban legend:

- *appears mysteriously and spreads spontaneously in varying forms.*

- *contains elements of humour or horror (the horror often "punishes" someone who flouts society's conventions).*
- *makes good storytelling.*
- *does not have to be false, although most are. ULs often have a basis in fact, but it's their life after-the-fact (particularly in reference to the second and third points) that gives them particular interest.*

Urban folklore is not restricted to events that supposedly happened in urban areas.

Jokes and Spoofs

The following are definitions of a joke and a spoof:

Joke[5]
Pronunciation: 'jOk
Function: *noun*
1 a : something said or done to provoke laughter; *especially* **:** a brief oral narrative with a climactic humorous twist **b** (1) **:** the humorous or ridiculous element in something (2) **:** an instance of jesting **: c :** PRACTICAL JOKE
2 : something not to be taken seriously **:** a trifling matter <consider his skiing a *joke* -- Harold Callender> -- often used in negative construction <it is no *joke* to be lost in the desert>

Spoof[6]
Pronunciation: 'spüf
Function: *transitive verb*
Etymology: *Spoof*, a hoaxing game invented by Arthur Roberts died 1933 English comedian
Date: 1889
1 : DECEIVE**,** HOAX
2 : to make good-natured fun of

Scams

Scam[7]
Pronunciation: 'skam
Function: *noun*
Etymology: origin unknown
Date: 1963
: a fraudulent or deceptive act or operation <an insurance scam>

By far the most widespread scam with the most variants seen, is the ‘undying’ Nigerian Money Scam.

I have received several dozen variants of the Nigerian Money Transfer scam already this year.

However, Nigeria is not the only country mentioned, Sierra-Leone, Ivory Coast, etc. You can find most of these variants listed at: http://www.quatloos.com/cm-niger/cm-niger.htm (137 variants listed as at 6/9/01).

[5] From the Merriam Webster Dictionary http://www.m-w.com/dictionary.htm
[6] From the Merriam Webster Dictionary http://www.m-w.com/dictionary.htm
[7] From the Merriam Webster Dictionary http://www.m-w.com/dictionary.htm

Psychology:

Let's take a short detour and look at some of the motivations and the other psychological reasons that drive the creation, development and deployment of these time and bandwidth stealing EEs.

We will also look at the reasons why many people feel compelled to pass on these things.

If the human mind were simple enough to understand,
we'd be too simple to understand it. - Pat Bahn

"The fewer the facts, the stronger the opinion." - Arnold H. Glascow

"The difference between genius and stupidity is that genius has its limits." - Albert Einstein

Why Do People Create EEs

There are a number of EEs that start their life as a Joke/Spoof and the original author does not expect it to ever be taken seriously. However it appears that it is almost impossible for anyone to create an EE that some person can't or won't believe in[AOL.EXE]. It seems that however preposterous or silly an EE appears, someone out there will not see the joke and pass it on, and so it goes 'fully wild'.

"Most of the evils of life arise from man's being unable to sit still in a room." -- Blaise Pascal

"Get your facts first, and then you can distort them as much as you please." - Mark Twain

There are many possible reasons why people create EEs, but at the end of the day, "*Only the original writer knows the real reason*", but some possibilities are:

- To see how far it will go. Almost like watching a life form develop[8].
- Requires no programming skill, and is therefore an easy option compared to writing a conventional computer virus.
- Naivety.
- To harass or slander another person (include an e-mail address and ask everyone to send mail). You could call this Revenge or Reverse SPAM.
- To damage a person's or organisation's reputation, maybe even start a scare that will effect the company's share price.
- Advertising (many believe that there's no such thing as bad publicity).
- Believe that they can create a World record of some sort.
- To trick money out of people using a pyramid or similar scheme.
- To kill some other chain letter (e.g. Make Money Fast).
- For the pure mischief of it.
- Create a spoof to poke fun at a hoax or other EE.

There are a large number of other possible reasons for the creation of EEs, and indeed many of these are the same that are attributed to authors of computer viruses, such as:

- Aggression.
- Anti-establishment /pro-anarchy or other political motivations.
- Low self esteem.
- To punish others. Exact revenge in some petty way.
- Rebellion.
- Become an anti-hero or underground hero. Infamy. Peer recognition.
- Because they can.
- Because someone stood up to them and challenged their actions or behaviour.

[8] In other words: The same basic motivation that many virus writers claim.

- De-humanisation. “I only wrote it”, the victim (usually called the ‘fool’) ran/executed/forwarded it and pulled the trigger. “I just supplied the Gun”.
- Competition, peer pressure.
- Sense of belonging to an ‘underground’ or ‘alternative’ scene or society.
- Sadistic tendencies.

