Lemming Aid and Kool Aid: Helping the Community to Help Itself Through Education

David Harley, ESET Senior Research Fellow, ESET North America
Sebastian Bortnik, Research & Technology Manager, ESET Latin America

Abstract

There's been no shortage of attempts to raise awareness of security issues in the community at large: probably everyone at a conference like AVAR has been involved in some form of security education at some time or other. But the quality and effectiveness of those attempts have been patchy at best. Are those who say that 'if education was going to work, it would have worked by now' in the right? Or is the problem with the piecemeal way that we do it?

This paper will look at a range of attempts to heighten awareness through a variety of channels initiated both from within and outside the security industry: blogging and social media, discussion forums, academic and governmental initiatives, community training schemes like the European Computer Driving Licence, inter-organizational community projects like AVIEN and AMTSO, Cyber Street and Cyber to the Citizen, and informational literature such as pamphlets, books and eBooks. We examine the advantages and pitfalls of education and training and the ethical complexities that arise when the security industry acknowledges its own responsibilities in terms of not only protecting but also informing the community, not only by self-promotion, but by finding ways to fit into a wider framework of community education and awareness.

How can we strike a balance when it comes to teaching of computer hygiene in an increasingly complex threatscape to audiences with very mixed experience and technical knowledge? Can user-friendly approaches to security be integrated into a formal, even national defensive framework?

The presentation will be divided into five main sections:

- A brief history of security education
- Channels of information (and misinformation)
- Ethics, marketing, and information
- Educational case studies
- Educational and informational coalitions

Introduction

Probably no-one at an AVAR conference believes that complete security is achievable through purely technical means, even though many administrators and end users may long for the install-and-forget solutions that overenthusiastic marketing departments sometimes claim to offer. On the other hand sometimes seems that the security industry is still thoroughly polarized into two camps [1]:

- One that believes that "If education was ever going to work, it would have done so by now"
- One that believes that "Education is the most important weapon in the security professional's armoury"

We don't think that there are many people in either camp who really believe that never attempting to teach the end user or consumer anything at *all about* security *wouldn't* have a negative impact on the global online community. However, we do think that education needs to go further than security companies enumerating their products with murmurs of 'these are what you need to buy.' Harley and Abrams have previously suggested that we don't really know if education works, because no-one has ever done it properly." [2] Perhaps that seems a little harsh, and it certainly doesn't mean that there haven't been effective education programmes – we'd like to think we've had a hand in some of them — but it's arguable that no-one has been able to devote the resources to security education that might give it a fighting chance of succeeding in eliminating security breaches except in very limited and localized contexts. In general, it's clear that current educational practice has not yet reached a point where there is no room for improvement.

Certainly, if we're only interested in strategies that are 100% successful, education isn't going to meet that criterion. But nor is any technical solution we know of. (The same, of course, applies in such disparate areas as law enforcement and healthcare: sophisticated forensic techniques and advanced medical and pharmaceutical technology have not eliminated crime and disease.) Not that we have no faith at all in technical solutions — that, after all, is the industry sector we choose to work in ourselves — but we prefer to believe that good technology is generally more effective if it's augmented by sound psychosocial practices such as education and training, policy enforcement, and so on. [3]

What, though, do we mean by education in the context of security? Primarily, raising the general awareness of information security issues sufficiently to cause them to behave in ways that offer an acceptably high standard of protection. There are no one-size-fits-all solutions here: the problems — and therefore the solutions — relevant to organizations and home users are very different, and no two companies or individuals face exactly the same problems.

In the context of corporate security, the educational and training needs of individuals within the enterprise are likely to vary even more according to where they fit into the enterprise structure, so we're not going to be able to provide a checklist solution within the confines of a (fairly) short conference paper.

While there is no point in trying to turn every staff member into a security guru, and few small organizations are likely to invest in a full-time cybersecurity officer, every organization needs someone who has enough awareness of the principles of security management and the technical issues behind it to help implement a useful security management process. While there's little we can do about the economic pressures that so often dissuade smaller organizations from investing sufficiently in security, there are at least resources available to the company that has the will to take advantage of them. There is a wide range of web sites, books, training courses, certifications, and consultancy options, even if the quality of those resources is by no means uniformly high.

What about the home user? There's certainly plenty of free information available, from many sources: the media, security vendors, government agencies, law enforcement, and more-or-less altruistically-minded individuals offering advice, product reviews and so on. Unfortunately, the quality of these resources is even more variable, and they're aimed at the sector of the community that may be least able to discriminate between good and bad advice. Especially advice that is in some sense competitive with other sources of advice.

A brief history of security education

In a paper about security education, while we must question how well are we doing it at the moment, it is also worth spending a few words on its history: how long have we been talking about information security awareness?

On November 2, 1991 Harvard University published the Information Security Handbook [4], stating that:

> An Information Security Working Group has been organized to review issues of safekeeping and confidentiality of information resources, identify risks, raise consciousness in the community and, where appropriate, develop policy statements, advisories, and guidelines.

This article makes an interesting read and helps us to understand the scope and perspective of Information Security initiatives at this time. For instance, the handbook claims that the '*already standard practices*' for physical documents should also be extended to '*electronic forms of information*'. This is almost the reverse of the current paradigm, whereby physical security can often be seen as subservient to the electronic information security field. Later on the article mentions that the handbook's goals include '*to raise community awareness to confidentiality (sic) and possible legal requirements in treatment of sensitive University information, as well as the possible liability for inappropriate uses of information resources*.'

While this is probably not the oldest document in history to take "*information security awareness*" seriously as a concept, it is nevertheless one of the first to demonstrate that — at least for large organizations — the early 1990's is the start of a growing awareness of the need for user education and awareness in cause of improving organizational security. Nevertheless, this Harvard document seems more like a specific case to determine a beginning than a real example of a popular trend. Actually, there is little evidence of massive campaigns to raise popular awareness of information security until the early 2000's, perhaps as the World Wide

Web became so pervasive as to be a global channel for raising awareness outside the workplace. Books and other resources with a more-or-less corporate slant, however, were becoming more education-oriented through the 1990s.

Security by the Book

'The Art Of Deception' [5], was possibly the first book that raised wider public awareness of the Social Engineering problem, though the term was already in common use in the specialized sense in which it's used in the security community [6]. Garfinkel and Spafford, in Practical Unix and Internet Security, observed [7]:

> Every user should have basic security awareness education ... Trained and educated users are less likely to fall for scams and social engineering attacks. They are also more likely to be happy about security measures if they understand why they are in place.

