New Webroot Survey Reveals Poor Password Practices that May Put Consumers' Identities at Risk

BOULDER, Colo., /PRNewswire/ -- When it comes to safeguarding personal information online, many people leave their virtual keys in the front door. New research commissioned by Webroot, the first Internet security service company, uncovers common password practices that are putting consumers' identities and wallets at risk.

In a survey of more than 2,500 people from the United States, United Kingdom and Australia, Webroot found the most commonly used password-protected sites among consumers are banks (88 percent), personal email accounts (86 percent), and Facebook (72 percent) – all of which are rife with sensitive information.

Among the findings:

•4 in 10 respondents shared passwords with at least one person in the past year.

•Nearly as many people use the same password to log into multiple Web sites, which could expose their information on each of the sites if one of them becomes compromised.

•Almost half of all users never use special characters (e.g. ! ? & #) in their passwords, a simple technique that makes it more difficult for criminals to guess passwords.

•2 in 10 have used a significant date, such as a birth date, or a pet's name as a password – information that's often publicly visible on social networks.

"We're seeing between 40,000 to 100,000 new samples of malware emerge daily, and in most of those cases the motivation behind the malware is financial," said Jeff Horne, Director of Threat Research at Webroot. "In fact, earlier this month the FBI reported that Zbot, a Trojan that steals passwords, led to the loss of $70 million from its victims. Using good password and security practices will help thwart similar attacks; make a common practice to never store your password in a browser or FTP site, and have reputable, up-to-date antimalware protection in place."

Summary of Key Findings:

Younger people are especially likely to take online security risks. Webroot found that among 18 to 29 year-olds:

o 12 percent have shared a password in a text message (vs. 4 percent overall).

o 30 percent logged into a site requiring a password over public WiFi (vs. 21 percent overall).

o Over half (54 percent) have shared passwords with one or more people in the past year (vs. 41 percent of people overall).

In addition, poor online password practices put consumers in danger of hacking and identity theft:

* 41 percent use the same password for multiple accounts.

* Only 16 percent create passwords with more than 10 characters in length.

* 4 in 10 people (41 percent) have shared passwords with one or more people in the past year.

* Almost half of Facebook users (47 percent) use their Facebook password on other accounts and 62 percent of Facebook users never change their password.

What Can You Do?

The threat experts at Webroot provide the following six Internet safety tips for developing passwords that will keep their information secure:

* Make Your Password Unique – As a critical line of defense, choose passwords wisely. Incorporate numbers, letters and special characters (such as punctuation marks) to strengthen your password. Form a password using letters, numbers and figures in a memorable sentence, such as "Webroot educated me in 10/10." Additionally, password management features in products like Webroot® Internet Security Complete can both help you select a secure password and protect you from online threats.

* Use one password for one site -- Once you've created a unique password, use it only for one Web site or one service. If you use the same password everywhere, you open up a gateway to the information stored on each of your password-protected sites if one of them is compromised. In addition, don't write down passwords and store them for your own recall on a notepad or in a Word document, both of which leaves them vulnerable to prying eyes. For help, use a password management tool.

* Not Sharing is Caring – Never share any password with anyone: Not your boss, your best friend, your cousin, your significant other or your spouse. Once a password is out of your control, you don't know how it will be used. If you've shared a password, to regain control of your account change the password.

* Change your passwords periodically -- Change the passwords you use most frequently, and never keep the same password on any account for more than a year even if you rarely use the site. For help, a good password manager feature will remind you when it's time to switch it up.

* Say no when browsers offer to save your password – Web site browsers like Firefox and Internet Explorer have a feature which lets users save passwords for later use. The most widely distributed password stealing Trojans, including Zbot and SpyEye, know where to look and how to steal that information if you get infected. This also applies if you use an FTP client.

* Any account can be valuable to a criminal -- Criminals use other people's identities for many purposes other than draining your bank account. Any old, unused free account on a message board, Web mail service, or social network can be hijacked for fraud. When you plan to quit a service or forum, change your password so criminals can't use your account for clickfraud, black hat SEO, or to try to convince your friends and family that you're stuck far from home and need a wire transfer to return.

Source URL (retrieved on *03/12/2014 - 6:33am*):
http://www.wirelessdesignmag.com/news/2010/10/new-webroot-survey-reveals-poor-password-practices-may-put-consumers-identities-risk