Survey Reveals How Lazy People are With Their Passwords

It never fails to amaze me when I read studies about how careless and stupid people are with regards to their online security – especially with online passwords. Most of you who are reading this likely don't fall into this category, but I'm sure you know many people who do.

Another study was released to today that once again, shows how careless people really are online. When it comes to safeguarding personal information online, many people don't seem to care very much, or don't think enough about it.

The password study, commissioned by Internet security firm Webroot, uncovers some scary common password practices. In the survey of more than 2,500 people, Webroot found some interesting trends in how users handle their online passwords.

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. (A separate recent study revealed that 75% of people use the same password for Social Networking Sites and their email accounts)

• 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. (*Yet not all sites support this option of special characters!*)

• 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.

Other Interesting Findings:

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

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

• 30 percent logged into a site requiring a password over public WiFi (vs. 21 percent overall) (*Note: This is typically only dangerous when you logon not using SSL -- aka HTTPS in your browser*)

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

The number of Web sites that require an extra layer of security has proliferated, driving careless habits:

• Three quarters (77 percent) of consumers have five or more accounts with online services that require passwords.

• One-third (35 percent) have 10 or more password-protected accounts. Only 10 percent ensure they never use the same password on different accounts.

• Passwords are forgotten occasionally, often or always by over half of consumers (51 percent).

Despite these disturbing figures, consumers still think they are safe, with 50 percent of people saying they feel their passwords are very or extremely secure. That being said, according to the survey:

• 86 percent do not check for a secure connection when accessing sensitive information when using unfamiliar computers.

• 14 percent never change their banking password.

• And 30 percent remember their passwords by writing them down and hiding them somewhere like a desk drawer.

• 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.

One thing that Webroot points out is that *any account can be valuable to a cybercriminal*, not just online banking accounts. Social networking accounts are a perfect example – just because your bank account isn't connected to your Facebook profile, your account is still valuable to fraudsters, and many scams

use hijacked facebook accounts to ask for money from your friends, while appearing to be you.

Smarten up, folks. It's really not so hard to setup some solid password practices. At the very least, promise to to make sure your online banking and email accounts have their OWN unique passwords. If you have many accounts and really don't see yourself having all unique passwords, at least keep your email separate as well as any finance related accounts. And, again since most of our readers don't really fall in this category, at least try to open the eyes of those around you.

Pointers On Password Security

• **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.

• **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.