Mitnick [5] too asserts that 'the central goal of any security awareness program is to influence people to change their behavior and attitudes', an interesting definition that closely matches a more academic, less security-oriented definition of social engineering. [3]

At the same time, the NIST (National Institute of Standards and Technology) launched its Special Publication 800-50 entitled "Building an Information Technology Security Awareness and Training Program" [9] making a similar observation that

> ...a strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources.

The timing of these publications may not be accidental [9]. In early 2000's, not only was the web becoming all-pervasive, but Web 2.0 (a concept first introduced in 1999) was starting to revolutionize the Internet and the ways in which people use and interact with it. From the point of view of information security, it generates greater need for user engagement in the application of best practices that minimize the impact of cyber-attacks on systems. The new tools associated with web 2.0 give the user more power and more capabilities to change their systems, to publish and share information and to modify Internet content. However, cybercriminals were fully aware of the implications of this change and paying more attention to social engineering techniques.

In summary, the early 2000's are definitely something of a watershed in the development of information security education efforts around the globe. 15 years ago, PC penetration per capita in Europe was just 13% of the population, now it is 50% [10]. In the United States, it has grown from 57 computers per 100 users to more than 80 in 2008 [11]. It makes complete sense that user education has become more important as the user community has grown.

Let's consider how the community has worked to develop in this area over the past 15 years.

Channels of information (and misinformation)

The 'education doesn't work' position is almost invariably held by researchers, especially those with a more or less academic or hands-on-techie background: those with a grounding in direct customer support are likely to have seen from personal experience that some groups and individuals do respond well to suitably targeted training and awareness materials. [12]

Research has been cited [13] suggesting that people started to forget what they learned in training in 60–90 days. Such a short retention period could be seen as reflecting an attempt to over-teach.

> In fact, people with limited expertise often behave more "safely" than people who see themselves as proficient, because they're more likely to ask for help or advice, being less concerned with maintaining a knowledgeable image. [14]

Our own experience suggests that individuals don't actually tend to make the same mistake time and time again, though there may be some clustering in particular user groups or teaching groups. Trainers and other support-oriented staff also tend to have lower expectations when it comes to educational outcomes than do security researchers: they're less likely to think of education (whether or not it's in security) as being a one-time, one-size-fits-all, fire-and-forget solution, and more likely to think of it as an ongoing business process.

In most cases, education and training in a corporate context is not about turning end-users into world-renowned experts (whether it's in security, spreadsheets, accounting software, publishing software, or social media in marketing) but in enabling them to use available and approved tools in order to conduct business processes to the best effect. However, it's also most effective in a context that makes sense to the participant. If you want to train people to use spreadsheets as a statistical tool, teaching them to use it to compile a database of their music CDs may not be the most appropriate approach. In the case of security training, it needs to be apposite and only as detailed as it needs to be, and set in the context of a sound infrastructure embracing business processes and risks, policy and information sharing, with the intention of raising the overall standard of threat awareness and responsible, informed behaviour. That said, there's certainly an argument – several arguments – for including information that participants can carry away to help protect themselves better at home, especially in the age of BYOD [15] and security perimeters that extend right into an employee's home. [16]

When it comes to educating the home user (or even the SOHO/small business) things are very different.

Ever since it became obvious that the fledgling Internet could not rely on the goodwill of academic to academic communication and the security imposed on participating military sites, there has been a range of attempts to heighten popular awareness through a variety of channels initiated both from within and outside the information security industry. [17]

For example:

- Blogging
- Social media
- Discussion forums
- Academic and governmental initiatives
- Inter-organizational community projects

There are many excellent user-oriented security blogs, white papers, and conference papers. Including our own, we'd like to think. Within the security industry, these materials occupy a space somewhere between marketing and education, and to some extent their effectiveness is compromised accordingly. It's not that the industry can't offer excellent and impartial advice: in fact it often does. However, some of the people who would benefit most from that advice will be put off by their own assumption — or the assumptions of other people whose assessment of their own expertise may or may not be well-founded — that anyone who works for a security vendor is, first and foremost, a salesman, and probably pushing an unnecessary product.

FUD for Thought

We can't say that no security company has ever failed to resist the temptation to indulge in FUD (Fear, Uncertainty, Doubt) marketing [17], and in fact the security market is comprised of people and organizations who buy our products because they consider the financial investment preferable to the negative consequences of exposure to malicious code and other security risks. Still, most of our colleagues in the industry are fully aware that:

> *"... there is a distinct difference between meeting a demand that originates in a reasonable fear of a genuine threat (AV, insurance, flak jackets), and creating a demand that originates in ruthless exploitation of the fear of a threat that doesn't exist (fake AV, garlic and silver bullets), and offers little or no protection against real threats (malware, injury, shrapnel)."* [18]

All that said, the feedback we get from our own articles does suggest that there is a growing audience for articles that are consumer-oriented as well as for highly technical information on malware, but it's debatable how much impact they have on the community at large. Who reads security blogs written by security professionals, apart from other actual or aspirant security professionals and the media? Certainly people who don't routinely read such material may be directed by search engines (for example) to specific articles relating to specific topics and questions ("how can I stay safe on Facebook?"). In all probability, most people will not read white papers — let alone conference papers — unless they are specifically interested in the issues they deal with, and the papers are flagged by a search engine (or are referenced in an article flagged by a search engine). Nonetheless, we have to assume that good information does sometimes 'trickle down' to the end user and home user by various intermediary channels: as security professionals, we feel obliged to provide the best, most accurate information that we can.

Unfortunately, while the media are usually eager to be seen to be helping the community by spreading information, some journalists are more hindrance than help, offering recycled marketing and PR content instead of informed opinion. Understandable among generalist reporters, if not forgivable; less so among computer/technology commentators; unforgiveable when indulged in by commentators who claim to be security experts. There are, of course, journalists whose opinion is always worth considering on security issues: however, there are many whose commentary is less helpful.

