Passwords Are Not Broken, but How We Choose them Sure Is

schneier.com/essays/archives/2008/11/passwords_are_not_br.html

This essay also appeared in The Hindu.

I've been reading a lot about how passwords are no longer good security. The reality is more complicated. Passwords are still secure enough for many applications, but you have to choose a good one. And that's hard. The best way to explain how to choose a good password is to describe how they're broken. The most serious attack is called offline password guessing. There are commercial programs that do this, sold primarily to police departments. There are also hacker tools that do the same thing.

As computers have become faster, the guessers have got better, sometimes being able to test hundreds of thousands of passwords per second. These guessers might run for months on many machines simultaneously.

They guess intelligently. They don't run through every eight-letter combination from "aaaaaaaa" to "zzzzzzzz" in order. That's 200bn possible passwords, most of them very unlikely. They try the most common password first: "password1". (Don't laugh; the most common password used to be "password".)

A typical password consists of a root plus an appendage. The root isn't necessarily a dictionary word, but it's something pronounceable. An appendage is either a suffix (90% of the time) or a prefix (10% of the time). One guesser I studied starts with a dictionary of about 1,000 common passwords, things like "letmein," "temp," "123456," and so on. Then it tests them each with about 100 common suffix appendages: "1", "4u", "69", "abc", "!" and so on. It recovers about 24% of all passwords with just these 100,000 combinations.

Then the guesser tries different dictionaries: English words, names, foreign words, phonetic patterns and so on for roots; two digits, dates, single symbols and so on for appendages. It runs the dictionaries with various capitalisations and common substitutions: "$" for "s", "@" for "a", "1" for "l" and so on. With a couple of weeks to a month's worth of time, this guessing strategy breaks about two-thirds of all passwords. But that assumes no biographical data. Any smart guesser collects whatever personal information it can on the subject before beginning. Postal codes are common appendages, so they're tested.

It also tests names and addresses from the address book, meaningful dates, and any other personal information. If it can, the guesser indexes the target hard drive and creates a dictionary out of every printable string, including deleted files. If you ever kept an email with your password, or saved it in an obscure file somewhere, or if your program ever stored it in memory, this process will grab it. And it will recover your password faster.

So if you want your password to be hard to guess, you should choose something that this process will miss. My advice is to take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary. Of course, don't use this one, because I've written about it. Choose your own sentence - something personal.

Strong passwords can still fail because people are sloppy. They write them on Post-it notes stuck to their monitors, share them with friends, or choose the same passwords for multiple applications. (I don't care

about low-security passwords here, only about ones that matter: your bank accounts, your credit cards, etc.) Websites are sloppy, too, allowing people to set up easy-to-guess "secret questions" as a backup password or email them to customers.

If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence - or better yet - a hint that will help you remember your sentence. Or use a free program like Password Safe, which I designed to help people securely store all their passwords. Don't feel this is a failure; most of us have far too many passwords to be able to remember them all.

Passwords can still provide good authentication if used properly. The rise of alternate forms of authentication is more because people don't use passwords securely, and less because they don't work any more.