Why People Forward Them on:

"Man will occasionally stumble over the truth, but most of the time he will pick himself up and continue on." - Winston Churchill, British statesman and writer (1874-1965)

"It is better to remain silent and thought a fool,
than to open your mouth and remove all doubt." - Anonymous[9]

"Man is a credulous animal and must believe something.
In the absence of good grounds for belief,
he will be satisfied with bad ones." - Bertrand Russell

"Experience is the hardest kind of teacher.
It gives you the test first, and the lesson afterward." - Anonymous

Common sense is not so common. - Voltaire

EEs try to get you to pass them on to everyone you know by using a number of methods, such as social engineering or memetic programming. Most of these messages play on your need to help other people.

Here are the most common reasons why people send on EEs:

- Altruism.
- Humour.
- Fear.
- Horror.
- Greed.
- For luck.
- Caution, better to be safe than sorry.
- Self-interest.
- Modelling behaviour.[10]
- Because it said so….
- Because my boss said so…
- Because it says XYZ anti-virus in it…
- Because it came from DEF big company….
- Trust in authority.
- Lack of scepticism..
- Sense of importance or belonging.
- The Media claims that it is a real threat.

According to one website that covers EEs there are rumours that some spammers (bulk mailers of unsolicited mail) are using/creating EEs to enable harvesting of e-mail addresses. If this is true then as you can imagine, after a few generations, many of these EEs would contain hundreds of valid e-mail addresses! Of course, this could be a new hoax/urban legend….

[9] Has been attributed to Mark Twain, Abraham Lincoln and Groucho Marx….
[10] As David Harley states his paper: “*350 previous suckers can’t be wrong*” or as P.T. Barnum allegedly said "*there's a sucker born every minute*."

"Chain letters that deal in money play on people's greed and are illegal no matter what they say in the letter."

Cost

The costs associated with dealing with EEs may not, at first sight, seem to be that worrying. And indeed it isn't if you only consider the cost of handling one EE on just one machine. BUT…..when you take into account everyone that receives an EE, the small individual costs soon multiply up into some very persuasive figures.

Here's an example below from the CIAC website:

For example, if everyone on the Internet were to receive one hoax message and spend one minute reading and discarding it, the cost would be something like:
*50,000,000 people * 1/60 hour * $50/hour = $41.7 million*

Most people have seen far more than one hoax message and many people cost a business far more than $50 per hour when you add in benefits and overhead. The result is not a small number.

Probably the biggest risk for hoax messages is their ability to multiply. Most people send on the hoax messages to everyone in their address books but consider if they only sent them on to 10 people. The first person (the first generation) sends it to 10, each member of that group of 10 (the second generation) sends it to 10 others or 100 messages and so on.

Generation:	*1*	*2*	*3*	*4*	*5*	*6*
Number of Messages	*10*	*100*	*1,000*	*10,000*	*100,000*	*1,000,000*

As you can see, by the sixth generation there are a million e-mail messages being processed by our mail servers. The capacity to handle these messages must be paid for by the users or, if it is not paid for, the mail servers slow down to a crawl or crash. Note that this example only forwards the message to 10 people at each generation while people who forward real hoax messages often send them to many times that number.

Policy

A good security policy should contain a section regarding not only traditional viruses, but also virus alerts/warning and EEs, as this can go a long way in helping to manage the problem.

Set up a good Hoax policy and get it endorsed by your board. Once approved, send it to all your staff, either electronically or as an addendum to their terms and conditions of employment.
(Legal implications of doing the latter have not been checked!)

An example policy might look like[VB2000-1]:

> ***If information about a new virus threat is received this must be passed to Security [or a named contact] for verification.***
>
> ***They will then decide if a general alert should be posted, which will include a confirmation or denial of the reported threat and any further steps that are required.***
>
> ***Only Security [or named contact] are authorised to distribute virus alerts.***
>
> ***Failure to follow this policy may result in disciplinary action.***

It may be possible to include such a policy in an employees terms and conditions of employment.

(But check the actual wording with your legal advisors!)

These quotes might be useful too:

"Remember, people will judge you by your actions, not your intentions. You may have a heart of gold, but so does a hard-boiled egg." –Unknown

To refrain from action is sometimes the greatest sacrifice, and the most fruitful of all actions. - Elisabeth Leseur

"Smart is when you believe only half of what you hear. Brilliant is when you know which half to believe." - Orben's Current Comedy

"If the aborigine drafted an I.Q. test, all of Western civilisation would presumably flunk it." - Stanley Garn

Procedures

This section will try and cover the following questions mentioned in the abstract:

- *How can virus hoaxes, other hoaxes, chain letters, etc. be successfully defused?*
- *How do I get my staff to stop sending hoaxes, etc. around?*
- *How do I stop or minimise their penetration within my company and manage them when they do get in?*

Reference Sources:

The first thing you need is access to good accurate and timely information. You can either setup your own Intranet site – either using the information from other sites [with due credit and authorisation] or link to one or more good 3rd party EE reference sites.