Doing it by the Book

Books (either as hardcopy or some form of eBook) dealing with security issues in general are plentiful, ranging from Dummies Guides (sometimes sponsored), to academic tomes costing hundreds of dollars. Books that have found a significant audience among end users and home users and that devote significant wordage to malware issues are less common. As one of the present authors wrote elsewhere [19]:

> ... despite having written or contributed to around a dozen security-oriented books myself, I've never managed to interest a mainstream publisher in a malware-oriented book that specifically targets consumers. Perhaps it's true ... that Joe Average isn't interested enough in his own security to buy books about it, though there are enough rather bad but consumer-facing books with a little malware discussion to indicate that some publishers see a market there...

In other words, there may yet be a consumer market there as opposed to the presumed market for enterprise-oriented books on malware and malware management [13, 16] and more technical works aimed at research oriented readers. [20, 21]

One of the disadvantages of living in the age of self-publishing is that it's even easier to publish a bad book today than it was 14 years ago. Robert Slade referred in a review [22] published around that time to:

> ...a collection of mistaken, valid, useless, and repetitive information. Sharp-eyed readers will have noted the inclusion of "valid" in that list. Unfortunately, you will have to be much more acute to pick out the true facts from the volume under discussion. As the old saying goes, if you can tell good advice from bad advice, you don't need any advice.

When the author is also the publisher, the risk of such an uneven performance becomes much greater. However, the combination of technically sound content *and* a readability index suitable for a technically unsophisticated reader is hard to achieve, though there have been some good attempts in that direction. [19]

Information channels and raising awareness

At this point, we look at some academic and governmental initiatives, including inter-organizational community projects like Cyber Street and Cyber to the Citizen, and some of the informational documentation they provide.

CERTs, CSIRTs, WARPs

For a long time one of the present authors had a keen interest in the WARP (Warning, Advice and Reporting Point) [23] concept, though it may be an idea whose time has come and gone in terms of widespread adoption. A WARP is a sort of junior CERT/CSIRT ("small, personal and not-for-profit") often representing the interests of a fairly narrow community, and doesn't presume high-grade security knowledge on the part of the operator. A CSIRT is likelier to have full-time staff and responsibility for a larger constituency, though that responsibility is even more likely to be indirect due to the size and distributed nature of its user population: a good example is the Joint Academic Network (JANET) CSIRT in the UK. [24]

WARPs don't necessarily have the direct technical response capability to resolve all problems immediately, though operators may manage some form of service desk function: rather, they act as a conduit for filtered advice and warnings to the community. In principle, only the warnings most likely to be applicable to members of the client community are passed on. Clearly, this is not unlike the way that many in-house IT support teams work.

However, the WARP community [25] in the UK has attempted to implement a two-way (or even multi-way) approach, so that in the face of a reported problem, the operator can also draw on a range of experience and expertise harvested from other groups within the community ('advice brokering'). At the same time the WARP can act as a collecting point for information regarding new threats detected at local level, so that the information can be disseminated to the wider community and upward to central government agencies.

In principle, a WARP can sometimes be run very economically (in many cases, it will be shared/voluntary responsibility). Consequently, a larger organization might regard a WARP-based infrastructure as a cheap substitute for full-strength, in-house security management solution: for example, the UK's National Health Service (NHS) was moving nearly ten years ago from a centralized Threat Assessment Centre to a devolved model where individual sites would subscribe to a network of more regional WARPS. [26]

Such a substitution can entail major risks (not least of scaling) [27] but for resource-starved groups like the charity or public sectors the concept could still offer a viable alternative to having an overworked volunteer sitting at a PC trying to filter out the useful information from a data tsunami. For example, the London Connects WARP provides a Filtered Warnings Service that, according to its entry in the WARP directory [28] is the 'primary source of cyber threat-intelligence' for a number of London boroughs.

However, despite early support for the concept from SANS et al, we aren't seeing evidence of a significant global WARP movement (i.e. outside the UK), while NHS implementation seems, despite the existence of at least one regional WARP [29] seems compromised by subsequent changes in infrastructure and re-engineering of outsourced services [30]. This is to some extent reflected in the highly generic and somewhat dated advice offered.

For instance, 'Security Tips for your Infrastructure' [31] comprise eight ideas that include using and updating anti-virus, scan all files received over the Internet or on diskette, use a firewall, be careful with attachments, make backups, use strong passwords, don't publish sensitive data. Not totally invalid in principle, even if diskettes are thin on the ground in offices and stationers these days, but all expressed in stratospherically high-level terms that would (or should) be seen as teaching any moderately competent IT team how to suck eggs.

(ISC)2's Safe and Secure Online programme [32] takes a double-barrelled approach to education. Suitably screened, trained and qualified volunteers from the organization's membership visit classrooms and community groups in order to teach children aged between 7 and 14 to use online services safely, using 'interactive presentations with videos' and 'materials covering cyber safety, cyber security and cyber ethics'. It also offers a presentation for parents [33] and addresses core online security topics including cyberbullying, malware, password protection, social media and messaging. The emphasis here is on delivery by experts rather than availability of online resources. However, a two-page flyer with the '(ISC)2 Top 10 Safe and Secure Online Tips for Parents' for 'Safe and Secure Online' suggests better quality material. [34]

While there are menu options to donate to the foundation, champion the cause, or volunteer to deliver, not much of the actual material seems to be freely available. This actually seems well in accordance with the programme's stress on expert delivery, but also lessens the risk of misuse or misinterpretation of advice and data, breach of intellectual property and so on. However, by restricting dissemination to the organization itself, it offers a public relations advantage: the material is (in theory at least) always tied to the public profile of (ISC)2 itself.

We don't find anything objectionable in this: the target's exposure to the brand of vendors who take part in cooperative initiatives is one of the incentives to participate in ventures that don't have a readily quantifiable commercial benefit. (Enlightened self-interest!) However, one consequence is that the actual material doesn't seem to be freely available without the blessing of (ISC)2: you might almost describe it as semi-proprietary. There's nothing intrinsically objectionable about that, either, but it does mean a more fragmented approach than the global, cooperative approach that we think might be better in the long term.

ECDL/ICDL

Why do you need a driving licence to drive? Obviously, because most countries it's illegal to drive (at least on the public highway) without one. But why the legal constraint? The short answer, of course, is that you have to take a test (usually) to prove that you know the rules of the road and won't be a danger on the roads to yourself and others. (The longer answer embraces politics and

sociology, and perhaps a consideration of why you don't usually have to take a similar test to ride a horse or a bicycle on a public highway — according to the UK's Department of Transport, a cyclist is 30 times more likely to be seriously injured than a car occupant [35] — but isn't really germane to this discussion.) The European Computer Driving Licence (known outside Europe as the International Computer Driving Licence), despite its name, has comparatively little to do with safety — at least in terms of information security — and much more to do with general proficiency in computing at a non-specialist level.

