People Patching

Is user education of any use at all?

Randy Abrams
David Harley, BA, CISSP, FBCS, CITP

This paper was written for and presented at the 11th Annual AVAR (Association of anti-Virus Asia Researchers) International Conference in New Delhi in 2008.

Table of Contents

Abstract

In general, the anti-malware community splits dramatically into two camps when it comes to the evergreen debate about the effectiveness of user education and security awareness as a protective measure. One camp argues that "if education was of any use, it would have worked by now": the other says that "education is key" and "you can't fix social problems with technological solutions".

Is the answer out there in No Man's Land? We don't believe that there is a 100% solution that will "fix" internet lawlessness, let alone human nature (if there is, it probably isn't education). We do, however, believe, based on our own observations and experience with very large user populations, that properly targeted and implemented education and training, supplemented by other non-technological approaches such as sound policy enforcement, can play a vital part in a multi-layered defensive strategy. In this paper we will therefore consider:

(1) The arguments for and against devoting resources to education, training and security awareness

(2) Approaches to integrating social, less-technological approaches to security into a formal defensive framework

(3) User-friendly approaches to teaching computer hygiene to audiences with very mixed experience and technical knowledge.

While we will, mindful of our own experience and the focus of the conference, be addressing the role of education in malware management in particular, we believe the general principles we'll be discussing are applicable across the whole range of computer security.

Introduction

There are two extremes of viewpoint held in security, whether from a corporate management point of view, or from the more rarified atmosphere of academia or practical security research. In the red corner, the "Education isn't going to work as a security measure because it never has yet" argument: in the blue corner, the view that education is a key component of security strategy.

In real life, there is an element of truth to both extremes of this particular continuum.

Clearly, user education hasn't worked, if the aim of education is to eliminate security breaches. The comparatively small and localized breaches that preceded the near-universal adoption of the internet have not been eliminated: in fact, quite the contrary. Transient but seriously debilitating attacks on early internet connectivity, as represented by the Morris worm of 1988, heralded an ever-increasing volume and scope of security breaches across

the online world (mass mailers, phishing attacks, network/internetwork worms, botnets). Education (global and user-targeted) has failed in the same way that medicine has failed to eliminate disease, or that many millennia of law enforcement evolution has failed to eradicate more traditional forms of crime.[1]

These two analogies are not drawn entirely randomly. Medical and related biological research has, especially in the past few centuries, evolved at an unprecedented rate, resulting in the near-elimination of older forms of disease, yet must continue to meet new challenges such as viral epidemics. Law-enforcement agencies, likewise, have moved into areas of technology that seemed inconceivable ten or fifteen years ago, yet must continue to play catch-up with criminals who have similarly learned to translate their core "businesses" from the real to virtual worlds. What is described as a failure on the part of user education is actually one aspect of the failure of education in a broader sense – that is, socialization in the sense of moral, religious and ethical education, and making the population at large aware of the realities of the world around us. Since education in this global sense has failed to eliminate the universal causes of crime (poverty, complete insensitivity to the rights and property of others, inability to recognize or act in accordance with the more-or-less accepted moral and legal frameworks by which we are expected to live), it's unsurprising that the education of end-users, management, and even the security community hasn't done any better.

It seems to us equally clear that if education has failed, so has the alternative. Advances in security technology have not eliminated cybercrime: rather, they've resulted in the accelerated evolution of malicious technologies, or the use of legitimate technologies for criminal purposes.

The Argument for Technology

Technological solutions are a viable approach – sometimes the only viable approach – to solving technological problems. Most of the problems we currently face in information security in general and anti-malware in particular have a technological dimension, so we are able to counter (if not eradicate) them with technical solutions. For instance:

- Macro viruses have largely disappeared, due at least in part to changes in the implementation of macro technology in Microsoft Office products, extensive signature detection, and so on.
- Boot sector infectors have largely disappeared (despite the occasional recent spike in detections of Stoned.Angelina, for instance): again, signature detection, advances in PC technology that have all but eliminated the need for floppy disks, better CMOS and BIOS configuration options, and so on, have contributed to this amelioration.
- Traditional mass mailers like those that dominated the malware scene earlier in this decade have largely disappeared except among computer users who continue to use unprotected machines [Half-yearly report]: again, such measures as signature detection (who'd have believed there was so much life left in a reputedly discredited

technology?), filtering of executable attachments, more rational gateway configuration options that reduce the impact of backscatter have helped here.