"The greatest and noblest pleasure which we have in this world is to discover new truths, and the next is to shake off old prejudices." - Frederick II

"I use not only all the brains I have, but all I can borrow." - Woodrow Wilson

"Human history becomes more and more a race between education and catastrophe." - H. G. Wells

If you decide to run an intranet then

1. on the home page: Link to a good virus hoax site, such as :

   http://www.kumite.com/myths or just about any AV company on the web.

or:

2. I give you my permission to repost the hoax and myths information pages from the ChekWARE site on your own Intranet. You can find this at: http://chekware.com/hoax.

To do this you can use web mirroring/ripper products such as WGET:

- Use the following command to get the hoax section of my site:

  ```
  WGET –m –l1 http://chekware.com/hoax
  ```

- `WGET (win32)is available from:`
  http://www.interlog.com/~tcharron/wgetwin.html
  The Unix version is available at ftp://sunsite.auc.dk/pub/infosystems/wget/ or http://www.gnu.org/software/wget/wget.html.

Or other tools you might like to use instead that offer similar functionality include:

- SamSpade (www.samspade.org)
- HTTrack (http://www.httrack.com/page3.php)

If you use a Palm/TRGPro/Sony Clie/HandEra/HandSpring type PDA you can use the Isilo desktop tool (available at www.isilo.com) to create/install a copy of the pages onto your PDA. Just set the URL to http://chekware.com/hoax, set the link depth to 1 and you are all set.

All I ask is, if you use the pages from my site, is that you include a link back to the original EE Home page at http://chekware.com/hoax/index.htm from your local Intranet copy. You may change your *local* [Intranet] copy of the home page to facilitate a local search engine, or for internal branding purposes, etc.

The main reason I ask that you include a link to the original page on my site is that it gets updated quite frequently and therefore if you are not mirroring it at frequent enough intervals then the local Intranet copy will become out of date.

Central EE Mail Box

To stop people from sending EEs around I would suggest that you ensure you have a good solid policy and procedures for dealing with these. This should include a specific person/team that are the only ones authorised to post virus alerts.

Setup a mailbox on your internal network and ask that your staff send suspect e-mails, all virus alerts, warnings, etc. to this. Make it perfectly clear that they must not forward them to anyone else, even if asked to by their manager, or an even more senior manager, as this would be in breach of the security policy and may make them liable for disciplinary action.

Publicise this e-mail address in your security/EE policy, newsletters, staff handbook, intranet site, etc.

Make it clear that you will reply to all mail, and confirm/deny if it is a real threat, hoax or whatever. And that virus alerts/warnings etc. should only be considered valid if sent from that mail account and duly signed by the recognised authority and must include a link to full information on your Intranet site or the approved Internet EE site.

Validating a Warning

"Common sense is instinct. Enough of it is Genius." - George Bernard Shaw

The following is good solid advice from the CIAC website:

*CIAC recommends that you **DO NOT** circulate warnings without first checking with an authoritative source. Authoritative sources are your computer system security administrator, your computer incident handling team, or your antivirus vendor. Real warnings about viruses and other network problems are issued by computer security response teams (CIAC, CERT, ASSIST, NASIRC, etc.) and are digitally signed by the sending team using PGP. If you download a warning from a team's web site or validate the PGP signature, you can usually be assured that the warning is real. Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist are probably hoaxes. Warnings about new malicious code are also available at the antivirus vendors sites and at the operating system's vendor site.*

When in Doubt, Don't Send It Out.

Furthermore you should check other good reference site [such as those listed in the appendices] to make doubly sure, especially if you are going to send out an e-mail alert to all your staff [not recommended!]

If an EE does get in and someone has ignored your policy, not checked your intranet site, or your approved external site and has sent it round parts of your company, what should you do?

The answer is: identify the individual responsible, and decide what action you wish to take against them, you must at least ensure that they don't do it again! Then I'm afraid you will probably have to Spam your own staff, debunking the EE, and offering a link to more detailed advice. You should also take the opportunity to remind all staff about the security/hoax policy and the correct procedure they should follow if they receive an EE, either internally or from an external 3rd party..

"To believe with certainty, we must begin by doubting." - Polish Proverb

People

"The brain is a wonderful organ. It starts working the moment you get up in the morning and does not stop until you get into the office." - Robert Frost

First off watch out for the problem known as 'Ultracrepidarian'[RR1] which is also known as 'False Authority Syndrome'. [RR1] In plain language, these both cover the situation of "a person who gives opinions beyond his scope of knowledge." However, those suffering from this affliction rarely qualify what they say, so their opinions, unfortunately, are more often than not treated as fact.

To qualify this…..let me state that I am not an expert and that all of the information, guidelines, etc. contained in this paper come from the 'True' giants in this field as well as over a decade of personal experience in tackling malware and EEs. Without their assistance and knowledge this paper would not have been possible.

"An expert is one who knows more and more about less and less until he knows absolutely everything about nothing."

