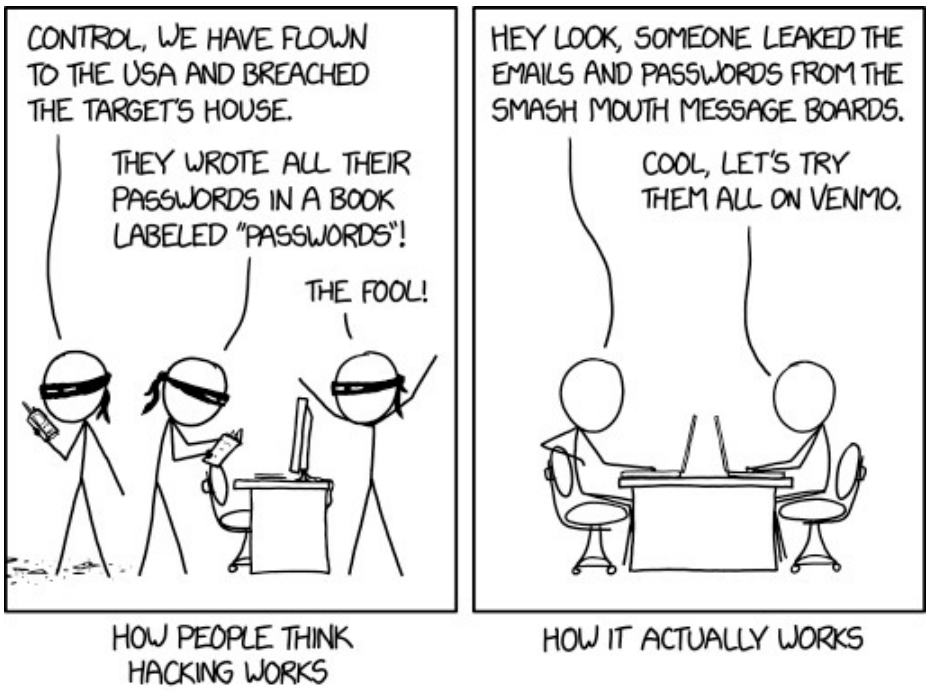
Science Translations
Established 1990
PC410.COM™
PC Updater News

Password, Password, Hack

Don’t repeat your online passwords. Let me repeat that: Don’t repeat your online passwords. Ever. Those of you who tell me that you have only one password, and you use it everywhere, are going to be in trouble at some point, and probably have already been hacked.

Here’s what happens in the real world, courtesy of XKCD.com:



All this applies to passwords used everywhere and anywhere on the internet. That's where passwords are stolen in bulk (mostly), captured by malware (often), captured in passing (sometimes), or guessed by brute-force repeat attacks (for short passwords). Local passwords, like a password used as an local login to a device sitting on your desk, are another matter, and have different security issues.

A story will help to explain the issues with re-used passwords online: Around 6 years ago, I signed up to take an online video course on a programming topic. I used a unique password there, didn't use it anywhere else. OK, done with that, haven't looked at that site since. And finally, late last year I received one of those bad emails with "this is your password" in it, and telling me that they have malware on my system recording everything, and threatening various nasty financial and other consequences if I didn't send a Bitcoin payment. That's a well-known fake, but the password was real. Here's what happened:

The video programming web site was hacked, and they lost their list of email addresses and passwords. Since they were incompetent to begin with, they did poorly financially as well, and now have been merged out of existence into another video tutorial site. Neither the original site or the buyer ever notified me that they had been hacked, but the normal practice after a hack is to set every password that was suspected to have been stolen to "must reset on next login." Again, not competent and not responsible. It's also misleading: each user didn't forget the password; the site lost loads of logins and forced everybody to reset them, with no reason given.

The stolen list of user names and passwords became available in the shadier parts of the internet, usually known as the 'dark web,' which is not generally searchable, but hackers and other bad guys refer each other to resources there. New lists are sold for up to ten dollars per login if they include account numbers and the back-of-card check codes and emails and passwords; older "dumps" are much cheaper if they're old, just emails and passwords, or from outside the USA.

So the list from the video site was a few years old, and therefore cheap. The blackmail letter sender bought, traded, or stole the list (no honor among thieves), and sent out a threatening letter asking for

Bitcoin and announcing the stolen password. If they had a fresher list, they would have tried that email and password at maybe the top-20 largest banks, Amazon, the Apple Store, Facebook, anywhere that stores payment information.

In my case, I word-searched my password list, and found that I had used that password, once, on that training site. As they never had any payment data, and my login didn't actually work at the successor's new web site, there was nothing to do. Email deleted.

But let's just say I had re-used that password. There are other hackers who have automated attempts to log into banks, and so on, until they find that they can get access, and then turn it over to a human to empty out whatever they can, or take over a web site or email address in order to have someone else's mail accounts and web sites to use to send out more attempts to get more emails, passwords, and access to financial accounts.

So if the password is re-used, the password has to be reset at every site where it was used. If that happens to to you, would you know where to reset that password?

The Cleanup

If you used Google Chrome to remember the passwords, you can read them from inside Chrome by clicking the three-dots icon (menu) at the top-right, clicking Settings, and in the Autofill section, clicking on passwords. Chrome hides the passwords; make them visible by clicking the eye logo, and entering your Windows password.

In Firefox, you can read your passwords from the three-bars menu icon, by choosing "Logins and Passwords." Again, click the eye to read any hidden passwords.

You can't read saved passwords directly in Microsoft Edge. Instead, go to start, Control Panel, User Accounts, Credential Manager, Web Credentials, and read the list there.