- Hobbyist virus writers and groups have pretty much disappeared: much of that is to do with the discovery that malware actually pays, but the sophisticated Proof-of-Concept (PoC) virus for the sake of peer recognition and bragging rights has become comparatively insignificant.

Unfortunately, these positive outcomes have not eradicated the malware problem. Increasingly sophisticated solutions such as behavior analysis, advanced heuristics, in-the-cloud computing, whitelisting and so on, have forced the bad guys to review and re-engineer their tactics, but have not put them out of business (and "business" is very much the operative word). Clearly, technology is no better at hitting the "100% successful" target than education. Of course, the ping-pong match between good guys and bad guys will continue, and technology will continue to evolve to meet new challenges: so why would we assume user education to be as good as it's every going to be?

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.

The Argument for Education

It is often argued that when even the superbrains of the information security community can't get everything right, it's not reasonable to expect the wider community of non-specialists and end-users to do better. That's perfectly true. But unless you can take all the decisions for these groups – or, even more difficult, produce technical solutions that render decision-making unnecessary at the user level – and ignoring the fact that many groups want to make their own decisions, system managers and administrators still have an incentive (and, often a statutory obligation) to try to help the end-user to make the right decision at least part of the time. The objective is not to make the average user do better, or even as well as the power user, the objective is to make the average user significantly better than the average user is today.

User education is often effective. If it's done well, a significant proportion of the target audience will learn enough to reduce their vulnerability and that of organizations they belong to. What education cannot be is The Answer™. There is no single, all-or-nothing solution, but sound user education can be a significant component of The Answer™.

User education is also an essential part of sociological evolution. The threats we face on the internet are not new in concept: only in technological implementation. Social engineering attacks have been around since well before Helen of Troy. However, the economy of scale in the execution of such attacks was so relatively small that widespread education in recognition of the techniques used was not deemed necessary. The story of the Trojan horse

has been taught for centuries as history and as a metaphor, but not seen as an illustration of one of the integral risks of everyday life. The Internet has resulted in an exponential increase in the use of social engineering attacks to the point where knowledge of how these attacks are perpetrated is a required life skill in contemporary society.

For several millennia technology has failed to solve the vast majority of social problems. Security education will not realize its potential until the social aspects involved in the exploitation of a highly automated technology are taught at an elementary school level by knowledgeable teachers. Fire drills in schools are repeated at frequent intervals. To expect security education to work as a one-shot approach requires a level of naivety orders of magnitude greater than that of the person who falls for a 419 scam.

Defense in Depth: Integrating Technology and Education

We do not believe that user education has failed: only that it has failed to eradicate security problems. The measure by which the "anti-education" faction judge education to be successful is far more demanding than their own measure of how successful a technological solution needs to be in order to be deemed valuable. The very concept of defense-in-depth embraced by both those who advocate and those who eschew education is founded on incremental gains in security.

Nobody expects schools to eliminate worldwide ignorance, yet an incremental gain in academic attainment and interpersonal intelligence is deemed worthwhile. To return to a previously used metaphor, we don't usually decline to treat a headache because aspirin doesn't cure the underlying condition, and we don't usually stop using a security solution because it's only partially successful. What we can do, and often do, is attempt to maximize our successes by using more than one approach. In medicine, it's sometimes counterproductive to use overlapping treatments simultaneously, as it may compromise diagnosis. In malware management, however, most client organizations will, if pressed, take the view that it's more important to forestall or repair a breach than to name it,[2] and are comfortable with the idea of multi-layering defenses (or Defense in Depth).