"Real Knowledge is to know the extent of one's ignorance." - Confucious

"An expert is someone who knows some of the worst mistakes that can be made in his subject and how to avoid them." - Werner Heisenberg

"It is easy enough to hold an opinion, but hard work to actually know what one is talking about." - Paul Ford

"There are two things that cannot be attacked in front: Ignorance and narrow-mindedness. They will not bear discussion." - Lord Acton

Internal People

Lets look at the corporate situation for a while. What should you do in your company?

As mentioned before, good timely and accurate information and a good security policy can go a long way to managing this problem.

Many people think that end-user education is the key to dealing with EE [as well as Malware] issues.

A number of years ago I came to the following sad conclusion [VB 96]: "*You may think that trying to educate your staff about the risk of viruses is like trying to nail jelly to a wall, and about as rewarding, and in most cases you are right. Your non-IT staff will generally be either blasé, paranoid or simply ignorant about viruses. They simply see it as not being their problem.*" Sadly the same goes for your staffs attitude to EEs.

To further support this conclusion, just take a look at the appearance, and fallout of the SULFNBK.EXE hybrid hoax and the AOL.EXE joke/spoof [in June].

I know some of you will disagree with my conclusion that end-user education is generally a waste of time. However, in my defence I would like to enter the following:

Your PC Support and other technical staff ARE worth educating, as they tend to understand the technology better and tend to be more sceptical about things that go bump in the net. Furthermore they might be interested in what you have to offer.

Some of them may want to penetrate the mystic aura that surround EEs, and may believe you when you tell them it doesn't require them to chant strange incantations over the entrails of EEs, and attend secret meetings at nodal points during the year. (Well at least they might believe the incantations part.)

If nurtured correctly, this interest may actually blossom and you may end up with another valuable member of your security or anti-virus function or team. If nothing else, it might help to spread the burden (and skills).

He who asks is a fool for five minutes,
but he who does not ask remains a fool forever. - Chinese proverb

Good timely, accurate information and a few savvy members of staff are probably the most important factors in the never-ending battle against EEs in your companies. Add a well-maintained Intranet or Internet reference site, a good EE and security policy (as covered earlier) and a central contact point for staff to send suspect e-mails too and things will improve dramatically.

Can't groups such as EVAC and AVIEN help?

Well EVAC appears to have disappeared even before it got off the ground. AVIEN is going from strength to strength, however there is no sign of them dealing with EEs, only real virus alerts.

What About Anti-Virus Vendors?

Many [if not all] major anti-virus vendors at least offer information on Virus Related EEs, but, many of these same vendors do not cover other classes of EE, such as Urban Legends, Scams, Chain E-Mails, etc.

Products?

Can the anti-virus companies do anything to help protect us?

According to my contacts at SurfControl their SuperScout Email Filter product detects many chain letters, hoaxes, etc. This feature is known as RiskFilter. SurfControl's web site describes it as:

"A unique feature that provides a pre-categorized database of content that automatically protects the organization from nuisance emails; such as, ***chain letters, get rich quick schemes****, joke lists, as well as GIF's, JPEG's, and MPEG's that contain offensive material and have spread like wildfire through email and the Internet."*

To the best of my knowledge this is the first product that specifically blocks EEs, even if it is only 80% accurate, it is a great step forward, and I expect their competitors will soon add similar features.

Most other products that offer some level of filtering, are those, which use Lexical analysis or similar technologies. These are not strictly anti-virus products as they tend to use anti-virus engines or technologies from other companies.

Use of tools that use Lexical Analysis, such as MailSweeper or MailMarshal.

These tools offer a useful and highly configurable way of stopping EEs at your mail server (both inbound and outbound). They do, however, require a good understanding of EEs, Lexical Analysis and Regular Expressions to set this up and to be maintained correctly. These types of products may also use weighting systems in conjunction with other text matching or regular expressions.

Below are some examples of weighted analysis strings:

MailMarshal
pass this FOLLOWEDBY=5 everyone
pass on FOLLOWEDBY=6 anyone
pass on FOLLOWEDBY=6 everyone
forward FOLLOWEDBY=6 everyone
email to FOLLOWEDBY=10 every
virus FOLLOWEDBY=10 pass it
please pass FOLLOWEDBY=6 as quickly
please share FOLLOWEDBY=6 everyone

Below are some examples of weighted analysis strings and Regular Expressions:

MailSweeper
pass this on .NEAR. everyone
forward to .OR. share with .NEAR. everyone
pass .OR. forward .NEAR. .REGEXP an|ever(yone)

The power of Lexical Analysis as you can see would allow searching for any words or strings. This could include:

Abusive or offensive words
VBS code commands
Spam
Mime types
Trademarks
Brand Names

However you must be aware that if used incorrectly then you may end up blocking quite innocuous and quite legitimate mail. Furthermore, if you have too many text/regular expressions then you may suffer from a noticeable or severe performance hit which may cause mail backlogs.

Heuristics

How can you spot hoaxes, scams, urban legends, etc. without spending half your life scouring the net looking for it being debunked?

