Surfing in Safer Waters â€“ What Students Need to Know

by (ARA)

Todayâ€™s students grew up with Internet connections in their cradles, so itâ€™s no wonder they donâ€™t hesitate to bank, shop or research on the Internet. Students use computers for everything from homework to playing games, to chatting with friends and just plain old surfing. However, they frequently forget they are surfing in an ocean of predators. Students often leave for college with bank account, credit card, driverâ€™s license and Social Security numbers â€“ sensitive data they store where they keep everything else, on their computers. Thatâ€™s where the risk comes in. In a new CompUSA TechInsights survey of college students nationwide, nearly 88 percent of respondents said they keep personal files on their computers. Survey findings went on to reveal that while most students are aware of basic computer security procedures, many donâ€™t practice them, leaving them and their parents open to identify theft. One of most notable survey findings involved phishing, an attempt to fraudulently acquire sensitive information by masquerading as a trustworthy person or business via electronic communication, such as an e-mail or instant message. Forty-one percent of the students surveyed werenâ€™t sure or didnâ€™t know what phishing was. And, nine percent admitted they had responded to e-mails asking for information, such as bank account numbers and passwords. â€œThe information students store on their computers is priceless. Many store thousands of dollars in music and movie files, alone, not to mention the photos and homework files that cannot be replaced. Still, most students donâ€™t take steps to protect that information,â€• said Brian Woods, executive vice president and general merchandise manager at CompUSA. â€œWith simple actions, such as logging out of banking sites and changing passwords frequently, students can protect themselves from the headache and heartache of losing their information and files.â€• Here are tips students need to stay safe on the Internet: Logout and Closeout Of the more than 635,000 identity theft complaints reported worldwide in 2004, 18 to 29 year olds were the largest affected age group, according to the Federal Trade Commission. Students need to read all privacy statements and transaction instructions on sites where they enter any personal information (e.g. bank account numbers, credit card information or telephone numbers). To properly end a session, first logout of the account and then close the Web browser. Restarting the computer after making any financial transactions on a public terminal adds another safety measure. Create Secure P@$$W0rds
Changing passwords often is key -- while 93 percent of survey respondents know what a secure password is, 61 percent admit they rarely or never change their passwords. Internet and computer passwords should be different for every account, longer rather than shorter, and include a combination of letters, numbers and symbols. Each password should be at least eight characters long and contain at least two numbers or symbols per every eight characters. Avoid common words, consecutive numbers and letters, and words and phrases easily associated with the account owner (for example, license plate numbers, names of friends and family or phone numbers). A good password can be a code for an easy-to-remember phrase. For example: â€œI like two chocolate chip cookies with milkâ€• becomes 1:)2cccw/m. Update Often Registered users regularly receive updates for their Web browsers, virus protection applications and programs that connect to the Internet. Updating software consistently will increase security against identity predators, keep computer programs functioning at top form and help students stay protected from unwanted viruses. Avoid phishing in murky waters Phishing e-mails are fabricated correspondence made to look like they were sent from a credible, well known Web site or company. These documents direct recipients to fraudulent Web sites and push students to provide personal information. Keep Social Networks Clean The popularity of social networks like MySpace, Facebook and Xanga continues to grow. CompUSAâ€™s survey reveals that 68 percent of respondents regularly post on at least one such community. Many students, however, are not using the best judgment as members of these online communities. Nearly one quarter of the students surveyed said they have posted pictures or text describing risky or illegal activities, such as underage drinking, to a social network page. Personal information including telephone numbers, home or school addresses or birthdays shouldnâ€™t be posted on personal pages in social networks. More than one third of survey respondents said they have friends who have posted home addresses to such sites. This makes it easy for online predators and identity thieves to harm students. Posting personal activities, pictures and friendsâ€™ names can have other ramifications. Many universities and corporations use the sites to gain information about potential students or job candidates. Students should evaluate how their profiles portray them to outside sources and remember nothing on these

sites is private. Unfortunately, the Internet is full of predators, but by using these tips, students can ensure that they are surfing in safer waters.

Surfing in Safer Waters â€“ What Students Need to Know by (ARA)