Practice Safe Surfing and Defensive E-Mail

By Barbara B. Oliver

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

No matter how many firewalls, virus protection software programs and anti-spam devices are protecting your computers the enemy can invade. Face it; the spammers are just more driven by profit, and the virus creators wily and one step ahead of those who provide software to protect the portals. “Legitimate” spammers simply make money from any sales their emails produce; “Phishers” pushing spam requesting personal information are looking to steal your identity; virus creators are simply out to enjoy the damage their wares create. Now is a perfect time to ask your staff to resolve to surf safely on the Internet and not to open e-mails from any source, suspicious or known, with odd subject lines.

Safe Surfing

Upside: Internet research is indispensable as it saves time and money.
Downside: your mission may indicate that you travel to Web sites that indicate an interest in products and services you don’t desire.

- Proofread the URL you type into the search engine BEFORE you hit “enter.” Many common misspellings and letter transpositions will take you to sites you very much DO NOT want to visit!
- Narrow your search: Google, for instance, has an advanced search that allows the user to indicate the main category (funding sources), a second subset (to nonprofits) and sub-subset (Texas). You can also indicate language, date, occurrences (where it appears on the page), domains, and “Safe Search” (to block adult sites on a per-search or universal basis). Take a few minutes and get familiar with the advanced search features in the site you normally use and some other search engines. Check out the Advanced Search feature on DogPile, AltaVista, Web Crawler, Yahoo or Ask Jeeves.
- If you download files or programs from the Internet be sure they are from a trusted source and scan the files or programs for viruses BEFORE opening them. When in doubt, jot down the URL and ask your IT person BEFORE you download.
- Update your virus definition files regularly. Set your computer to update automatically at a time when your computer will be turned on.

Defensive E-Mail

I think we all know now that there’s no money waiting for us in Africa if we supply our bank account numbers. However, spam messages keep coming and coming and coming. So many people out there must be opening and answering them. Don’t let any of these people be your staff members.

- BEFORE opening an e-mail from an unknown person, check that the subject line is legit. Be alert to strange spellings, inclusion of symbols in the word (i.e., D!scount C1al,l!s). Don’t waste your time adding the e-mail addresses to your email blocker’s “black list”; the next message most likely will be a different address.
- If you receive an unexpected e-mail-even from someone you know-don’t open it. Ask the sender (via e-mail or phone), it the attachment is legitimate. If you can’t verify legitimacy, delete the e-mail, then write the sender an e-mail telling them you’ve deleted the message and why.
- Disguise your e-mail address on your Web site to avoid it being scraped off by spammers. For example: if your e-mail address is someone@nonprofit.org post it as “someone at nonprofit.org.”
- Don’t respond to spam. Delete it. If you click the “Remove Me” button from the spam message, this just verifies that the e-mail address is active and opens the door to receive more and more and more spam.
- NEVER EVER NEVER provide personal information in response to an e-mail message or follow a link provided “for your convenience” in an e-mail that is allegedly from your bank, credit card company or anyone else! If you wish to check if the message is legitimate, use your known established safe shortcuts to go the company in question. DO NOT under any circumstance use any links provided in the e-mail!

Many thanks to Walter Light whose adage became the title of this piece and who added technical expertise to the advice.