Many of the classes of Electronic Ephemera have 'signatures' or standard wording that gives the game away. Let's look at some of the most common of these :

Here are four lines from four different hoaxes, can you see the trend?

- `PLEASE pass this warning along to EVERYONE in your address book` [VC]
- `Forward this to everyone in your address book` [PoF]
- `Forward this letter out to as many people as you can` [WaH]
- `Forward this to all your friends` [GT]

Most genuine virus alerts from reputable and well-respected security firms/organisations do NOT ask you to *spam* everyone you know. If a message strongly or persistently insists that you pass it on to everyone you know, then be very suspicious and DON'T.

Did it come from a real security/anti-virus firm and was it signed (PGP signature) or does it have a link to a 'real' page on the claimed originators site?

Does it use 'TEOTWAWKI'[GC1]language? Below are some examples:

- `…unparalleled in its destructive capability` [GT]
- `This virus will attach itself to your computer components and render them useless…` [RUD]
- `…your computer practically useless` [UI2]
- `…your hard disk will be infected in an irremediable way` [WU]
- `…classified by Microsoft and by McAfee the most destructive ever!` [VC]
- `AND THEN PROCEED TO DESTROY YOUR HARD DRIVE AND YOUR MODEM` [HY]

Claims that NO anti-virus or other cure exists, or is likely to exist:

- `Mcaffe affirms that no antivirus can destroy it` [WU]
- `is completely undetectable to all current anti-virus programs` [NIA]
- `…there is no remedy…` [PBR]
- `and there is no Anti-Virus program as yet which is capable of destroying it.` [BWSCR]

Other Pointers

- Lots of text in CAPITALS or lots of !!!!!!! (Exclamation marks)
- Bad grammar and poor spelling.
- The text was not actually written by the person who sent it to you, but usually from another individual or third party, such as another company and certainly not the cited source.
- Credibility by association – use of company names, such as : IBM, AOL, FCC, CIAC, BT, Demon, Microsoft, Intel…..
- Credibility by association with claimed (but often Bogus) professional, such as: Lawyer, Doctor, Judge, Police, etc.
- Credibility by association with real person, such as: Bill Gates, etc.

- Technobabble, such as…."nth-complexity infinite binary loop".
- Dire consequences if you don't pass it on….
- Statements like 'This is not a hoax', 'This is not a scam' or 'This is not an urban legend.' This usually indicates the opposite.
- States that deletion is the only cure.
- More persuasive than informational.
- Emotional buttons being pushed 'Sex', 'Greed', 'Concern', 'Fear', etc.
- Logical inconsistencies, false claims and/or violates common sense.
- Hidden or obvious jokes. Leg pulling.
- Promises of great or instant wealth for minimal/no outlay or wants your credit card number.
- If it claims to be legal, then it probably isn't.
- Lack of corroborating evidence from a 'trusted' third party.
- Signs of false authority syndrome.
- If it seems 'too good to be true' then it probably is.
- Frequently have no date or time to maximise the shelf life of the EE.
- Fake or non-existing URLs for verification. Vague date related terms 'Released yesterday', 'Just Released', 'Released Monday, Tuesday, Wednesday……etc.', 'Released this week'.

Other Resources

www.memecentral.com
http://chnm.gmu.edu/courses/magic/intro/barnum.html
http://www.electricscotland.com/history/barnum/

Chain Letters/E-mail

www.cs.rutgers.edu/~watrous/chain-letters.html
hoaxbusters.ciac.org/
urbanlegends.about.com

Hoaxes

www.vmyths.com
hoaxbusters.ciac.org/
urbanlegends.about.com

Urban Legends

www.urbanlegends.com
www.snopes.com
urbanlegends.about.com

Scams

http://www.faqs.org/faqs/net-abuse-faq/scams/
http://www.scambusters.org/index.html
http://www.quatloos.com/
http://www.umich.edu/~virus-busters/

Conclusions

The recommendations and guidelines covered in this paper have cut the re-posting of hoaxes by around 80% in one company. It has also significantly reduced the number of calls that the help desk receives about hoaxes and other related electronic ephemera.

"Never tell people how to do things. Tell them what to do,
and they will surprise you with their ingenuity." -- George S Patton

As you can see, even though EEs are not viral in the sense we usually understand, they do 'infect' people and get them to do their bidding and their replication for them. The costs of EEs can, and do, mount up to seriously large amounts of money. Nip the problem in the bud as early as possible and you can save, time, bandwidth, and most importantly your company's money.

The main thing to understand about EEs is this: *Don't panic and immediately send them on, stop….think….read it again slowly….digest and process each line…use the heuristics in this paper [and others, see references] as well as your own common sense….and if you are still in doubt, send it to an expert and let them confirm/deny it and take and act on their advice.*

Never, ever, follow the advice offered in an EE, the least you will do is waste some bandwidth and your time. The most you will do is waste hundreds or thousands of people's time, cause unnecessary worry/fear. You could also be held responsible for damage to systems owned by those people YOU have forwarded it to (if they foolishly trusted you and followed the EEs instructions forwarded by you).