The ECDL Foundation's mission statement [36] tells us that:

> ECDL Foundation's mission is to enable proficient use of ICT that empowers individuals, organisations and society, through the development, promotion, and delivery of quality certification programmes throughout the world.

While a driving licence authority that also licences training schemes might legitimately present a mission statement in similar terms, IT security is only one of many standard modules of the ECDL, though it could certainly be said that the notion of safe computing is (or should be!} integral to ECDL's introductory EqualSkills programme as well as to its wider-ranging e-Citizen programme. However, it isn't a compulsory module. In short, while ECDL has its attractions for an individual wanting to add to his or her marketable skills, or for an organization wishing to outsource its IT training, it's impact on the home user engaged in home-banking or using social media is relatively light.

Educational and informational coalitions

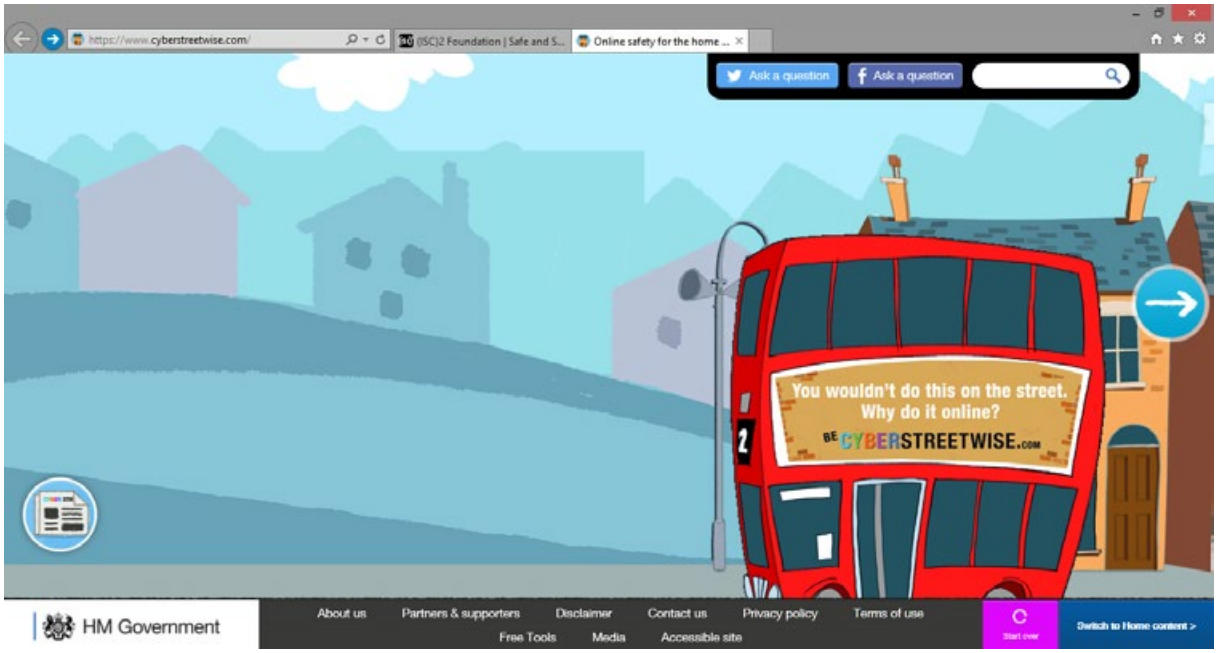
AVIEN, formerly the Anti-Virus Information Exchange Network [37], came about as the result of discussions between attendees at a Virus Bulletin conference in 2000 [38] who were specifically responsible in some measure for malware management in their respective organizations. While there was originally a certain amount of mutual distrust between AVIEN (which had strict entry criteria excluding security vendors) and the anti-virus industry (which for a while was convinced that AVIEN was involved in the unethical exchange of samples), AVIEN and its sister organization AVIEWS (for which entry restrictions were much more relaxed) eventually merged. While the group initiated a number of projects — the most successful of which were a couple of online conferences and a major book project [39] — AVIEN's target audience was corporate rather than consumer. In recent years traffic on AVIEN mailing lists has virtually ground to a halt, though the site is still updated as a blog and scam information resource, mostly concerned with tech support scams. Ironically, this gives the site more of a consumer orientation. [40]

AMTSO, the Anti-Malware Testing Standards Organization [41], remains devoted to the raising of standards in the testing of security products, and its membership comprises '...academics, reviewers, publications, testers and vendors, subject to guidelines determined by AMTSO.' AMTSO has largely focused on the provision of guidelines documents and other measures aimed primarily at testers and testing organizations, some documentation [42] is potentially useful to end users and consumers, as are some of the 'outreach' documents published and presented in magazines, at conferences and so on [43], some being made available at or via the AMTSO resources page. Attempts to engage more directly with the general public by providing a public forum and a cheap subscription that didn't carry the same privileges as full membership have met with little success to date. However, branching out into the provision of utilities that stretch the definition of testing rather further than you might expect have attracted a certain amount of attention. [44]

CPNI (the UK's Centre for the Protection of National Infrastructure) is the most recent incarnation of the government entity previously known as NISSC (the National Infrastructure Security Coordination Centre, closely associated with the development of the WARP model [45] described previously and incorporating UNIRAS — formerly described as the UK government CERT but not to be confused with CERT-UK, the UK National Computer Emergency Response Team launched in March 2014. While there is a publicly-acknowledged relationship between CIPNI and other government departments [46] and a less public relationship with the private sector (presumably with particular reference to the private companies that are considered to be part of the CNI (Critical National Infrastructure)), there seems to be no expectation that advice and warnings will be directly used by members of the public. This model seems to be characteristic not only of CERT-like organizations globally, but of law-enforcement related organizations whose performance tends to be measured by volumes of incident reports and their presumed impact on the financial damage sustained by business. [47, 48] In fact, the conflation of the issues of national security and cybercrime seems to be a persistent theme in the media nowadays. [49]

While there is a wide range of cooperative resources specifically aimed at consumers, such resources are sometimes unambitious in terms of the level of understanding they expect from their audiences.

