We’re Here to Pump Your Passwords Up!

Given the focus on Cybersecurity Awareness, you’ve probably been seeing articles and graphics like the “Pump Up Your Password Strength” recently. The articles and graphics pretty much all say the same thing:

- Use strong passwords
- Change your password regularly
- Don’t share your passwords
- Don’t reuse passwords
- Don’t make easy-to-guess passwords

I'll Admit, my Passwords "Were Once Flabby Pathetic Losers"

As someone who's been online since the early 1990s, I've done all of the above, including:

- **Shared a password** (mostly with family) My sister has shared her passwords with me so we could both look at web sites to get my parents a gift.
- **Used only 2 passwords for years** (one where my credit card was used and one where it wasn't—secure, right???) for everything
- **Just used plain, normal, easy-to-lookup words** Heck, before password managers, **who had the bandwidth** to think of different passwords much less remember them?

Hear me now, and Believe me... NOW- Tips to Pump Up Your Passwords

Don't do as Hanz and Franz and "Here me now, believe me later." **Start using sensible, strong passwords now**. We've come up with a few ways to ensure your passwords stay secure:

Choose a Password That is Easy to Remember but Hard to Guess

Duh, that is probably the first thing you thought about. One trick I use is to think of a quote from a favorite movie or book. Imagine Hanz using his catch phrase, “We’re here to pump you up,” and using the first letters of each word. Add a few numbers/symbols, and you have this: “**W’reH2Pyu0418!**”

In this password, **you have all the requisites most secure sites call for**:

- 8 characters or more (this one is 14 and easy to remember)
- Mix of capital and lower-case letters
- Numbers and symbols, such as punctuation marks

Here are a couple more to get you going:

- Goodfellas was my favorite movie when I was 20! – Gwmfmwlw20!6420
- No one likes a tattletale, Danny… except, of course, me. – NoLatt,D… e,of,m.6420

Test Your Password Beast

Then you can test out your password at Password Monster (http://www.passwordmonster.com/) which grades it.

Figure 1: Password Monster gives a rating (Very Strong), how long it would take to crack your code, and a nice comparison saying your password is as secure as...

- **Rating**: I got "Very Strong" for the Hanz quote, the highest rating
- **Time to crack**: PM also shows how long it would take to crack your code (using what means, I'm not sure)
- **Analogy**: As a nice touch, PM says your password is as secure as "Fort Knox". My first password when I started working was deemed "Oh dear, using that password is like leaving your front door wide open," and took 00.03 seconds to crack!