There is even a possibility that YOU or your company may face legal action (although I'm not aware of any legal precedents at this time) or lose your Internet connection. If you use an ISP, by forwarding an EE on to everyone you know, you are effectively spamming, which is prohibited and clearly documented in nearly all ISP's Acceptable Use Policy, Terms of Service, or their contract with you.

Finally, EEs are here to stay, as long as there are people, there will be tall stories, urban legends, jokes, spoofs, chain mail, hoaxes and many other classes of EE. It is US that gets infected by EEs, our very minds get programmed….and many slavishly follow the program, instead of using a little common sense.

I see no solution to this problem as to regard us, the human element, as the pre-runners to EEs have been around in some shape or other since we first started to communicate with others of our species. That communication was originally verbal, we progressed to the written word when we saw the first chain mails, printing came and allowed mass-production of the fore-runners to EEs. These have currently reached their peak of evolution in this increasingly electronic era, with the advent of computers and the unexpected ubiquity of computers and the Internet everywhere, EE have blossomed and borne unexpected quantities of fruit.

You could say that EEs have now found their ideal distribution vector and things are only going to get worse with the rush towards attaching everything to everything. Fridges, freezers, phones, washing machines, PDAs, and toasters either already are, or will soon be able to receive e-mail, SMS, or the future equivalent. If you extrapolate this to a possible future, then you should really start to worry when our brains, our very bodies, are hooked up to the Internet or its successor….the final barrier for EEs will then be breached and they may not require any conscious thought for the infection/payload to trigger…..Welcome to the world of the true Meme EE….

Those of you that have read Snow Crash[SC] and/or Blood Music[BM] will know what I'm on about……Maybe now is the time for anti-virus software to transform itself into a full anti-malware solution that includes EEs, before it's too late?

"Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." - Albert Einstein

Appendix A – Example Urban Legend

Status: **False**

Subject: IT'S JUST A GREEN SNAKE
Green Garden Grass snakes can be dangerous. Yes, grass snakes, not rattlesnakes.

A couple in Rockwall, Texas had a lot of potted plants, and during a recent cold spell, the wife was bringing a lot of them indoors to protect them from a possible freeze. It turned out that a little green garden grass snake was hidden in one of the plants and when it had warmed up, it slithered out and the wife saw it go under the sofa. She let out a very loud scream. The husband, who was taking a shower, ran out into the living room naked to see what the problem was. She told him there was a snake under the sofa. He got down on the floor on his hands and knees to look for it. About that time the family dog came and cold-nosed him on the leg. He thought the snake had bitten him and he fainted. His wife thought he'd had a heart attack, so she called an ambulance. The attendants rushed in and loaded him on the stretcher and started carrying him out.

About that time the snake came out from under the sofa and the Emergency Medical Technician saw it and dropped his end of the stretcher. That's when the man broke his leg and why he is in the hospital at Garland. The wife still had the problem of the snake in the house, so she called on a neighbor man. He volunteered to capture the snake. He armed himself with a rolled-up newspaper and began poking under the couch. Soon he decided it was gone and told the woman, who sat down on the sofa in relief. But in relaxing, her hand dangled in between the cushions, where she felt the snake wriggling around. She screamed and fainted, the snake rushed back under the sofa, and the neighbor man, seeing her lying there passed out tried to use CPR to revive her.

The neighbor's wife, who had just returned from shopping at the grocery store, saw her husband's mouth on the woman's mouth and slammed her husband in the back of the head with a bag of canned goods, knocking him out and cutting his scalp to a point where it would need stitches. The noise woke the woman from her dead faint and she saw her neighbor lying on the floor with his wife bending over him, so she assumed he had been bitten by the snake. She went to the kitchen, brought back a small bottle of whiskey, and began pouring it down the man's throat.

By now the police had arrived. They saw the unconscious man, smelled the whiskey, and assumed that a drunken fight had occurred. They were about to arrest them all, when the two women tried to explain how it all happened over a little green snake. They called an ambulance, which took away the neighbor and his sobbing wife. Just then the little snake crawled out from under the couch. One of the policemen drew his gun and fired at it. He missed the snake and hit the leg of the end table that was on one side of the sofa. The table fell over and the lamp on it shattered and as the bulb broke, it started a fire in the drapes. The other policeman tried to beat out the flames and fell through the window into the yard on top of the family dog, who, startled, jumped up and raced out into the street, where an oncoming car swerved to avoid it and smashed into the parked police car and set it on fire. Meanwhile the burning drapes had spread to the walls and the entire house was blazing.

Neighbors had called the fire department and the arriving fire-truck had started raising its ladder as they were halfway down the street. The rising ladder tore out the overhead wires and put out the

electricity and disconnected the telephones in a ten-square city block area of south Rockwall along Texas State Route 205.

