A security patch for your brain

The quickest way to improve online security is to upgrade your mental software

TWO decades ago only spies and systems administrators had to worry about passwords. But today you have to enter one even to do humdrum things like turning on your computer, downloading an album or buying a book online. No wonder many people use a single, simple password for everything.

Analysis of password databases, often stolen from websites (something that happens with disturbing frequency), shows that the most common choices include "password", **"123456"** and "abc1**23".** But using these, or any word that appears in a dictionary, is insecure. Even changing some letters to numbers ("e" to **"3",** " i " to **"1"** and so forth) does little to reduce the vulnerability of such passwords to an automated "dictionary attack", because these substitutions are so common. The fundamental problem is that secure passwords tend to be hard to remember, and memorable passwords tend to be insecure.

Weak passwords open the door to fraud, identity theft and breaches of privacy. An analysis by Verizon, an American telecoms firm, found that the biggest reason for successful security breaches was easily guessable passwords. Some viruses spread by trying common passwords. Attacks need only work enough of the time-say, in 1% of cases-to be worthwhile. And it turns out that a relatively short list of passwords provides access to **1%** of accounts on many sites and systems.

Fingerprint scanners and devices that generate time-specific codes offer greater security, but they require hardware. Passwords, which need only software, are cheaper. In terms of security delivered per dollar spent, they are hard to beat, so they are not going away. But they need to be made more secure.

The solution, say security researchers, is to upgrade the software in people's heads, by teaching them to choose more secure passwords (see page **81).** One approach is to use passphrases containing unrelated words, such as "correct horse battery staple", linked by a mental image. Passphrases are, on average, several orders of magnitude harder to crack than passwords. But a new study by researchers at the University of Cambridge finds that people tend to choose phrases made up not of unrelated words but of words that already occur together, such as "dead poets society". Such phrases are vulnerable to a dictionary attack based on common phrases taken from the internet. And many systems limit the length of passwords, making a long phrase impractical.

An update is ready for installation

An alternative approach, championed by Bruce Schneier, a security guru, is to turn a sentence into a password, taking the first letter of each word and substituting numbers and punctuation marks where possible. "Too much food and wine will make you sick" thus becomes **"2mf**SwwmUs". This is no panacea: the danger with this "mnemonic password" approach is that people will use a proverb, or a line from a film or a song, as the starting point, which makes it vulnerable to attack. The ideal sentence is one like Mr Schneier's that (until the publication of this article, at least) has no matches in Google.

Some websites make an effort to enhance security by indicating how easily guessed a password is likely to be, rejecting weak passwords, ensuring that password databases are kept properly encrypted and limiting the rate at which login attempts can be made. More should do so. But don't rely on it happening. Instead, beef up your own security by upgrading your brain to use mnemonic passwords.

Fonte: The Economist, London, v. 402, n. 8777, p. 18, 24 a 30 Mar. 2012.