Click to Print

3 Scary Online Security Mistakes to Avoid

Posted by Brian Patrick Eha | October 31, 2012

URL: http://w w w .entrepreneur.com/blog/224847

image credit: Lazy Dork

In the online world, terrors aren't reserved for Halloween. Hackers are very real, and they haunt the web like Freddy Krueger haunts people's dreams, looking to use your most personal information against you.

Fortunately, there are plenty of things you can do to protect yourself. Sometimes it's not a matter of making your system impregnable, just of making it a little bit more difficult for hackers to break into yours than into someone else's. With that in mind, here are three scary security mistakes you should avoid:

1. Not masking your social activities. When it comes to using social networks and other online communities, it helps to "think like a thief," says Brad Gobble, a senior manager of information security at Mozy, an online backup service. In other words, don't divulge information a thief would want, such as your full name, age or place of residence. In the age of oversharing, that may sound impossible, but it's safest to keep identifying information to a minimum in online communities.

When it comes to sharing images, Gobble warns against posting pictures that include your car's license plate, your house number or the street sign for your neighborhood. Similarly, you might consider not wearing clothes in photos that could give away your school or business affiliations.

Related: **How to Turn Your Fear into Fuel**

2. Not protecting your data. "Data has value -- just like dollars or gems -- and is significantly more portable and easier to put in the hands of attackers," Gobble says.

Your first line of defense is a strong password. Don't use the same login name and password on different devices, and use a different set for each important website -- your bank, your email and so on. Each of your computers and mobile devices should also have its own password.

In addition to password-protecting your electronic devices, consider encrypting individual files. Do you calculate your taxes on your computer? Keep client invoices? Encrypt those files. A free tool such as Pretty Good Privacy can do this for you.

Beyond individual files, there are options for protecting the entire contents of your computer should it fall into the wrong hands. Gobble suggests Microsoft's Bitlocker or Apple's File Vault.

3. Not updating your software. You might not think about it when using desktop software and mobile apps, but these programs can quickly become outdated. Even the best programmers can make mistakes, and when developers discover security flaws in their code, they patch the holes by putting out an update for users to download. Downloading these updates is one of the easiest ways you can protect yourself from intruders, Gobble says.

Consider turning on the auto-update function of your operating system and of any software programs that have one. For anything else, check regularly for new versions and download them promptly, he says.

Related: **3 Tips for Dealing with the Skeletons in Your Closet**