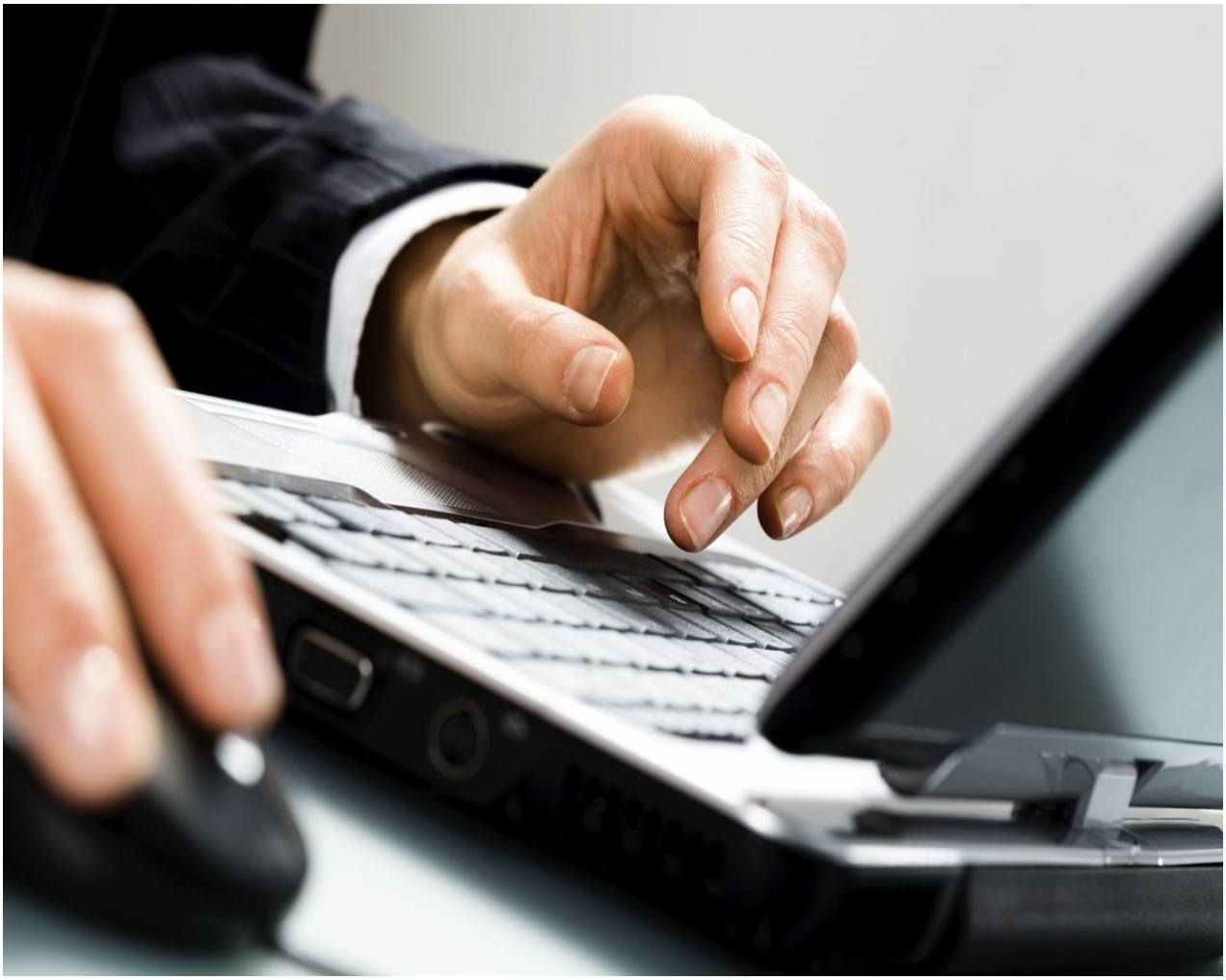
The Virgin Islands Consortium

How to Keep Data Out of Hackers' Hands

Technology / **Published On August 05, 2014 10:04 PM /**

Ernice Gilbert August 05, 2014



(The New York Times) -- The numbers sound abstract: Hundreds of millions of email addresses and other types of personal identification found in the hands of Russian hackers. For people worried that they are caught in the mix, however, the discovery by Hold Security of a huge database of stolen data is very personal. But personal doesn't mean helpless. There are common sense steps everyone can take to keep the impact of hackers to a minimum.

How do I know if my personal information was stolen?

Assume it is. The latest breach is huge, and similar attacks and smaller thefts are happening all the time. Hold Security is creating an online tool to allow consumers to see

whether their records have been stolen, but they are not certain when it will be ready. At this point, it is wisest to improve your online security immediately.

Should I change my password?

The first step, as always, is to change passwords for sites that contain sensitive information like financial, health or credit card data. Do not use the same password across multiple sites.

How do I create stronger passwords?

Try a password manager like LastPass or Password Safe, which was created by security expert Bruce Schneier. These sites create a unique password for each website you visit and store them in a database protected by a master password that you create. That sounds dangerous, but password managers reduce the risk of re-used passwords or those that are easy to decode. If you must create your own passwords, make sure they are not based on dictionary words. Even a word obscured with symbols and numbers can be cracked relatively quickly. Mr. Schneier suggests creating an anagram from a sentence, and using symbols and numbers to make it more complicated. For example, the sentence “One time in class I ate some glue” could become “1TiC!AsG.” Create the strongest passwords for the sites that contain the most sensitive information and do not re-use them anywhere.

Are passwords enough?

Passwords are not enough. If a site offers additional security features like secondary or two-factor authentication, enable them. Then, when you enter your password, you’ll receive a message (usually a text) with a one-time code that you must enter before you can log in. Many bank sites and major sites like Google and Apple offer two-factor authentication. In some cases, the second authentication is only required if you’re logging in from a new computer.

How can I stop my information from being stolen in the first place?

Increasingly, you cannot. Regularly monitoring your financial records can help minimize the damage if someone gets your information. But only the companies storing your personal data are responsible for securing it. Consumers can slow down hackers and identity thieves, but corporate computer security and law enforcement are the biggest deterrents.