

AMERICANS ARE AT A DIGITAL LOSS TO PROTECT PERSONAL AND FINANCIAL INFORMATION

Growing number of Americans register increasing concern to keep information secure

MAHWAH, NJ, April 8, 2008 -- As Americans do their taxes, a majority are unaware that they may be putting personal and financial information required on tax returns in jeopardy. According to a recent survey by Sharp Electronics Corporation, almost half of all Americans are unaware of the danger of using insecure public copiers and printers, leaving themselves at risk for data theft if a copier is not equipped with data security measures. The survey, conducted by Roper on behalf of Sharp in February 2008, polled 1,004 adults regarding their perceptions of digital copier security.

Another survey item of note indicated that 60 percent of Americans don't know about the ability of a digital photocopier to store a document image on the hard drive, which could be later retrieved by a hacker.

"Tax season is here and many Americans appear not to be aware of the risk they take when making copies in public or at their office," said Ed McLaughlin, president, Sharp Imaging and Information Company of America. "Secure copiers can scramble data after every image is copied. We take pride in offering one of the most comprehensive approaches to MFP security cross the widest range of products, and the more we educate consumers and businesses to the risks, the more likely they will be to protect themselves against data theft." Personal and financial information is at risk when highly confidential forms containing social security numbers, Employer Identification Numbers, personal finance and even sensitive health information are duplicated on a copier that is not equipped with appropriate data security measures. Images of the documents can remain on the unit's hard drive indefinitely. This practice puts personal financial information at risk of theft by anyone with access to the copier's hard drive, or anyone with basic hacking abilities. When leased copiers are replaced and re-sold, they are an easy target for hackers. Additionally, in many businesses, a security breach can also occur via network connections, since MFPs are often linked to the network.

According to Paul DeMatteis, Senior Adviser on Corporate Security Programs, Office of Continuing and Professional Studies at John Jay College of Criminal Justice, information can be retrieved after equipment is traded in or discarded. "Companies purchasing secondhand equipment have reported finding considerable amounts of confidential data on their new machines," he says. "The same information can be obtained from your local network or the Internet if the unit sits on a network and is not appropriately protected."

The Sharp survey showed that a large majority of Americans feel their tax professional should secure their personal tax information when it is copied or printed. Nearly all respondents -- nine in ten Americans -- felt their tax preparer should be required to protect their personal information. And three in four Americans who have their taxes prepared by a professional feel their tax preparer's copier or printer should be secure.

Survey Results:

- 49 percent believe digital copiers and printers are secure.
- Three in ten Americans have made photocopies of their personal, financial or health information in their office or

a public place.

- 60 percent don't know about the ability of digital photocopiers to store a document image on the copier's hard drive which could later be retrieved by a hacker.
- 44 percent are more concerned than last year about the security of their personal information.
 - 52 percent are just as concerned as they were last year.
- 93 percent who have taxes prepared by a professional feel their tax preparer should be required to protect their data
 - 76 percent feel their tax preparer's copier or printer should be secure.

Sharp's Security Leadership

Consumers and businesses alike can take steps to ensure their copied information is safe. If consumers are making copies outside the home, it is important to ask if the public copier has data security installed. Sharp is a leader in the industry with one of the most secure copier line offerings available through direct sales and its dealer network. The data security kit offered on Sharp copiers encrypts and then overwrites every document that passes through the copier or multifunctional peripheral (MFP) with a "digital shredder." Sharp further secures the copier with a network interface card (NIC) that creates a virtual firewall, restricting unauthorized users from accessing the device's internal data or launching denial of service attacks.

Sharp Information and Imaging Company of America (SIICA), a division of Sharp Electronics Corporation, markets the advanced, color and production MX Series and IMAGER™ multifunctional peripheral (MFP) systems that help companies manage workflow efficiently and increase productivity.

For more information about the complete line of Sharp document solution products, contact Sharp Information and Imaging Company of America, Sharp Plaza, Mahwah, N.J. 07495-1163, or call 800-BE-SHARP.

###

Sharp OSA and related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies.

* In 2006 Sharp received the BERTL's BEST "Most Secure MFP Range" award and its color MX Series was the first color product line to achieve BERTL Five Star – Exceptional status throughout the entire line.

The study was conducted by Roper Public Affairs, a division of GfK NOP, on behalf of Sharp Electronics Corporation. Results are based on OmniTel™ telephone interviews conducted from February 29 – March 2, 2008 among a nationally representative sample of 1,004 US adults using a random digit dialing (RDD) probability sample of all telephone households in the continental United States. The sample has been weighted by age, sex, education, race, and geographic region. The margin of sampling error for the sample is +/- 3.1 percentage points.