How to Devise Passwords That Drive Hackers Away

Published on-line in Yahoo Finance -- November, 2012

I have annotated the article with my personal practices, in CAPITAL LETTERS after the relevant paragraphs.

Not long after I began writing about cybersecurity, I became a paranoid caricature of my former self. It's hard to maintain peace of mind when hackers remind me every day, all day, just how easy it is to steal my personal data. I'M NOT AS WORRIED ABOUT IT HAS HE IS. I DOUBT MY LAPTOP WILL EVER BE STOLEN, SO I DO KEEP PASSWORDS ON IT UNENCRYPTED. HOWEVER, I DON'T USE THE WORD "PASSWORD" IN THE FILE THEY'RE IN, TO MAKE IT HARDER TO DO A SEARCH FOR THEM.

Within weeks, I set up unique, complex passwords for every Web site, enabled two-step authentication for my e-mail accounts, and even covered up my computer's Web camera with a piece of masking tape — a precaution that invited ridicule from friends and co-workers who suggested it was time to get my head checked.

But recent episodes offered vindication. I removed the webcam tape — after a friend convinced me that it was a little much — only to see its light turn green a few days later, suggesting someone was in my computer and watching. More recently, I received a text message from Google with the two-step verification code for my Gmail account. That's the string of numbers Google sends after you correctly enter the password to your Gmail account, and it serves as a second password. (Do sign up for it.) The only problem was that I was not trying to get into my Gmail account. I was nowhere near a computer. Apparently, somebody else was.

It is absurdly easy to get hacked. All it takes is clicking on one malicious link or attachment. Companies' computer systems are attacked every day by hackers looking for passwords to sell on auction-like black market sites where a single password can fetch $20. Hackers regularly exploit tools like John the Ripper, a free password-cracking program that use lists of commonly used passwords from breached sites and can test millions of passwords per second. I TRY TO STEER CLEAR OF MALICIOUS SITES, AND SHUN ATTACHMENTS I DON'T TRUST.

Chances are, most people will get hacked at some point in their lifetime. The best they can do is delay the inevitable by avoiding suspicious links, even from friends, and manage their

passwords. Unfortunately, good password hygiene is like flossing — you know it's important, but it takes effort. How do you possibly come up with different, hard-to-crack passwords for every single news, social network, e-commerce, banking, corporate and e-mail account and still remember them all?

To answer that question, I called two of the most (justifiably) paranoid people I know, Jeremiah Grossman and Paul Kocher, to find out how they keep their information safe. Mr. Grossman was the first hacker to demonstrate how easily somebody can break into a computer's webcam and microphone through a Web browser. He is now chief technology officer at WhiteHat Security, an Internet and network security firm, where he is frequently targeted by cybercriminals. Mr. Kocher, a well-known cryptographer, gained notice for clever hacks on security systems. He now runs Cryptography Research, a security firm that specializes in keeping systems hacker-resistant. Here were their tips:

FORGET THE DICTIONARY If your password can be found in a dictionary, you might as well not have one. "The worst passwords are dictionary words or a small number of insertions or changes to words that are in the dictionary," said Mr. Kocher. Hackers will often test passwords from a dictionary or aggregated from breaches. If your password is not in that set, hackers will typically move on. I DON'T USE DICTIONARY WORDS. I DO MIX UPPER AND LOWER CASE, AND SOMETIMES THROW IN NUMBERS AND SOMETIMES PUNCTUATION. I AM MOST CAREFUL ABOUT SITES WHERE SOMEONE GAINING ACCESS COULD DO ME HARM - BANKS, BROKERAGES, ETC.

NEVER USE THE SAME PASSWORD TWICE People tend to use the same password across multiple sites, a fact hackers regularly exploit. While cracking into someone's professional profile on LinkedIn might not have dire consequences, hackers will use that password to crack into, say, someone's e-mail, bank, or brokerage account where more valuable financial and personal data is stored. I DO USE THE SAME PASSWORD MULTIPLE TIMES, BUT NOT ON SITES WHERE I WORRY THAT SOMEONE AT THE SITE COULD BE A BAD GUY.

COME UP WITH A PASSPHRASE The longer your password, the longer it will take to crack. A password should ideally be 14 characters or more in length if you want to make it uncrackable by an attacker in less than 24 hours. Because longer passwords tend to be harder to remember, consider a passphrase, such as a favorite movie quote, song lyric, or poem, and string together only the first one or two letters of each word in the sentence. I USE A COUPLE DIFFERENT

TRICKS FOR CREATING PASSWORDS THAT I CAN REMEMBER. I THINK COMING UP WITH A METHOD IS A GOOD IDEA, AND IF IT IS SITE-SPECIFIC IT GETS AROUND THE PROBLEM OF USING THE SAME PASSWORD TWICE.

OR JUST JAM ON YOUR KEYBOARD For sensitive accounts, Mr. Grossman says that instead of a passphrase, he will randomly jam on his keyboard, intermittently hitting the Shift and Alt keys, and copy the result into a text file which he stores on an encrypted, password-protected USB drive. “That way, if someone puts a gun to my head and demands to know my password, I can honestly say I don’t know it.” I DON'T USE A USB DRIVE FOR THE PASSWORDS - I'M RELYING ON MY LAPTOP NOT BEING STOLEN OR ACCESSED MALICIOUSLY.

