



Awareness program activities for Identity theft

Introduction

This paper aims to help you get the most out of the NoticeBored security awareness materials. Every month, we suggest some creative awareness activities and communications techniques to expand the reach of your awareness program. By all means pick and choose and maybe adapt our ideas to suit your organization.

By the way, if you have some good awareness methods or tips you're willing to share with the rest of the NoticeBored community, we'd love to hear from you: email gary@isect.com any time. Have you found any approaches that work really well in your organization? We'd love to hear from you.

Suggested security awareness activities this month

1. Review and select awareness materials suitable for your audience/s

2. Customize and supplement the materials where necessary

3. Distribute the awareness materials

- Update the corporate intranet
- Send suitable materials to selected distribution lists as email attachments (e.g. the **newsletter**);
- Print and distribute the **briefings** and possibly the **mind maps** as desk-drops, leaflets *etc.* on paper, send them by email and/or publish them on your Information Security intranet website (see below);
- Print and pin up the **posters** in areas such as internal notice boards in corridors, rest rooms *etc.*, maybe even some dedicated 'security corners' throughout the organization. Be sure to remove old posters before they become tired-looking and boring;
- Cut-and-paste interesting sections, news stories or quotes from the NoticeBored materials for your internal staff newsletters, management reports or other internal communications;
- Present the **PowerPoint presentations**, perhaps in conjunction with departmental managers, team leaders, HR or internal communications people *etc.* Consider manning a conference-style presentation stand in the reception area or staff restaurant, with the slides projected onto a screen or TV display and posters/leaflets to hand out. Naturally, the people presenting the materials should be familiar with the content but they have the benefit of access to the detailed NoticeBored briefings, mind-maps *etc.* in addition to the detailed speaker notes;
- Present the **case study** through interactive facilitated seminar sessions involving groups of approximately 10 to 30 people. In our experience, open discussion tends to be limited in smaller or larger groups but 'your mileage may vary';
- Install one or more of the **screensavers** on your desktop PCs (don't forget to set the password-locked inactivity timeout!);
- Circulate the **crossword** either by itself or in conjunction with other awareness materials. It might be worth including a regular "Information Security Crossword Corner" in your staff magazine, for example;
- Circulate the **awareness survey** (possibly as an intranet page with voting buttons) to gather basic statistics and encourage feedback from your audience. Survey your employees to understand their level of awareness and understanding, whether specifically on this month's

topic or more broadly on information security in general. Develop a structured approach to your awareness surveys and conduct them periodically to identify trends. Be careful how you analyze and report the findings – security metrics are notoriously difficult;

- Speak to management about the **business case** for two factor authentication. Is this a helpful way of analyzing and presenting the costs and benefits of information security controls to facilitate better investment decisions?
- Use the **internal controls checklist** to review the security controls in your organization relating to identity theft. Drawing on the risks identified in the NoticeBored newsletter and the controls detailed in the briefings and presentations, the checklist can be used directly for a high-level review to identify significant risks that deserve further management attention. Functions such as Internal Audit will probably be interested in the results and may even be persuaded to help conduct such reviews.
- In conjunction with HR, perhaps, pick out suitable items from the module to incorporate into your new employee induction pack, taking the opportunity to review and update the pack once again. [The NoticeBored **induction module** provides a starting point and some introductory level materials specifically designed for this purpose.]

4. Gain the support of other people with an interest in security awareness

Identity theft is of general interest and is particularly relevant to IT, external and internal communications functions, marketing and fraud units. Use your security awareness ambassadors throughout the organization to spread the word and maximize employee engagement.

Speak to your colleagues in IT to find out whether the anti-phishing toolbars now available for many browsers could be integrated into corporate desktop builds. Microsoft Internet Explorer 7 will incorporate one by default when released later this year and several others are already available as add-ons: Google on terms such as “anti-phishing.toolbar” for examples such as SpoofStick and SiteAdvisor, and don’t forget to test them properly before deployment (there are privacy implications with those which track user browsing habits).

5. Phishing-style email honeypot ideas

- First, if you intend to use an idea like this, get explicit written approval from your management!
- Send your users an email with a fake sender’s address and with an executable attachment claiming to contain a joke (it could easily be a phishing message or something else). The executable should write an entry into a database containing the user ID plus the date and time stamp, and display a warning message to the user stating that the user’s PC has just been hacked and infected with a virus.
- Track those who report the incident to the IT Help Desk and correlate the list of names with the database entries. Then either call the individuals for a quiet word or call to account those who opened the attachment, double-shame those who opened it and did not report the “incident” to the IT Help Desk. Don’t forget to praise anyone who reported the message without opening the attachment.
- A simpler and perhaps more acceptable version of this awareness exercise involves simply creating and sending fake phishing messages to your staff and tracking their responses, with follow-up emails to explain what is going on and promote the awareness materials.

6. Hinson tips: further creative suggestions to raise information security awareness

- Hold a “**password day**.” On that nominated day, take time out from the usual day job to wander around the offices offering employees confidential advice on their passwords and giving them some tips to help them choose stronger passwords.
- With explicit management permission, you could try running a password cracker (such as Cain & Able or L0phtcrack) against your password databases and hand out prizes for those whose password were difficult or impossible to crack. **Do not reveal the actual passwords!!** You have a express duty of confidentiality.

- Catch-phrases can be used on security awareness materials. We use them on our posters. Some organizations use them on mouse mats, mugs, Post-It Notes, pens and other trinkets that make cheap prizes for awareness competitions and thank you's for people who demonstrate good security practices (handouts for "password day" maybe?). Here are some catch-phrases to set you thinking:
 - Identity theft: deliberate misappropriation of someone's identity for criminal purposes
 - If you steal my identity, I have nothing left
 - Don't get hooked by the phishers
 - Don't be phishing bait
 - Passwords: keep them secret and change them often
 - Sharing passwords is as distasteful as sharing gum
 - Token appreciation: love my PIN
- Identity theft awareness DVDs are available from public sources such as the US Federal Trade Commission. Use a DVD presentation (perhaps over lunchtime), coupled with appropriate NoticeBored materials, to introduce the topic and prompt a group discussion. You may be quite surprised to find out just how many people in the audience have had personal experience of identity theft. Hearing personal stories from co-workers will create more of an impact on your audience than the DVD alone.

7. References and additional resources

- The new identity theft page in the [NoticeBored links collection](#) has an extensive range of links for further reading on this topic. The [authentication links page](#) is also relevant. ■