Train-the-trainer guide

Malware awareness module

Introduction and scope

Malware - malicious software - includes viruses, Trojans, worms, spyware, APTs, ransomware and other nasty programs written deliberately to subvert system security and perform unauthorized/inappropriate/improper activities, usually covertly.

We update the malware awareness materials every year for three key reasons:

(1) Malware is ubiquitous – it's a threat we *all* face it to some extent;
(2) Malware-related risks are constantly changing – the associated threats, vulnerabilities and impacts all vary, sometimes markedly. Malware is being actively developed and exploited, while technical controls inevitably lag behind;
(3) Security awareness is vital to prevent or avoid infections, and to recognize and respond promptly and effectively to those that occur.

Learning objectives

The awareness module is intended to:

- Gently introduce and explain malware for everyone, where appropriate using plain English terms such as 'virus' and 'antivirus' and everyday examples;
- Expand on the information security risks involving, associated with or arising from malware, highlighting changes since a year ago;
- Describe and promote various information security controls intended to prevent, identify and respond to malware infections/incidents;
- Emphasize the practical things workers can and should be doing to mitigate the risks (*e.g*. avoiding inherently risky activities such as opening dubious attachments and randomly installing applications, keeping up with antivirus updates, patching and backups, and reporting suspicions or incidents promptly to Help Desk);
- Provide both informational and motivational content, stimulating people to think - and most of all to *act* - more securely. We're looking beyond merely making them 'aware' of malware.

What are *your* learning objectives on malware? What do you most want to put across? What has changed since your awareness program last covered this topic?

Suggested awareness activities

We're keen for you to make the most of your NoticeBored subscription, so here are some things you can do to make your security awareness program even more successful.

1. Select, customize and use the awareness content

- Check through the NoticeBored materials using the contents checklist (item 00) to decide which items to use and how.
- Customize/adapt/supplement/elaborate on the generic content supplied.

- Distribute selected materials using suitable internal communications routes or mechanisms, at the same time taking down any dog-eared awareness content that is no longer relevant or is showing its age.
- Update your intranet *Security Zone* with fresh content, and again clean out any stuff that has 'seen better days'. Use the **poster** images, Visio **diagrams** or other graphics, screen-shots *etc*. currently embedded in the presentations and briefings, to liven-up the *Zon*e, with links to additional downloadable content.
- Print and display the **posters**. These are meant to make people think, to amuse, intrigue and so hook them into checking out the other awareness content.
- Cover malware in your staff magazine, blog, email blast *etc*., using extracts from the NoticeBored content directly or for inspiration at least. Follow up with hot news and topical information on actual malware incidents during the month ahead.
- Present the **PowerPoint presentations** at seminars, meetings, workshops *etc.*, or turn them into video clips for the intranet.
- Decide on suitable prizes (perhaps relating directly to this topic *e.g*. retail antivirus packages) then circulate/use the **wordsearch, test** and **quiz.**
- Discuss the **case study**, perhaps adapting the scenario to reflect an actual malware incident from your organization, industry or locale. You could even use it as a business continuity exercise …
- Circulate the **awareness survey** and exploit useful feedback.
- Check/update your malware **metrics** and use the template malware **policy** and **job description** for a malware analyst to review or replace yours – or at least discuss possible changes with management.
- Check out your organization's malware controls using the **Internal Controls Questionnaire (ICQ)**, focusing especially on any areas of apparent weakness identified from your security metrics, post incident reviews, concerns voiced by IT/PC Support/Help Desk *etc*.
- In conjunction with HR/Training, check and update your new employee orientation materials plus any other courses on this important topic – concentrating on those most likely to be targeted by, or be particularly at risk from, spear-phishing campaigns, bank Trojans, data-thieving malware, ransomware and so forth.

2. Strengthen your security culture

Enhance your corporate security culture by spreading awareness materials and messages widely throughout the organization, using informal social networks as much as classical awareness mechanisms. Malware is likely to be especially relevant to:

- IT professionals - in particular the PC/tech support, systems and network security people who routinely deal with malware incidents and controls such as antivirus;
- The Help Desk workers, who *know* the kinds of malware-related queries, concerns and incidents that crop up most often, and have anecdotes concerning more unusual ones;
- Incident Management and Business Continuity who should have strong malware response plans and capabilities;
- (Information) Risk and Information Security (of course!);
- Various security awareness friends and training contacts throughout the business – your corporate social network of 'information security ambassadors';

- Any business units, departments, teams or individuals that recently suffered or were somehow caught up in malware incidents (*e.g*. those affecting business partners). Persuade them to talk about the situations in which they found themselves: find out how the incidents happened, what were the consequences for the people directly involved, and what were the impacts on the business *e.g*. the rough costs. Interview the people involved, or better still invite them to present in person at your seminars/courses, or build a more impactful case study around them.