And finally, if you're using Internet Explorer, stop. Call me and I'll remove it for you. No one should be using Internet Explorer for anything. It's obsolete, no longer meeting standards in any way, and is no longer getting any security patches from Microsoft.

And if you have no list anywhere, well, just go everywhere you've ever been, and reset the password. Also file a fraud alert at your banks. And enroll in credit monitoring.

Help from Google

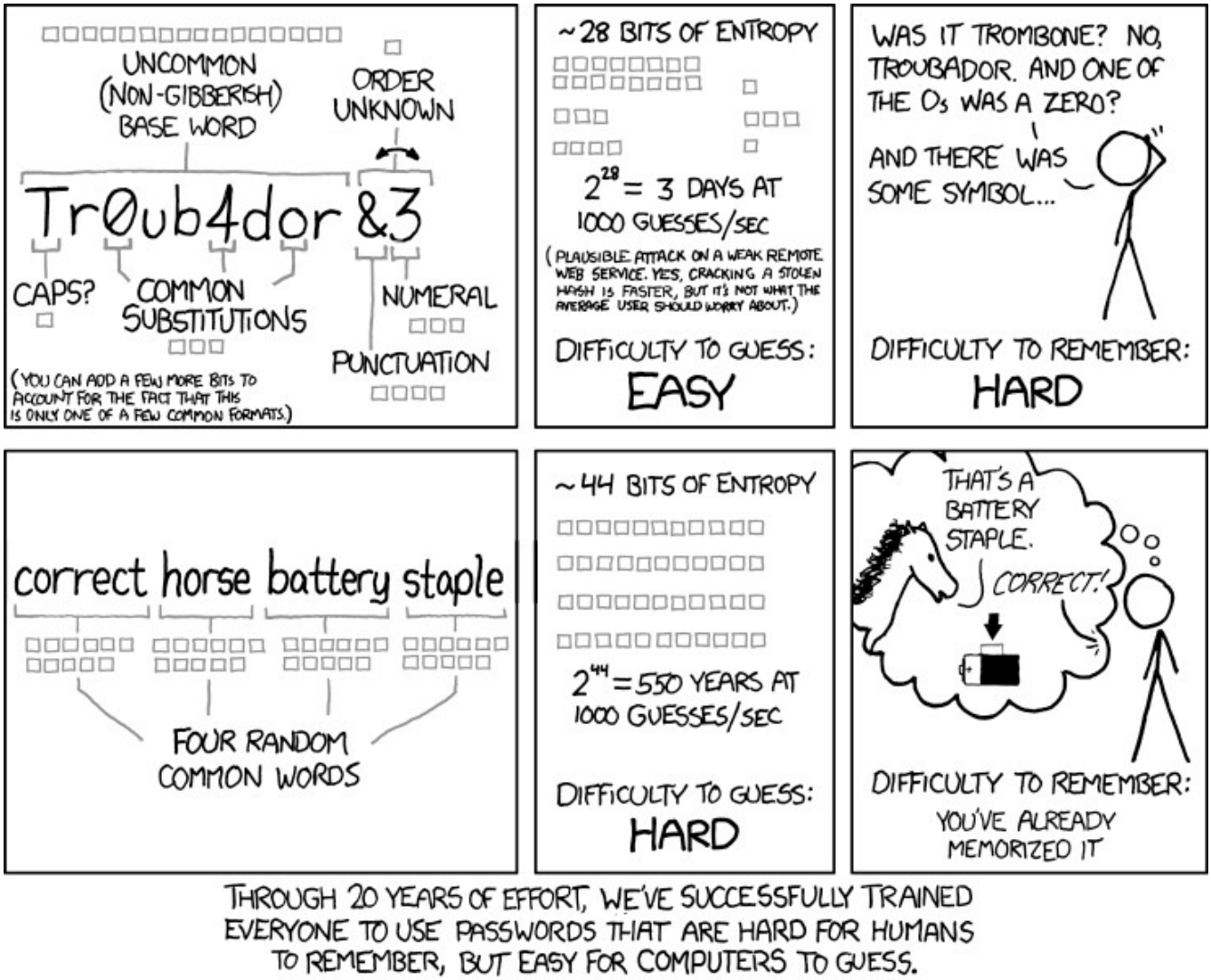
If you use Google, by using any of their products: Android phones and tablets, Google Chrome, Google Drive, or any product using a login, you have a Google account, and can check for security issues at: https://myaccount.google.com/

Click on 'Security Issues Found,' and it will show you passwords that it knows you've repeated, and in

some cases, passwords that it knows were found in an online dump of stolen email addresses and passwords, just as were used in that scam email. Log into every site affected, and replace them all with a different password for each.

Google's account page will also warn you if the passwords it sees are too simple. Passwords that are used online need to be at least 12 characters long, preferably 16 characters or longer. Length is the most important factor here. A password of "pa$sw0r6" is trivial for an automated system to crack, and "Zebra54_Treadmills" is far too long to be guessed by repeat login attempts, and it's actually possible to type that into a cell phone when needed. The famous example of that is "CorrectHorseBatteryStaple" and you can create random long passwords here:
https://CorrectHorseBatteryStaple.com

And here's the XKCD.com cartoon that inspired it, also shown on the page above:



So passwords need to be long, easy to type, and unique. Use them once. Just once.

Stay Safe, Stay Home

But if you really need a computer repaired, I now have a no-contact dropoff & pickup room for hardware repairs. Or I can drop-ship hardware, and configure it remotely. Call ahead for a repair appointment or a consultation.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735