

## Why you can't trust password strength meters

By Chester Wisniewski, Senior Security Advisor Sophos

Passwords are a weak link in the computer security chain because they rely on us being good at something we find extremely difficult. And while [we aren't getting any better](#) at choosing strong passwords, password cracking hardware and software continues to improve relentlessly. Website owners can employ a range of measures to help users choose better, stronger passwords and one of the most popular techniques is to include a password strength meter.



The meters are designed to help users understand if their password choices will resist attempts to crack them. The trouble is, they don't quite do that.

### The Theory

The best way to determine how difficult it is to crack a password is to try doing just that. But attempting to crack passwords requires lots of time and lots and lots of processing power, and it isn't a practical solution for websites. The next best option is to try to work out what characteristics passwords that are difficult to crack share, and to check for those instead. Simple password meters check the length and entropy of the password and have checklists for the kinds of things that users are advised to include in their passwords; mixtures of upper and lower case letters, numbers and special characters, for example. That helps determine a password's ability to withstand a brute force attack (an attacker making guesses at random), but being resistant to brute force attacks is only useful if that's what an attacker is going to do, and it probably isn't.

A brute force attack assumes that all guesses are equally good. The reality is that some guesses are far better than others because our password choices are not random - they're underpinned by patterns and habits. Modern password cracking is about making smart guesses in the order that's most likely to yield the greatest number of cracked passwords for the least effort. Attackers can feed their cracking software with huge repositories of real words and then create rules to modify those words in the same way we do when we create passwords.

They know that some words are used more often than others and they know about the cute tricks and bad habits we use to obfuscate them. They know that we use 0s instead of Os and 4s

instead of As, and they know that we tend to put our upper case letters, special characters and numbers at the beginning and end of our passwords. To illustrate the difference, I thought I'd run a test on the kind of password strength meters that web developers are likely to include in a website.

## The Test

I chose five truly awful passwords and then tested them using the first five embeddable password strength meters I found...

## The Passwords

I downloaded a list of the [10,000 most common passwords](#) and quickly chose five that had characteristics I thought password strength meters might overrate:

- **abc123** - number 14 on the list, first to mix letters and numbers
- **trustno1** - number 29, second to mix letters and numbers
- **ncc1701** - number 158, registration number of the [USS Enterprise](#)
- **iloveyou!** - number 8778, first with non-alphanumeric character
- **primetime21** - number 8280, longest with letters and numbers

Be in no doubt, these passwords are dreadful and offer no useful protection; they're short and non-random, they include dictionary words, the numbers are always tacked on the end in a predictable way, and they appear in a list of words anyone can download off the internet. Just in case you're still not convinced about how bad they are I'll show you. I measured how long it takes to crack them using a password cracking program, [John the Ripper](#), with an out-of-the-box configuration running on a normal, two-year-old laptop. The times are rounded to the nearest second:

Password	Time to crack (Day:Hour:Min:Sec)
abc123	0:00:00:00
trustno1	0:00:00:00
ncc1701	0:00:00:00
iloveyou!	0:00:00:00
primetime21	0:00:00:00

They were all cracked instantly, before the first second was up. And I was doing it the slow way - a dedicated password cracker would use [proper equipment](#).

## The meters

To make this as realistic as possible I tested strength meters that come as jQuery plugins. If you asked a web developer to add a password strength meter to your website there's a very good

chance they'd use a [jQuery plugin](#) - a bit of code that can be dropped into almost any website to extend its functionality. I googled [jquery strength meter](#) and picked the first five I came across so, according to Google at least, these are five of the most popular. I've included the same words (abbreviated) and colours that the password strength meters use in my chart:

Password	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>
abc123	Weak	Weak	Good	Weak	Weak
trustno1	Norm.	Weak	Good	Norm.	Weak
ncc1701	Med.	Weak	Good	Weak	Weak
iloveyou!	Med.	Good	Good	Med.	Weak
primetime21	Med.	Good	Good	Med.	Med.

Remember that *it takes 0 seconds to crack any of these passwords*. None of the passwords on my list were anything less than awful. A password strength meter that doesn't reject all five out of hand is not up to the job of measuring password strength. They **all failed**. And not only that, **they don't agree**. There were no good password strength meters in my test but that doesn't mean there aren't good ones out there. Unfortunately, because you don't know which one you'll be using next time you type a password into a website you can't trust any of them. I'm not the only one who's noticed that password strength meters don't deliver. Researchers at Concordia University, Montreal published detailed [research](#) in 2014 that concluded:

In our large-scale empirical analysis, it is evident that the commonly-used meters are highly inconsistent, fail to provide coherent feedback on user choices, and sometimes provide strength measurements that are blatantly misleading.

There is, however, a faint glimmer of hope. [Research from Microsoft](#) that looked at the success of password strengthening techniques in the real world concluded that despite their inadequacies, password strength meters lead to stronger passwords:

Those who saw a meter tended to choose stronger passwords than those who didn't, but the type of meter did not make a significant difference.

So, password meters are not a reliable guide to how likely it is that *your* password will be cracked but they do seem to nudge people in the direction of creating stronger passwords in general.