3. Hinson tips: creative security awareness ideas

- Catchy sayings for awareness purposes – trinkets, notices, messages, email sigs, posters, mouse mats, tee-shirts, whatever:
  - Computer being held to ransom? Call in the official hostage negotiators: Help Desk
  - The best antivirus is … not getting infected
  - Practice safe hex: keep your antivirus updated, systems patched and threats avoided
  - Report possible virus infections *immediately* - sooner if possible
  - Vile viruses violate vulnerabilities while worms wander the web willfully
  - The original Trojan horse was Greek
  - Spyware, malware, ransomware, Tupperware, scareware: one of these does not belong
  - Any fool can catch a computer virus, and many do
  - Rootkits are as welcome as root canals
  - Malware really ***is*** out to get us
  - Click-regret: the sinking feeling that follows an unwise click on a dubious link, app or attachment
  - Behind every major malware incident lies a raft of control failures and missed clues
  - Famous last words: "Malware? Not *my* problem!"
  - Famous last words: "Oh look! Cool new app!"
  - Famous last words: "I'm too busy to patch right now"
  - Famous last words: "Go away, warning message, go *away*!"
  - Famous last words: "*Tomorrow* is backup day"
  - Famous last words: "It's perfectly safe: we have antivirus"
  - Famous last words: "That was an odd message …"
- Ask your corporate antivirus software supplier/s for assistance with or possibly sponsorship of your awareness program – some freebies to use as rewards maybe or information about the state of the art in malware prevention. Can you persuade them to send a guest speaker or podcast for your awareness seminars/courses, provide additional malware awareness content, or put on a safe lab-type demo of live malware?
- Identify specific, realistic, measurable goals for your awareness activities, and share them with participants (*e.g*. "After today's session, you will know how to tackle ransomware"). Use these on your promotional materials and invitations for the events. Bring them up at the start and end of the sessions, perhaps even later ("Thank you for attending the recent security seminar. We set out to help you tackle ransomware. Visit the intranet *Security Zone* for a quick recap."). If queries or issues come up during the sessions that you can't address and resolve on the spot, make a note and follow-up later: the follow-up is an excellent opportunity to remind people about the sessions.

- When someone tries to open an infected file, visit a blocked website or download a blocked app, that's a golden awareness opportunity. Instead of the usual bland, generic warning message, explain how they have triggered an alert and link to further information on the *Security Zone*.
- How would workers be informed in the event of a virus outbreak? Use the same mechanism/s to spread an 'all clear' security awareness message this month, such as "We are not aware of any malware incidents so far today: please help keep it that way! Visit the intranet *Security Zone* for more."
- Publish the metric "**Days since the last serious malware incident**" on the *Security Zone*, automatically incrementing the counter every day. The definition of 'serious' is arbitrary but, in the interest of using the metric for periodic awareness reminders, we suggest defining it such that no more than 5% of malware incidents, maybe one per month or one per quarter on average, qualify as serious, and then stick to your definition. Publicize and celebrate reaching significant milestones such as malware-free months, with increasing attention to build up the tension as the months pass. If (when!) a serious incident occurs, don't just quietly reset the counter but talk it up. Outline the incident with a link to a case study explaining how the infection occurred, what problems it caused and to whom or to which parts of the business (or beyond!), how it was detected and resolved, and what improvements have been made to prevent it happening again. [Just don't forget that this is an awareness activity: be very wary of using such an arbitrary metric to drive bonuses, strategy, policy, compliance or whatever!]
- Picking up on last month's awareness topic, malware is of concern to your business partners, suppliers, customers *etc*. Do you coordinate responses with them if there are major outbreaks? Do you even have an emergency means to contact them during an outbreak, if email and phone systems are down and the network is stuffed? Can you get hold of your ISP/CSPs (Internet and Cloud Service Providers), professional advisors, forensics experts and/or the authorities in a hurry? Check the extent to which your business continuity arrangements are truly prepared for *serious* malware incidents. Possibly stage a simulated major malware outbreak or incident this month for awareness, practice and learning/improvement purposes – assuming you don't suffer real incidents on a sufficiently frequent basis that is! [As specific examples, make absolutely certain your backups are sound in case of a ransomware attack on critical systems, and double-check that anyone with access to corporate bank accounts truly appreciates the possibility that they and their systems might be specifically targeted by criminals wielding bank Trojans, spear-phishing and other social engineering tricks.]
- If you genuinely want to drive up reporting of incidents, near-misses and concerns, make an extra effort to thank/reward anyone who reports actual or suspected malware *etc*. Word will soon spread! Work with the Help Desk, IT and HR on this. Be generous to those who followed the correct procedures and helped avert potentially serious incidents. Weave these situations/stories into your awareness program: good news is a rare commodity in our field, so milk it for all it's worth.
- With explicit, written, prior permission from senior management, run a malware awareness test against your own organization, for instance casually distributing a few "infected" USB memory sticks, CD-ROMs/DVDs, apps, email attachments, phishing messages, files on shared areas *etc*.: instead of being actual malware, have them display awareness messages along the lines of "This COULD easily have been a virus! Please call the Help Desk for advice." Be absolutely sure that they are harmless! If feasible, gather statistics on the number of test failures *e.g*. by counting "I've been silly" calls to the Help Desk or hits on embedded links, web bugs *etc*. Also count the number of test passes *e.g*. people who reported their suspicions to the Help Desk *without* falling victim. Possibly follow up with some of them to find out what caught victims out (why did they

fall for the lure?), and how security-aware workers spotted and responded to the threat – you should pick up some anecdotes to use in management reporting and other awareness activities.

- Convince workers to "tell their own virus stories", putting them up on a real or virtual wall-of-shame (a display board or a page on the *Security Zone*). Ask them to describe not just the literal events but their feelings and the personal and/or business consequences. What did they learn from the experience? What do they do differently now? If they could pass on just one piece of advice to someone else facing a similar situation, what would they say? If appropriate, award prizes for the best ones, as voted by workers and/or managers. Encourage people to read and talk about the stories, for instance by picking out the highlights or notifying people about any new stories every few days. Pump-prime the initiative using a handful of real or imagined stories in the style and detail that you want to promote (you can always quietly remove them once there are enough real stories).

4. Get in touch!

While it's always a pleasure to hear from customers, we'd love to learn about other security awareness topics and novel approaches, formats *etc*. you think we should adopt. Please email Gary@isect.com or call the office (+64 6874 3344 any day during NZ daylight hours please: we are 13 hours ahead of UTC). Keep us on our toes! ■