

## **10 Things Every Consumer Must Know When Shopping, Searching or Surfing Online**

- 1) Never click on links in suspicious e-mails—these are often phishing e-mails that appear to be from a legitimate organization but actually lead to spoofed, look-alike Web sites designed to capture consumers' personal information—like bank account and credit card numbers—for malicious intent.
- 2) Never call the phone numbers provided in suspicious e-mails claiming to be from a bank, financial institution or even a charitable organization. These phone numbers often ring crooks that are waiting to capture consumers' confidential information like passwords, bank account numbers and credit card information. Instead, call the number listed on the back of your ATM or credit card, or a number that you get from an organization's Web site.
- 3) Always type Web addresses directly into the Internet browser when visiting banking or credit card sites – rather than clicking on a link in an e-mail message, for example.
- 4) Review financial statements on a regular basis to catch any suspicious activity. Even small, seemingly meaningless charges that you don't recognize may actually be the work of a cybercrook.
- 5) Use Internet security software that includes antivirus, firewall, intrusion protection and transaction security protection. While many Internet browsers offer free Internet security protection, this often is not enough to protect consumers. Sources like CNET.com or *PC Magazine* offers thorough reviews of software so that consumers can find the solution that's best for them.
- 6) Regularly update Internet security software. Don't forget to install security software on *all* computers in the household—including the kid's PCs and those of college students.
- 7) Regularly update all software (especially Internet browsers) with the latest patches from the vendor – this will protect from known vulnerabilities.
- 8) Never view, open or execute any e-mail attachments unless the attachment was expected and the purpose is known.
- 9) Change passwords frequently. If possible, avoid dictionary words and try to include a variety of numbers and symbols.
- 10) Beware of gadgets such as MP3 players and smart phones that may carry viruses between home and work computers. Consider mobile security software to avoid the spread of viruses from mobile devices to home computer networks.

**Most importantly, use common sense when shopping, searching or surfing online. If something seems askew, don't proceed.**