Best Practices for Online Shopping, Part 1

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My former graduate student Steven Zeligman, MSIA, CISSP, MCP has just submitted another article for the column. Here are his practical suggestions (with the usual editing from MK). I think that his two-part series will be useful in employee newsletters as a way of getting people to think about security. Remember that providing useful information to employees (especially if they then carry practical suggestions to family and friends) increases our colleagues’ sense of involvement in security and helps shift corporate culture towards security awareness and compliance with policy. For a PowerPoint presentation on this topic, see my files on “Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy” available on the INFOSEC Management page of my Website < http://www2.norwich.edu/mekabay/infosecmgmt/index.htm >. The following text is Steve’s.

* * *

Online shopping does pose risks, but the risk can easily be reduced.

1. **Eliminate Malware**

Before shopping online, clean your computers of malware (malware = MALicious softWARE). Keep your malware up to date.

2. **Shop Only at Trusted Online Retailers**

Use the same common sense when shopping online that you would use when shopping in the physical world. Be as vigilant when choosing online retailers as when choosing brick-and-mortar merchants. If you are uncertain about a particular Website, check the Better Business Bureau’s ratings < http://www.bbb.org >. Reliable online merchants provide a phone number where you can talk to a customer-service representative about security issues. Look for third-party seals of approval such as BizRate < http://www.bizrate.com/ >, BBBOnLine < http://www.bbbonline.org/ >, VeriSign Secured < https://seal.verisign.com/ >, and HackerSAFE < https://www.scanalert.com/ >. Usually clicking on the symbol will bring you directly to the report for the Website you are visiting.

3. **Look for Website Security Indicators**

Although the following are by no means absolute indicators of security, they’re a start:
   1. A padlock in the browser window’s status bar (be discriminating - sometimes it’s a false indicator or even just a symbol placed on the Web page itself < http://www.w3.org/2006/WSC/wiki/PadlockIconMisuse >);
   2. URLs that start with https:// instead of just “http://”; and
   3. The phrase "Secure Sockets Layer (SSL)" in the description of the communications protocol.

These are all indications that the online merchant may have taken measures to protect their
customers’ private information in transit.

In the second part, Steve looks at privacy issues when shopping online.

* * *

Steven Zeligman, MSIA, MCP, CISSP is the Network Security Manager at Dataline, Inc., and has more than 15 years of experience in information technology and security. His opinions are entirely his own and do not constitute the opinions of his employer. You are welcome to write to him mailto:steven.zeligman@gmail.com with comments on this article.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Website at <http://www2.norwich.edu/mkabay/www.mekabay.com/index.htm>.

Copyright © 2007 S. Zeligman & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Website, and to republish it in any way they see fit.