Time passed ..... Both men were discharged from the hospital, the house was re-built, the police acquired a new car, and all was right with their world .....

About a year later they were watching TV and the weatherman announced a cold snap for that night. The husband asked his wife if she thought they should bring in their plants for the night.
She shot him.

Appendix B – Example Spoof/Joke

VIRUS WARNING--- CIV---VIRUS WARNING---CIV---VIRUS WARNING---CIV

On April 9, 1997, Dr. V.S. Verman, head of the epidemiology unit at the Glenn Roes Hospital in Edmonton, Canada, announced that an NWT resident, whose identity was not revealed, has become the first human on record to be infected by a computer virus.

Symptoms of CIV (Computer Induced Virus) include memory loss, a bloated feeling, general sluggishness and erratic ambulation (crashing into things). Dr. Verman added that CIV also causes system disorders such as seeing noises in the next room, hearing perfume and absorbing TV signals directly into the stomach.

The patient is known to have opened a file downloaded from the internet without first checking its history and origins. How the virus moved from the file through the computer to the user remains unexplained, however, and Dr. Verman cautioned that until the transfer mechanism is better understood, computer users should protect themselves against possible CIV infection.

You can reduce the risk of CIV infection significantly, said Dr. Verman, with a few basic Safe Computing practices: use disinfectant; use a non-permeable, transparent protective membrane over the key-board; lock your floppies; avoid unnecessary licking, kissing or other intimate contact with computer parts and peripherals; and do not share your computer with others. Computer professionals and addicts, Dr. Verman advised, should wear a breathing mask with a .001 micron filter to freshen the air fanned out of the CPU. But until a cure or vaccine for CIV is found, Dr. Verman warned, the best prevention is computer abstinence. He suggested that people looking for a challenging and rewarding alternative to computering might try reading books instead.

Appendix C – Example Hybrid Hoax

FOLLOW THE INSTRUCTIONS, I HAD IT!!!!!....

I received this message from a friend today and it is true. I searched for the file by following the instructions and I found it, I had it without knowing.

Neither Norton 2001, or McAfee can detect it, I have that software installed and the virus wasn't detected.

This virus is arriving hidden inside the e-mails.

Because of this warning I could detect it (I had it without knowing) and I could delete/remove it.

Search for it by following these instructions:

1) Go to Start
2) Then Find
3) Then For Files or Folders
4) Type: sulfnbk.exe
5) Delete it (do not open it)
6) Empty Recycle Bin

Because of these instructions I have deleted/removed it...

Good luck...

Appendix D – Example Chain Mail

Subject: Angels
Date sent: Tue, 27 Mar 2001 18:29:16 -0800

Keep reading to the bottom of the page - don't stop at the feet (You'll see).

THINGS ARE NOT ALWAYS WHAT THEY SEEM

Two travelling angels stopped to spend the night in the home of a wealthy family. The family was rude and refused to let the angels stay in the mansion's guestroom. Instead the angels were given a small space in the cold basement. As they made their bed on the hard floor, the older angel saw a hole in the wall and repaired it. When the younger angel asked why, the older angel replied, "Things aren't always what they seem."

The next night the pair came to rest at the house of a very poor, but very hospitable farmer and his wife. After sharing what little food they had the couple let the angels sleep in their bed where they could have a good night's rest. When the sun came up the next morning the angels found the farmer and his wife in tears. Their only cow, whose milk had been their sole income, lay dead in the field. The younger angel was infuriated and asked the older angel how could you have let this happen? The first man had everything, yet you helped him, she accused. The second family had little but was willing to share everything, and you let the cow die.

"Things aren't always what they seem," the older angel replied. "When we stayed in the basement of the mansion, I noticed there was gold stored in that hole in the wall. Since the owner was so obsessed with greed and unwilling to share his good fortune, I sealed the wall so he wouldn't find it."

"Then last night as we slept in the farmers bed, the angel of death came for his wife. I gave him the cow instead. Things aren't always what they seem."

Sometimes that is exactly what happens when things don't turn out the way they should. If you have faith, you just need to trust that every outcome is always to your advantage. You might not know it until some time later...

Some people come into our lives and quickly go.

```
             OooO
             (  )
Some people   \ (
become friends \_) and stay awhile...
leaving beautiful footprints on our hearts...
```

```
OooO
(  ) and we are never quite the same because we have made a good
friend!!
\ (
 \_)
```

Yesterday is history.

Tomorrow a mystery.

Today is a gift.

That's why it's called the present!

I think this life is special...live and savour every moment...

This is not a dress rehearsal!

____

THIS IS A SPECIAL GUARDIAN ANGEL...

YOU MUST PASS THIS ON TO 5 PEOPLE WITHIN THE HOUR OF RECEIVING HER..AFTER YOU DO MAKE A WISH....IF YOU HAVE PASSED HER ON, YOUR WISH WILL BE GRANTED AND SHE WATCH OVER YOU FOREVER....IF NOT..HER TEARS WILL FLOW AND NO WISHES WILL BE GRANTED....