Cyber Street [50] is an alarming example of a site that at first sight prioritizes a simplicity of graphic-heavy presentation that would make a reasonably literate 8-year-old feel patronized.



Well, you may not be too put off by the presentation, but do you consider this solid and useful information for a business seeking to improve its security?

- Install updates and antivirus software
- Use strong passwords
- Only download from trusted sites or organizations
- Beware of phishing emails
- Review and protect your business' [sic] information

And here's one of the questions offered as part of a 'Business Health Check' checklist:

> Do you know what IT equipment your business has and whether the operating systems, software and web browsers are up to date on all of them?

While there may be the occasional SMB that needs a pointer that basic to better security, we would be surprised if any business large enough to require an IT support person (even part-time or outsourced) or team has never thought that such information might be a good idea. However, slightly better information is provided by a series of links to partners: for example, clicking on the '*solicitor's office*' opens a Guide to IT Policies and Procedures, essentially a terse summary that includes links to GetSafeOnline and the Information Commissioner's Office giving basic information on the UK's Data Protection Act, a paper by one of our competitors on data loss strategy, and links to the same three information providers concerning employee training. While the linked pages alone don't provide anything like a complete guide to this aspect of business security, let alone a comprehensive list of available resources, they do at least provide a starting point. And, unlike CyberStreetWise, they also provide information in a form that is printable/cut-n-pastable for offline reference or incorporation into other resources.

Sadly, the CyberStreetWise front end for home users is equally basic to the point of oversimplification. Following the links again indicates that the site relies on its partners to provide better information. While those partners include a number of reputable information and service providers, there is little indication of the much wider range of resources beyond that circle of partners.

One of the problems with a site like the GetSafeOnline, with a wide range of partners, is that such a site may see the same issue in very different ways to its partners. For instance, its page on Viruses and Malware [51] defines the problem in terms that would cause most people at an AVAR or Virus Bulletin conference to wince:

> A **virus** is a file written with the sole intention of doing harm, or for criminal activity. There are many types of **virus** ... A **worm**, for example, can exploit security vulnerabilities to spread itself automatically to other computers through networks. A **Trojan** horse (or simply 'Trojan')

> is a program that appears harmless but hides malicious functions ... A **virus** may be designed to replicate itself ... Spyware is a type of **virus** that is specifically designed to steal information about your activity on your computer...

It's hard to imagine that the antivirus vendors who are among the organization's partners [52] would express it in quite the same terms.

Cyber to the Citizen [53] has taken on board the existence of a range of initiatives including (ISC)2 Safe and Secure [54] and Get Safe Online [55], and notes that of 'the £650M allocated to cyber security within the Strategic Defence and Security Review (SDSR) [56] in 2010' only two per cent of this money was allocated to The Department for Business, Innovation and Skills (BIS) [57] who are responsible for education, skills and professionalism and educating society.

> A cyber security marketing campaign targeted at the citizen should commence at the earliest opportunity with sufficient funds made available. Office of Cyber Security and Information Assurance (OCSIA) [58] should lead this initiative with BIS the implementers. We advocate a soft and effective campaign e.g. Think Before You Click. [59]

Rather like (ISC)2, the BCS is asking its expert members (Associate grade and above) to deliver the materials for the initiative (which it is developing in partnership with Get Safe Online), but will provide "'*event in a box*' materials including leaflets, presentations, posters and interactive tools": the slides from the launch event in January 2014 [60] give a flavour of the scope of the project, which is aimed at local community groups, schools and small businesses. [61] Looking at a standard presentation associated with the event, there's quite a lot of highly generic advice—for instance "Make sure you are on the genuine web site of the organization you wish to pay" and "Ensure the payment page is secure before entering your details" for a slide on '*Making your online payments*' but it does make a start on addressing the sort of transaction context where advice is necessary, and a qualified presenter would certainly be able to add appropriate notes and answer questions arising from such a slide. We suspect, however, that expanding on such material would make it necessary to offer a more bite-size presentation, rather than the 53-slide standard presentation.

Securing Our e-City [62], a community project with which at least two security companies and other security-minded organizations are participants, is just one example of how the security industry can provide expertise for the benefit of the community extending beyond its point of origin, and hopefully without turning it into a PR-fest for the participants.

Ethics, marketing, and information

When awareness derives from security vendors that develop products, there are always ethical dilemmas regarding the ways in which of the information is communicated. Both the senders and recipients of these communications have different ideas that may impair the effectiveness of the message.

The FUD (Fear, uncertainty and doubt) strategy is the first accusation made against many awareness campaigns when they are initiated by a security company. The idea that there is a commercial or marketing objective behind any awareness campaign is ineradicably instilled in certain sectors of society. In consequence, vendor announcements of new security threats, are often dismissed as attempts to scare users, rather than help them. We acknowledge that unfortunately there is sometimes some merit to for this accusation, but we really believe it is not usually the case. It is our intention focus on the majority, those who seek to provide real help to real users on real threats rather than prioritize their companies' marketing needs.

How do we educate the population and avoid instilling unnecessary "fear" at the same time? Is there a right way? Of course there is, in theory: to provide information as specific as possible, free from subjectivity or bias about how serious or not the situation is, and always accompanied by positive messages about good practice and including safety tips. The theory is beautiful but in practice is not nearly so simple.

Even in cases where a vendor has published all information and specific data relating to analysis of threats and threat types, and has been scrupulously careful in the wording of the communication, some readers have still regarded it with suspicion, confirming how difficult it is for a security company to impart security education. A blog comment recently observed that exemplifies this type of thinking was this: "I'd like a more independent source, they are telling us of a threat and selling us a solution in the same breath."

In the end, the marketing component is always assumed: '*you're trying to persuade me to buy your product?*' Many readers of this paper have probably heard similar comments: '*Do not tell me to install an antivirus, tell me how to protect myself*'. Leaving aside common mistrust AV marketing practice and the glib dismissal of malware-specific technology, the fact that the anti-malware industry makes products in order to protect users and goes out of its way to share good practice tips to complement the product doesn't always seem to matter, but that is the right way to proceed.

There are evident ethical complexities that arise when the security industry acknowledges its own responsibilities in terms of not only protecting but also informing the community. The ethical aspect is non-negotiable, and there is a fundamental need for security companies to avoid both the practice and appearance of scaremongering. Publications intended to raise awareness should be supplemented by accurate data and realistic examples in order to avoid any suspicion that it has been exaggerated for marketing purposes. Apart from carefully reviewing our own publications, finding ways to fit into a wider framework of community education and awareness is offers a significant opportunity to manage the ambivalence between marketing and information provision.