We are sometimes accused of wanting to turn end users into malware analysts or security experts. This is far from our intention: making them part of the solution is not the same as making them the solution. Rather than trying to teach every user to be an expert, the point is to target what you teach and to whom so that it's within the limits of the achievable. People tend to do a better job of remembering things they understand, so long lists of things that should or shouldn't be done to conform to Policy X or Guideline Document Y aren't necessarily effective. They are, however, more effective if they are:

- easily accessible

- properly indexed
- appropriately cross-referenced

Meeting these conditions is not enough in itself, however: this approach works best when the user has enough training to think: "I seem to remember I was advised to beware of (for example) drive-by downloads when I visit external sites: perhaps there's some information on the security page that will tell me more." Or, "now what was that stuff about money mules again?" However, the continuing evolution of social engineering attacks makes it ever harder for potential victims to tell the difference between genuine and fake security software, codecs, browser plug-ins and so on. So it's not enough simply to tell them what social engineering is, for instance. There has to be sound backup (knowledgeable second-line support, for example) to ensure that ambiguous scenarios can be explained and resolved.

The effectiveness of education is greatly enhanced when the following factors are accounted for. Education must:

- Clearly explain why learning is of value (personal investment)
- Use currently understood conceptual examples (current point of reference)
- Be entertaining (yes, dry subjects are entertaining when competently presented)
- Stick to the essential concepts that must be taught (we are not trying to turn out computer science majors).

Let us admit here that some groups are inevitably easier to part-educate than others. Security training works better in corporate environments (where it's actually done) than it does on the home user population because it's obviously easier to (part-) educate a population if you have some control over its members' computing activities. We should note, however, that education in the workplace can often be carried over into the home computing environment.[3] Certainly, where education and training have been part of our jobs (formally or not) we've made a particular effort to cover home use wherever appropriate. Nonetheless, we have argued that education works least well in terms of raising awareness, because of the quantity of contradictory and often poorly-informed advice out there. If advice and education has the implicit or explicit backing of management, then maybe the recipient has the luxury of not needing to evaluate the accuracy of advice given. "The boss isn't always right, but he's always the boss." However, none of this reduces the need for the boss to ensure (as best able) that the information given is both accurate and presented in such a way as to maximize the possibility that a high proportion of it will be retained.

Now Wash your Hands, Please: User-Friendly Education

We sometimes say that "We don't know if education works, because no-one has really tried

it yet." This is not just a soundbite. Education is not a one-time, one-shot process. People forget what they don't use, and have to be retrained, or change posts or employers, so that their replacements have to be trained.

According to Gattiker,[4] a suitable re-training period is as short as 60-90 days, but this is likely to be the result of over-teaching. In fact, our experience suggests that in general, individuals tend not to make (exactly) the same mistake time and time again, even though there may be clustering within particular groups. That said, individuals with limited expertise may often behave more safely than self-perceived experts, because they don't have ego-issues with asking for help or advice.

In fact, where the information shared is realistically uncomplicated but still relevant, and there is a sound support infrastructure in place, this almost invariably raises the overall level of awareness and responsible behavior.[5]

However, many educational resources, even where they are technically well-founded, suffer from the fact that they were put together by a security geek with little awareness of pedagogical principles or ergonomics, or human psychology. Gary Hinson[6] describes a particularly horrible example of an awareness program based on a web-hosted learning management system displaying a number of user-hostile characteristics :

- No attempt to lead into the subject by explaining the need for the program or the logic of the learning plan
- A totally inflexible serial topic sequence: the victim was required to start at module 1 and work through to module 15 in sequence: if he wanted to find out about a particular module, he had to go through all the preceding modules first.
- Material cut and pasted from other materials such as policies and guidelines. The material wasn't tailored or rewritten for the use of any particular target group, and had not been edited to address inconsistencies of style or content between various source documents or to activate and make use of hyperlinks. In fact, it appears to have been an attempt to generate training materials without considering training issues, re-using heterogeneous materials with insufficient attention to establishing a sound initial teaching framework.
- Poorly constructed quiz questions:
    - Triple choice questions with two (and too) obvious distracters
    - Yes/No questions where the correct answer was obvious from the wording of the question, making it unnecessary to consider the reference material that preceded the quiz.
    - No feedback on why a given answer was correct or incorrect: just a tick or a cross. No way of referring back to the information page to clarify the reasoning behind the "true or false" verdict. In Hinson's own words, "this was really a quiz not an awareness activity."