Now don't delete this message, because it comes from a very special angel.

Appendix E – Example Scam

Subject: BUSINESS PROPOSAL

From the desk of:- **MRS GRACE ITA**

C/O Barrister Chike Egobia

Lagos Nigeria

Sir,

URGENT AND CONFIDENTIAL BUSINESS PROPOSAL

I am Grace Ita (mrs) widow of the late col. Bello Ita the former governor of Kano State of Nigerian. My late husband was one of the victims of the November ADC Aircraft Boeing 722 that crashed in Lagos.

I have just been informed by family attorney Barrister Chike Egobia that my late husband operated a secret account with fictitious name in a Nigeria bank into which total sum of Nineteen Million, Five Hundred Thousand US Dollars ($19.5) was transferred and credited in his favour. The attorney now advised me to seek in confidence a foreign account into which this fund could be transferred for disbursement as directed by my late husband in his will.

It has been resolved that 25% will be your share for nominating an account for this purpose and any other assistance you will give in that regard. 10% has been mapped out to payback all local and international expenses, which may be, incurred in the transfer process and 5% has been conceded to the local bank manager here assisting facilitating the transfer.

Finally, 60% will come to myself and my children and good part of this shall be directed towards executing his will which is to buy shares and stocks in foreign country to securities his childrens future to facilitate the conclusion of this transaction if accepted do send to me promptly by fax through family attorney, the following.

1. The account number to be used for remittance
2. Name and address of your bank
3. Fax and telephone numbers, through which you will be contacted
4. Promptly whenever you attorney/ assistance may be required

Please note that i have been assured that the transaction will be concluded in ten (10) banking working days upon my receiving from you the above listed information will commence the process of retrieving the will immediately i hear from you.

May at this point emphasize the high level of confidentiality, which this business demands hope you will not betray the trust and confidence, which is reposed in you. However, you may need to give me sufficient assurance that you will not sit on this fund when it is finally remitted into your account.

Please direct your reply by email to my box in which the family attorney will communicate with him towards effective completion of this transaction.

Regards.
Grace Ita (Mrs)

Reference Papers

Dealing with internet Hoaxes/Alerts – David Harley 1997
E-Mail Abuse – Internet Chain Letters, Hoaxes and Spam – David Harley 2001
Hoaxes and Hypes – Sarah Gordon, Richard Ford & Joe Wells, Proceeding of the 1997 Virus Bulletin International Conference pp 49-66
Multiplatform Attack – In the land of the Hoaxes – Jakub Kaminski, Proceedings of the 1997 Virus Bulletin International Conference pp 197-214
Safe Hex in the 21st Century – Part 1 – Martin Overton, Virus Bulletin June 2000 pp 16-17
Safe Hex in the 21st Century – Part 2 – Martin Overton, Virus Bulletin July 2000 pp 14-15
Virus of the Mind: The New Science of the Meme - Richard Brodie, Integral Press, 1996, ISBN 0-9636001-1-7)
The Selfish Gene by Richard Dawkins Oxford Univ Pr (Trade), 1990; ISBN: 0192860925

Bibliography

[RB] Virus of the Mind: The New Science of the Meme - Richard Brodie, Integral Press, 1996, ISBN 0-9636001-1-7)
[RD] The Selfish Gene by Richard Dawkins Oxford Univ Pr (Trade); ISBN: 0192860925
[AFU1] http://www.urbanlegends.com/afu.faq/intro.html
[VB2000-1] Safe Hex in the 21st Century – Part 1, Virus Bulletin June 2000 pp 16-17
[Hoaxfaq] http://chekware.com/hoax/What_is_a_HOAX.htm
[JK97] Multiplatform Attack – In the land of the Hoaxes – Jakub Kaminski, Proceedings of the 1997 Virus Bulletin International Conference pp 197-214
[RR1] Rob Rosenberger (http://www.vmyths.com/fas/fas1.cfm)
[VC] Virtual Card
[PoF] Pictures of Family
[WaH] Win a Holiday
[GT] Good Times
[GC1] **T**he **E**nd **O**f **T**he **W**orld **A**s **W**e **K**now **I**t – shamelessly stolen from Graham Clueley
[RUD] Returned or Unable to Deliver
[UI2] Perrin.exe aka Upgrade Internet 2
[WU] WAZ UP
[HY] Hey You
[NIA] New Ice Age Virus
[PBR] PBR
[BWSCR] Bud Frogs variant
[SC] Snow Crash – Neal Stephenson Bantam Doubleday Dell Pub (Trd Pap); ISBN: 0553380958
[BM] Blood Music – Greg Bear, currently out of print.

[AOL.EXE] AOL.EXE joke/spoof, see http://chekware.com/hoax/AOL_EXE.htm