The (limited?) role of the security industry

We've already indicated that there may be an expanding channel for communication between security vendors and consumers, including such approaches as:

- Access to educational material built into a software package
- Informational apps for mobile devices – most of the apps made available for iOS by security vendors are informational/educational in intent rather than true security apps
- 'Tips' web sites
- Discussion forums
- Consumer-oriented informational newsletters
- Podcasts, videos and so on
- Sponsored books (ranging from sponsored Dummies books to eBooks like one of those reviewed here [19] to Peter Szor's major technical book [20].

These approaches are particularly useful for directing customers towards resources that they would not have accessed otherwise, but it's ethically responsible to ensure that resources are security-centred rather than marketing-focused, though it's too much to hope that informational resources can never include any sort of marketing agenda. [18]

The security industry's direct influence on the community as a whole is probably overestimated in ways other than those described earlier, involving popular mistrust of the industry and lack of interest in products that are seen as expensive and overhyped. Another issue that continually preoccupies us is how much of what we *do* say is lost in translation when filtered through the media, or a well-intentioned but not necessarily expert commentator (such as sometimes occurs with informational coalitions — see below). Another is that such less expert interpretation might be actively exploited by the maliciously-minded. Finally, there is a focus problem: most users of security products choose products because they perceive as working to protect them from threats. Most of our users are not looking for education or advice from us. Certainly many of them find awareness-raising information on security vendor sites and are grateful for it, but that is not what they came for. For one reason or another, and despite what many of the professionals in the industry believe, it appears that the ability of security companies to fulfil an educational role is overestimated.

But if the industry in which so much security expertise is concentrated is unable to fill the knowledge gap on its own, what's the alternative? It's our belief that security education is too important (not to mention too complex) to be left to people and organizations whose knowledge and experience of the field is so highly variable. The question is, can user-friendly approaches to security be integrated into a formal, even national defensive framework?

Although this may not accord with the ideals and opinions of many in the industry, the security community is not neither the problem nor the solution to the problem, but only a *part* of the solution. New initiatives based on a cooperative approach could lead to a new era in terms of community awareness of information security. Some of the above initiatives are already choosing this path, where the participation of the education and government sectors alongside industry professionals is beginning to make a difference.

Awareness of any other field of knowledge is at root based on school and basic primary education in most societies. From basic skills such as language or mathematics, to driving awareness, sex education or environmental care, all of these fields are greater or lesser education concerns for almost any government.

How much would know an ordinary citizen about the Highway Code or rules of the road if all they had to go by was an instruction booklet provided when they bought their car? And how much would young people know about sex education if they received that all education from the manufacturers of contraceptives? Perhaps the best that security companies can do in terms of raising universal awareness, is to point to and inform those who are the real enactors of society's educational policies.

Raising Standards

Garry Hinson's piece for the (ISC)2 blog [63] was written in 2008, but is a classic example of how workplace education can go wrong, starting with what Hinson called 'the mold of once-a-year inform-and-test'.

- An inflexible learning/testing plan, with no room for adapting to the needs and skills of the individual. 'If I had questions about password construction, for example, I had to have answered the first nine of 15 modules to get to number 10 on passwords.'
- Information lifted more or less verbatim from a disparate and sometimes contradictory assortment of materials, mostly policies and guidelines, with no concession to suitability for presentation in a training context.

- 'Idiotic' quiz questions. (See also "Phish Phailures" below.) No attempt to explain why an incorrect answer was incorrect, and it wasn't possible to return to the information pages. In Hinson's words, "In other words, this was really a quiz not an awareness activity."
- Information and questions that were "inaccurate, ambiguous or misleading, occasionally technically incorrect."

He also commented, echoing David Phillips' suggestions in the AVIEN Guide [16]:

> Maybe if it had explained why installing and updating antivirus software on my home system would help protect me and my family from identity theft, then I might just have paid more attention.

Certainly many of the problems that face corporate users also face home users. The difference is that the home user doesn't usually have an IT team to advise him or her (appropriately or otherwise) and take the blame if things go wrong, and is generally less likely to search out advice, yet may be in much more need of it.

While we can't undertake to improve the whole spectrum of security education in a single paper and presentation, we will take a couple of 'case study' areas where we can look at 'standard' advice and see if we can offer suggestions for improving it.

Phish Phailures

There's a proverb to the effect that 'if you give a man a fish, you feed him for a day: teach him to fish, and you feed him for a lifetime." Or a more security-oriented version might be: "If you show a man a phish, you prevent him from falling for that one: if you teach him to recognize phishing, you save yourself and him a lot of hassle."

However, we see time and time again unsafe practices by legitimate organizations that almost seem designed to make the phisher's life easier, such as embedding login links into unpersonalized email sent from domains with no obvious relationship to the provider's domain. So can we expect the everyday *user* of commercial services to understand how best to recognize and protect themselves against malicious activity when the *providers* of those services fail to recognize that they're making it harder to distinguish between good and bad?

We hope we can, in the absence of a better-coordinated and holistic educational initiative that would educate *everyone* who needs better awareness, not just the end user. But it would make all our lives easier if service providers were better at finding a balance between ease of use and realistic security, helping us to distinguish between Phish and Phowl.

In 2007 Harley and Lee offered a range of suggestions for recognizing phish, but also ways in which educational tools such as a generally unsatisfactory range of phishing quizzes could be more helpful and providers can better meet their responsibilities. [64] Cursory review of some of the same (and similar) quizzes while putting this paper together didn't find much improvement, but the topic probably deserves a more rigorous revisit. The continuing success of phishing generally strongly suggests that security conference papers are not going to change the world all by themselves. We can only hope to do better in future, with good research from events put on by organizations like the Anti-Phishing Working Group [65] (which works closely with other security groups including vendors) backed up by other channels of communication.

Passwords and Passing Grades

You can tell an end-user (or even a home user) that they need to use less obvious passcodes/passwords/passphrases, but you can't *force* them to. As ever, some people will respond appropriately to advice and training and will be guided by policy. Others won't and service providers need to impose restrictions where possible to prevent the use of stereotyped passcodes, just as they do (or some of them do) with passwords, offer alternatives, and offer the best (most practical) advice. Here's an example of advice from a public sector organization with a very large user population that echoes recommendations made time and time again over the last 20–30 years:

> Use strong passwords which contains the mix of different types of characters. Change your password often, and do not leave it written on a piece of paper where others may see.