We'd like to tell you that material this poor is the exception rather than the rule. Unfortunately, we've reviewed a great deal of material that displays similar faults: for example, many of the phishing quizzes reviewed by Harley and Lee[7]

Quizzes can be excellent teaching tools, when they stimulate interest by adding an element of game play and competition. However, an over-long, poorly constructed and ergonomically unsound quiz will quickly lose the interest of its participants. For user education purposes within the enterprise, a policy-based approach can actually work very well. Consider a policy structure like the following:

- A "mission statement" defining the objectives of the policy and the strategy it represents
- A simple but accurate (yes, we know that it's not always easy to meet both those criteria!) summation of the problem.
- Cross reference to other resources (informational, external and internal, other policies, standards and guidelines)
- An overview of the appropriate defensive strategy
- A "What This Means to You" section describing "correct" responses to well-chosen example scenarios.

While this is a feasible design for a single document, it's also the basis of an integrated teaching program, bolstered with such extras as an ergonomically designed quiz program.

Conclusion

We are often told that "drivers don't need to know how the internal combustion engine works to drive a car." Indeed they don't, and we don't expect end users to understand complex systems and technologies like heuristic analysis or encryption algorithms in order to protect themselves against malicious code or breaches of privacy. However, we don't consider drivers absolved of any responsibility for the safety of others or themselves when they sit behind the wheel. We expect them to be trained in the use (not the internals!) of the technology, to be familiar with the rules of the road, and to be on the lookout for possible danger from other road users (or misusers). In fact, when properly presented, even an explanation of heuristics is well received by relatively non-technical audiences.[8]

Unless we reach a point where we can rely absolutely on technology (or law enforcement, or socialization or some form of compulsory education), or some combination of mitigating factors) to protect our end users or customers in spite of themselves, education and training can play an important part in helping them to help themselves. In the meantime, by conditioning users to assume that technology can protect them irrespective of or in spite of their own actions, we do them a disservice and provide Orwellian disinformation. Too often, we allow them to think that even if technology can't protect them, that inability simply represents a purely technological failure for which they need never accept any responsibility, never considering that it's in their own interest to take responsibility for their own actions.

While education (global or otherwise) has never ensured that people always make the right decisions, that doesn't excuse us from trying to help them improve their chances of making

the right decisions. If you can educate even a fairly small number of the right people, good information and good hygienic practice cascades further than you might think.

Yes, the risks have increased and the technology that underpins safe computer usage is harder to understand than it was in the previous decade. But it's not about teaching every driver to be a professional mechanic. Good user education is all about filtering: not teaching everything but about teaching the right things, and reinforcing those messages often enough to create a culture of security awareness, where staff take it for granted that they are part of the solution.

If we can "teach skepticism" by making end users more resistant to social engineering, we reduce the cost-effectiveness of the technique for the attacker. But if we can at the same time engineer technology that will heighten the risk of detection at the same time as reducing the reward, we stand some chance of implementing a serious short-to-mid term win.

References

1. Craig Johnston: User Education in the Fight Against Cybercrime; AusCERT, 2008.
2. Pierre-Marc Bureau, David Harley: "The Name of the Dose"; Virus Bulletin International Conference Proceedings, 2008
3. David Phillips, in "The AVIEN Guide to Malware Defense in the Enterprise"; Syngress, 2007
4. Harley, Slade, & Gattiker: "Viruses Revealed"; Osborne, 2001
5. David Harley: "Education, education and education"; http://blog.isc2.org
6. Gary Hinson: "Security awareness: a 'How not to do it' guide"; http://blog.isc2.org/
7. David Harley and Andrew Lee: "Phish Phodder: Is User Education Helping or Hindering?"; Virus Bulletin 2007 Conference Proceedings
8. Randy Abrams: "Understanding and Teaching Heuristics"; AVAR 2007 Conference Proceedings.

Corporate Headquarters

ESET, spol. s r.o.
Aupark Tower
16th Floor
Einsteinova 24
851 01 Bratislava
Slovak Republic
Tel. +421 (2) 59305311
www.eset.sk

Americas & Global Distribution

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845
www.eset.com

PP20081208