STORE YOUR PASSWORDS SECURELY Do not store your passwords in your in-box or on your desktop. If malware infects your computer, you’re toast. Mr. Grossman stores his password file on an encrypted USB drive for which he has a long, complex password that he has memorized. He copies and pastes those passwords into accounts so that, in the event an attacker installs keystroke logging software on his computer, they cannot record the keystrokes to his password. Mr. Kocher takes a more old-fashioned approach: He keeps password hints, not the actual passwords, on a scrap of paper in his wallet. “I try to keep my most sensitive information off the Internet completely,” Mr. Kocher said. I HAVE COPIES OF MY PASSWORDS ON PAPER IN OUR HOME SAFE, AND ON THE INTERNET IN DROPBOX. I USE A VERY SECURE PASSWORD FOR DROPBOX.

A PASSWORD MANAGER? MAYBE Password-protection software lets you store all your usernames and passwords in one place. Some programs will even create strong passwords for you and automatically log you in to sites as long as you provide one master password. LastPass, SplashData and AgileBits offer password management software for Windows, Macs and mobile devices. But consider yourself warned: Mr. Kocher said he did not use the software because even with encryption, it still lived on the computer itself. “If someone steals my computer, I’ve lost my passwords.” Mr. Grossman said he did not trust the software because he didn’t write it. Indeed, at a security conference in Amsterdam earlier this year, hackers demonstrated how easily the cryptography used by many popular mobile password managers could be cracked. I HAVE JUST STATED USING LastPass AS MY PASSWORD MANAGER. SO FAR I AM LIKING IT. IT IS PRETTY EASY TO USE, AND DOES A NICE JOB OF AUTOMATICALLY LOGGING INTO SITES. AGAIN, I ASSUME THAT MY LAPTOP WON’T BE STOLEN.

IGNORE SECURITY QUESTIONS There is a limited set of answers to questions like “What is your favorite color?” and most answers to questions like “What middle school did you attend?” can be found on the Internet. Hackers use that information to reset your password and take control of your account. Earlier this year, a hacker claimed he was able to crack into Mitt Romney’s Hotmail and Dropbox accounts using the name of his favorite pet. A better approach would be to enter a password hint that has nothing to do with the question itself. For example, if the security question asks for the name of the hospital in which you were born, your answer might be: “Your favorite song lyric.” I PLAY IT STRAIGHT WITH SECURITY QUESTIONS. TOO HARD TO REMEMBER FAKE ANSWERS.

USE DIFFERENT BROWSERS Mr. Grossman makes a point of using different Web browsers for different activities. “Pick one browser for ‘promiscuous’ browsing: online forums, news sites, blogs — anything you don’t consider important,” he said. “When you’re online banking or checking e-mail, fire up a secondary Web browser, then shut it down.” That way, if your browser catches an infection when you accidentally stumble on an X-rated site, your bank account is not necessarily compromised. As for which browser to use for which activities, a study last year by Accuvant Labs of Web browsers — including Mozilla Firefox, Google Chrome and Microsoft Internet Explorer — found that Chrome was the least susceptible to attacks. I OCCASIONALLY DO THIS. SAFARI IS MY MAIN BROWSER. IF I'M GOING SOMEPLACE SUSPICIOUS I MIGHT USE CHROME OR FIREFOX, BOTH OF WHICH ARE ON MY COMPUTER.

SHARE CAUTIOUSLY “You are your e-mail address and your password,” Mr. Kocher emphasized. Whenever possible, he will not register for online accounts using his real e-mail address. Instead he will use “throwaway” e-mail addresses, like those offered by 10minutemail.com. Users register and confirm an online account, which self-destructs 10 minutes later. Mr. Grossman said he often warned people to treat anything they typed or shared online as public record. I OFTEN USE ALIASES FOR ONLINE ACCOUNTS - I HAVE CREATED ABOUT 100 OF THEM OVER THE YEARS - ALL AT CLOSEREACH.COM, SO MY YAHOO-IMPOSED LIMIT ON THE NUMBER IS PRETTY HIGH. 10MINUTEMAIL SOUNDS USEFUL - I DIDN'T KNOW ABOUT IT. IT'S SIMILAR TO USING A 'VIRTUAL' ONE-TIME-ONLY CREDIT CARD, WHICH I DO FOR UNKNOWN VENDORS. AT&T UNIVERSAL CARD OFFERS THAT - PROBABLY OTHERS AS WELL.

“At some point, you will get hacked — it’s only a matter of time,” warned Mr. Grossman. “If that’s unacceptable to you, don’t put it online.” PROBABLY MORE TRUE FOR WINDOWS

PCS THAN MACS. ONE PROMINENT TARGET, THOUGH, IS ONLINE EMAIL ACCOUNTS. IF I READ/SENT MY MAIL ONLINE I WOULD USE A SERIOUS PASSWORD FOR IT.