It's not useless advice, though it's far from comprehensive and some contemporary thinking actually goes against the stereotypes. [66] Our view of what constitutes minimal, generic advice of organizations seeking advice is, alas, rather less minimal. [67]

In the age of Bring Your Own Device, unauthorized or inappropriate access to a device may give an attacker access to highly sensitive internal resources. So there's also a need within the enterprise to find ways to encourage and enforce sensible, security-aware behaviour when it comes to password and PIN selection strategy. And consider using alternative authentication strategies, where practical, even if your users protest about the inconvenience.

Inside and outside the workplace, it's critical that those who've embraced the 'share everything and don't worry about privacy or security' philosophy of social media are encouraged to recognize that the ready availability of so much personal and even sensitive data makes it less safe as a source of passcodes and passwords with personal meaning.

Conclusion

In a 2009 paper for the Virus Bulletin Conference, Debrosse and Harley suggested using the behaviour of the user *as well as* that of malware to train both the software and the user to be more effective at defending a system [68]. Analysing the behaviour of the user rather than (or as well as) that of executable code is a dramatically different approach to incorporating education into marketing.

However, like many of the other approaches to education discussed here, it has one major flaw: preaching to the choir is fine, but how do you preach to someone who never goes to church? That is, they are most likely to benefit someone who has already sufficiently security-aware to have bought a product. We can't ensure that everyone whose awareness needs a shot in the arm hears and acts on advice appropriate to their situation, but vendors can (individually and cooperatively) think more holistically about their responsibility to provide education. Not only in semi-proprietary contexts such as blogs and papers, but by participating in multi-disciplinary forums and community projects.

Advances in security technology have not eliminated cybercrime: rather, they've resulted in tactical review and engineering by the bad guys, accelerated evolution of malicious technologies, and the increased use of legitimate technologies for criminal purposes. Clearly, it's naïve to expect that user education – even good user education — can reach some kind of optimal point where there's no further reason to keep working at it. As previously asserted [14]:

> Technology often gives us significant respite from serious security problems. However, solving social problems with technology is rather like treating an irreversible condition with pain relief. It might work some of the time for some people, but it treats a symptom rather than a condition. Of course, sometimes, treating the symptom is the only option available.

Sadly, the same is true of education. Consider, for example, how sophisticated (some) phishing attacks are compared to those of a decade ago. [69]

In an article in Virus Bulletin, Eddy Willems concluded "If we want to change people's behaviour and reduce the attractiveness of becoming a virus writer or hacker, we must start ethical computer education at a much earlier age ..." [70] In a later paper, we took this position as a starting point, but contended that we should think more globally [71] commenting that "Other issues that need to be addressed include the reliance of teachers and parents who rarely happen to be security experts on a wide range of conflicting information from many sources, including "official" teaching materials and government web sites."

We acknowledge that 'the central goal of any security awareness program is to influence people to change their behavior and attitudes' [3] and there's no denying the importance of teaching people of all ages to behave as ethically and morally online as we'd like them to in the 'real' world. [73] On the other hand, the continuing success rates of cyber threats give weight to claims that 'security education do not work'. There are nevertheless reasons to be cheerful, or at least to remain hopeful.

It is not possible to teach the entire world about new threats and remedial practices on a day-to-day basis, and at the same fast rate at which new technologies are adopted. On the other hand, most of the people that have ever received awareness-raising advice are likely to change *something* in the short term, so it is probably a matter of how frequently they receive the message in order to reinforce the lesson and sustain change. (Bearing in mind that an overfamiliar message may actually dull the recipient's receptivity.) Finally, holistic integration with other approaches to security awareness and enhancement is still needed: the information security community cannot do it by themselves, and improved cooperation and information exchange with other key actors should be encouraged.

We believe that these approaches (and some patience) will bring us to a not-so-distant future where information security is not only something that really matters to the community, but something that even home users can realistically achieve.

References

[1] David Harley, 'Education, Education and Education'; (ISC)2, 2008; http://blog.isc2.org/isc2_blog/2008/06/education-educa.html

[2] Randy Abrams & David Harley, 'People Patching: is User Education of any use at all?', AVAR Conference Proceedings, 2008; http://www.welivesecurity.com/media_files/white-papers/People_Patching.pdf

[3] David Harley, 'Re-floating the Titanic: Dealing with Social Engineering Attacks', EICAR, 1998; http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf

[4] http://all.net/books/document/harvard.html

[5] Kevin D. Mitnick and William L. Simon, 'The Art of Deception', Wiley, 2002.

[6] Stephen Cobb: 'The NCSA Guide to PC and LAN security, McGraw-Hill, 1996

[7] Garfinkel & Spafford, Practical Unix Security/Practical Unix and Internet Security, O'Reilly, 1991/1996

[8] http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[9] Rebecca Herold, 'Managing an Information Security and Privacy Awareness and Training Program, Second Edition', CRC Press, 2004/2011; http://www.crcpress.com/product/isbn/9781439815458

