Avoid Internet Dangers: Practice Safe Surfing & Defensive E-Mail

The information highway may hold more pitfalls than you realize.

By Barbara Oliver & Walter Light

No matter how many firewalls, virus protection programs, and anti-spam devices protect your organization's computers, an enemy can invade. This is a perfect time to ask your staff to adopt safe surfing and e-mailing practices. Share the following tips with them.

Safe Surfing

Internet research is indispensable, but there's a downside: You may accidentally travel to websites you very much *don't* want to visit! To avoid such problems, be sure you and others in your organization follow these guidelines:

Proofread the URL you type into the search engine *before* you hit "enter." Many common misspellings and letter transpositions will take you places you don't want to go.

Narrow your search: Google, for instance, has an advanced search that lets you indicate the main category (funding sources), a second subset (to nonprofits), and sub-subset (Texas). You can also specify language, date, occurrences (where it appears on the page), domains, and "Safe Search" (to block adult sites). Take a few minutes and get familiar with the advanced search features in the site you normally use. Also check out the advanced search features on dogpile.com, altavista.com, webcrawler.com, yahoo.com, and askjeeves.com.

If you download files or programs from the internet, be sure they're from a trusted source, and scan them 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. In addition, you may wish to update these files manually if someone in your organization receives a virus, if you hear about a new virus replicating through computers, or if people you e-mail regularly tell you they've received a virus.

> "Spam messages wouldn't keep coming unless people were opening them. Don't let any of these people be your staff members!"

Defensive E-Mail

By now we all know there's no money waiting for us in Africa if we supply our bank account numbers. However, spam messages wouldn't keep coming unless many people were opening and answering them. Don't let any of these people be your staff members! Be sure they pay attention to the following warnings:

Before opening an e-mail from an unknown person, check that the subject line is legit. Be alert to strange spellings or symbols added to words (i.e., D!scount C1al,l!s). Don't waste your time adding the e-mail addresses to your e-mail blocker's "black list"; the next message most likely will come from 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) if 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.

Don't post your e-mail address on public message boards or newsgroups. If you do, you risk having your e-mail address harvested by spammers. If you must use an e-mail address on a public message board to post to the web or request online services, create a dummy address on your mail server or on Yahoo Mail. Change it when it attracts too much spam.

Disguise your e-mail address on your website to avoid having it 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 for you to receive more spam.

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! To see if the message is legitimate, use your established safe shortcuts to go to the company in question. Don't under any circumstance use any links provided in the e-mail!

Barbara B. Oliver is the former director of communications for the Nonprofit Risk Management Center (nonprofitrisk.org) and former editor-in-chief of Public Risk, *a magazine for risk managers. Walter Light is a retired electronics hardware designer and naval weapons systems engineer.*

Be Alert to Hidden Threats

Create plans that keep you safe from peril, using the guidance in these articles from NonprofitWorld.org:

- **Mitigate Cyber Risks with the Right Security Controls** (Vol. 36, No. 1)
- **Seven Questions You Must Address to Thrive in the Digital Age** (Vol. 35, No. 1)
- **Workplace Identity Theft: Curing the Latest HR Headache** (Vol. 25, No. 5)
- **Don't Get Caught by Phishing Schemes** (Vol. 35, No. 2)
- **Protecting against Fraud** (Vol. 31, No. 5)
- **Keep Your Online Identity Safe** (Vol. 35, No. 4)
- **Hacking People: Why Your Biggest Vulnerability Isn't in Your IT Department** (Vol. 37, No. 1)
- **Wire Transfer Fraud: It Could Happen to You** (Vol. 35, No. 3)
- **Nine Surefire Steps to Lock Down Your Cybersecurity** (Vol. 36, No. 3)