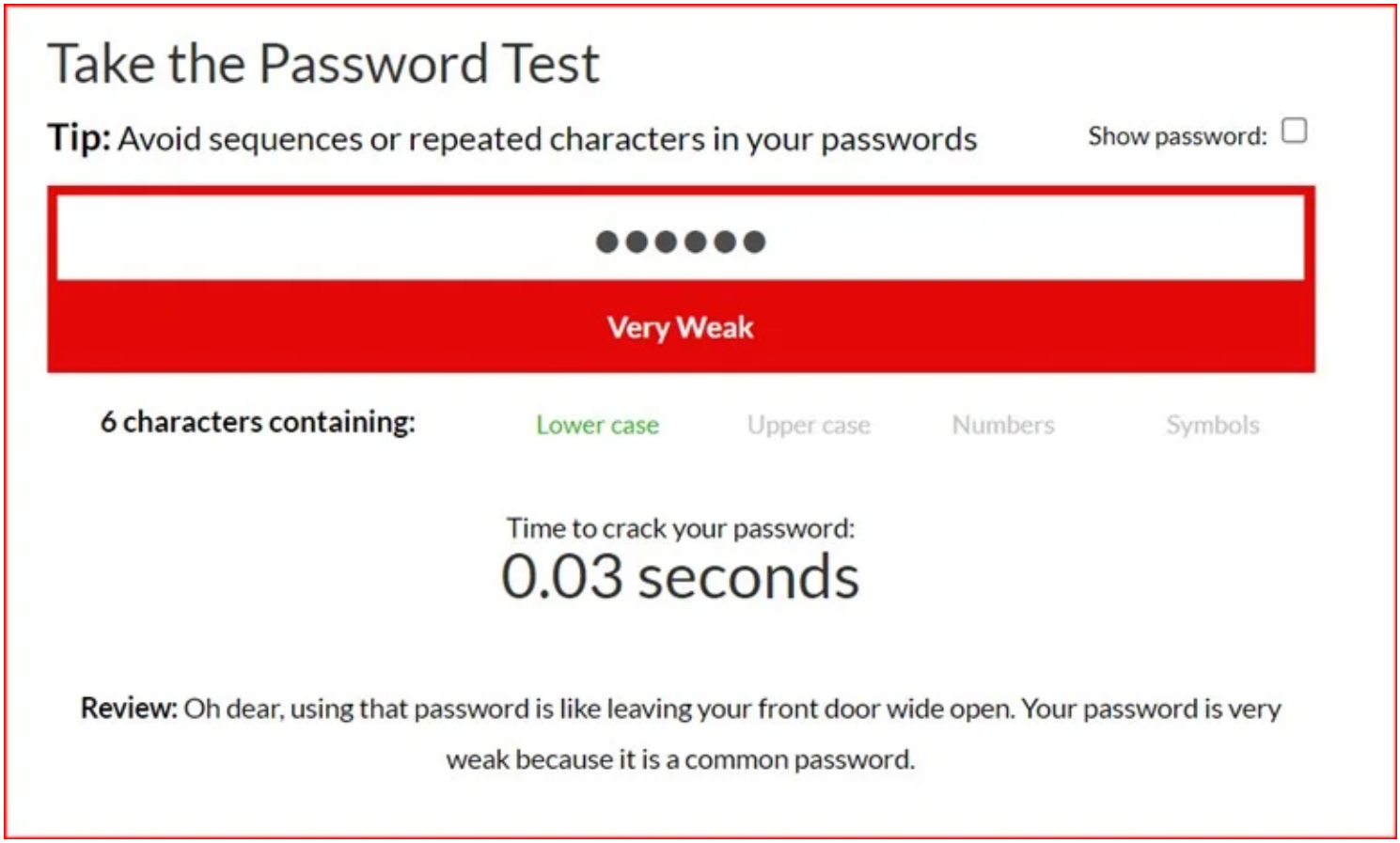

Figure 2: An example of an easy-to-guess password.

Using a Password Manager

Of course, you can't use the same password repeatedly (tell that to my 2010 self). If you've been looking for a password manger, you're in luck because there are several out there, including Apple's iCloud Keychain, Norton Password Manager, browser-built ones, and two-factor authenticators such Google, Microsoft, and Twilo.

The problem arises when you end up having various password managers you must maintain in your life on your various devices. Some are just easier to use depending on the device. For instance, iCloud is built into my iPhone and my personal Mac accounts while in my work account (Windows, Office) I use

Windows' built-in manager. Plus, I've been using Norton forever on my various PCs. And don't get me started on my kid's laptop, my wife's laptop, my parents' home computer, etc. etc. etc.

Sharing your Passwords Between Password Managers

Fortunately, if you have to use multiple password managers, **it's fairly simple (though a hassle) to export passwords back and forth between iCloud and Norton**. Simply go into each client, export your passwords to a *.txt or *.csv file, and save it to your desktop. Then import it into the other password manager.

Tip: *You'll of course either want to zip up and password protect the exported files or delete it with* encryption. In Microsoft Windows, you'll need to download a small app (https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete)*to securely delete the files, or on MacOS 12 (older Macs are easier. Just press the Command key when emptying the Trash):*

1. *Launch Terminal (Applications>Utilities)*
2. *Type sudo rm -rf <add a space>*
3. *Drag the file/folder you want to permanently remove to Terminal, and press Return.*

Are Passwords Going Away?

Not in the immediate future, but according to Knowbe4, **the average employee has to keep track of more than 200 passwords**. Several companies, including Apple, Microsoft, and Google, have been hinting that passwords as we know them are going away. If you've been using biometrics (fingerprints, facial ID) over the past few years, you know that day may be sooner than you think. And thank goodness for that!

Find out how Covestic brings you safe and secure ServiceNow solutions by contacting us. (mailto:servicenow@covestic.com)

A Quick Guide to Automated Testing in ServiceNow: Part I

A Quick Guide to Automated Testing in ServiceNow: Part I In the age of continuous delivery, teams must explore and deploy new testing approaches to stay ahead of the game. With the ServiceNow Automated Test Framework, your team can identify bugs quicker and reduce manual testing requirements to ultimately speed up the development process. Automated ... Continue reading

Covestic - A Milestone Company

Categories: Cybersecurity (https://www.covestic.com/blog/category/cybersecurity/)