[10] http://www.statista.com/statistics/203667/pc-penetration-per-capita-in-western-europe-since-2000/
[11] http://www.econstats.com/wdi/wdiv_597.htm
[12] David Harley, 'Education, Education and Education', (ISC)2, 2008; http://blog.isc2.org/isc2_blog/2008/06/education-educa.html
[13] David Harley, Robert Slade, and Urs Gattiker, in 'Viruses Revealed', Osborne, 2001; http://geekpeninsula.wordpress.com/security-books/
[14] Randy Abrams & David Harley; 'People Patching: is User Education of any use at all?', AVAR Conference Proceedings, 2008; http://www.welivesecurity.com/media_files/white-papers/People_Patching.pdf
[15] Righard Zwienenberg, "BYOD: (B)rought (Y)our (O)wn (Destruction), Virus Bulletin Conference Proceedings, 2012; http://go.eset.com/us/resources/white-papers/Zwienenberg-VB2012.pdf
[16] David Phillips, in 'The AVIEN Malware Defense Guide' ed. Harley, Syngress, 2007; http://geekpeninsula.wordpress.com/security-books/
[17] David Harley & Randy Abrams, 'Malware, Marketing and Education: Soundbites or Sound Practice?', AVAR Conference Proceedings, 2009; http://www.welivesecurity.com/media_files/white-papers/Malware_Marketing_and_Education_Soundbites_or_Sound_Practice.pdf
[18] David Harley, 'Security Software & Rogue Economics: New Technology or New Marketing?', EICAR Conference Proceedings, 2011; http://geekpeninsula.wordpress.com/2013/06/26/eicar-paper-9-security-software-rogue-economics-new-technology-or-new-marketing/
[19] David Harley, 'Don't Forget to Write', Virus Bulletin, February 2014; http://geekpeninsula.wordpress.com/2014/05/02/vb-article-dont-forget-to-write/
[20] Peter Szor, 'The Art of Computer Virus Research and Defense', Addison-Wesley/Symantec Press, 2005; http://www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543
[21] Aleksandr Matrosov and Eugene Rodionov: 'Bootkits and Rootkits'; No Starch, publication due in 2015
[22] Robert Slade, Risks Digest, Vol. 21 Issue 10, 7th November 2010; http://catless.ncl.ac.uk/Risks/21.10.html#subj11
[23] https://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/WARPs.aspx
[24] https://www.ja.net/products-services/janet-connect/csirt
[25] http://www.warp.gov.uk/directory-map.html
[26] https://warpnetwork.org/wmnhswarp/
[27] David Harley: 'WARPed and Proud of it', (ISC)2, 2008; http://blog.isc2.org/isc2_blog/2008/06/testing-our-pat.html
[28] http://www.warp.gov.uk/directory-lcwarp.html
[29] https://warpnetwork.org/wmnhswarp/aboutus.html
[30] http://www.microsoft.com/health/en-gb/Pages/index.aspx
[31] https://warpnetwork.org/wmnhswarp/securitytips.html
[32] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/SSO-Trifold-Brochure.pdf
[33] https://www.isc2cares.org/internet-security-for-kids-parents/
[34] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/top-ten-tips.pdf
[35] https://www.gov.uk/government/publications/think-cyclist
[36] http://www.ecdl.org/index.jsp?p=93&n=94
[37] http://avien.net/
[38] Robert Vibert, in 'The AVIEN Malware Defense Guide' ed. Harley, Syngress, 2007; http://geekpeninsula.wordpress.com/security-books/
[39] Martin Overton, 'Birds of a Feather', Virus Bulletin, November 2007; https://www.virusbtn.com/virusbulletin/archive/2007/11/vb200711-AVIEN-malware-defense
[40] http://en.wikipedia.org/wiki/AVIEN
[41] http://amtso.org/

[42] http://www.amtso.org/released/20081031_AMTSO_Fundamental_Principles_of_Testing.pdf
[43] David Harley, 'AMTSOlutely Fabulous', Virus Bulletin, January 2010; https://www.virusbtn.com/virusbulletin/archive/2010/01/vb201001-AMTSO
[44] David Harley, 'Feature Checking: from EICAR to AMTSO'; Anti-Malware Testing, 2013; http://antimalwaretesting.wordpress.com/2013/06/05/feature-checking-from-eicar-to-amtso/
[45] http://www.warp.gov.uk/downloads/InfoSharingflyer.pdf
[46] http://www.cpni.gov.uk/about/Who-we-work-with/
[47] David Harley, 'Cybercrime, Cyberpolicing, and the Public', WeLiveSecurity, 2012; http://www.welivesecurity.com/2012/02/14/cybercrime-cyberpolicing-and-the-public/
[48] Rob Waugh: 'UK Cyber-Security Strategy Beginning to Deliver Benefits', WeLiveSecurity, 2013; http://www.welivesecurity.com/2013/02/07/uk-cyber-security-strategy-beginning-to-deliver-benefits/
[49] http://www.globalscape.com/blog/2014/6/2/cybercrime-a-bigger-national-security-threat-than-terrorism
[50] https://www.cyberstreetwise.com/
[51] https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/
[52] https://www.getsafeonline.org/partners-and-supporters/
[53] http://policy.bcs.org/position_statements/taking-cyber-security-citizen
[54] https://cyberexchange.isc2.org/safe-secure.aspx
[55] http://www.getsafeonline.org/
[56] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62500/Factsheet18-Cyber-Security.pdf
[57] http://www.bis.gov.uk/
[58] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[59] http://www.efinancialnews.com/story/2012-04-26/kevin-slavin-think-before-you-click-algorithm-trading
[60] http://policy.bcs.org/sites/policy.bcs.org/files/Cyber%20to%20the%20Citizen%20slides%20FINAL.pdf
[61] http://policy.bcs.org/getsafeonline
[62] http://securingourecity.org/
[63] Gary Hinson, 'Security Awareness: a "How not to do it" Guide', (ISC)2, 2008; http://blog.isc2.org/isc2_blog/2008/06/security-awaren.html
[64] David Harley and Andrew Lee, 'Phish Phodder: is User Education Helping or Hindering?', Virus Bulletin Conference, 2007; http://geekpeninsula.files.wordpress.com/2013/04/davidharleyandrewleevb2007.pdf
[65] http://apwg.com/
[66] David Harley, 'Shaggy Dogma: Passwords and Social Overengineering', WeLiveSecurity, 2014; http://www.welivesecurity.com/2014/07/23/shaggy-dogma-passwords-social-engineering/
[67] David Harley, 'Education and Privacy: PIN and Passphrase Selection Strategies', presentation for Cybercrime Forensics Education and Training Conference, 2014
[68] Jeff Debrosse & David Harley, 2009, 'Malice Through the Looking Glass: Behaviour Analysis for the Next Decade', Virus Bulletin Conference, 2009; http://geekpeninsula.wordpress.com/2013/04/04/virus-bulletin-conference-papers-8-9/
[69] http://www.ibtimes.co.uk/new-operation-emmental-malware-campaign-targeting-banks-various-european-countries-1458575
[70] Eddy Willems, "The End of Cybercrime?", Virus Bulletin, August 2004
[71] David Harley, Eddy Willems and Judith Harley, 'Teach Your Children Well: ICT Security and the Younger Generation', Virus Bulletin Conference 2005; http://geekpeninsula.files.wordpress.com/2013/04/teach-your-children-well1.pdf
[72] David Harley and Judith Harley, in 'The AVIEN Malware Defense Guide' ed. Harley, Syngress, 2007; http://geekpeninsula.wordpress.com/security-books/