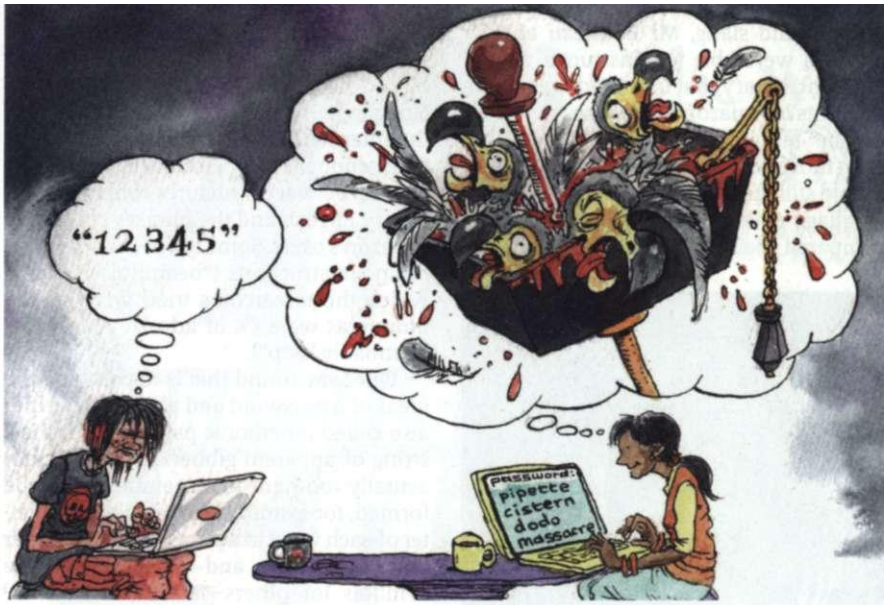

For daily analysis and debate on science and technology, visit
Economist.com/science

Computer passwords

Speak, friend, and enter

Computer passwords need to be memorable and secure. Most people's are the first but not the second. Researchers are trying to make it easier for them to be both

PASSWORDS are ubiquitous in computer security. All too often, they are also ineffective. A good password has to be both easy to remember and hard to guess, but in practice people seem to plump for the former over the latter. Names of wives, husbands and children are popular. Some take simplicity to extremes: one former deputy editor of *The* Economist used "z" for many years. And when hackers stole 32m passwords from a social-gaming website called Rock You, it emerged that *11%* of the site's users-365,000 people-had opted either for "123456" or for "12345".

That predictability lets security researchers (and hackers) create dictionaries which list common passwords, a boon to those seeking to break in. But although researchers know that passwords are insecure, working out just how insecure has been difficult. Many studies have only small samples to work on-a few thousand passwords at most. Hacked websites such as Rock You have provided longer lists, but there are ethical problems with using hacked information, and its availability is unpredictable.

However, a paper to be presented at a security conference held under the auspices of the Institute of Electrical and Electronics Engineers, a New York-based professional body, in May, sheds some light. With the co-operation of Yahoo!, a large internet company, Joseph Bonneau of Cambridge University obtained the biggest sample to date-70m passwords that, though anonymised, came with useful demographic data about their owners.

Mr Bonneau found some intriguing variations. Older users had better passwords than young ones. (So much for the tech-savviness of youth.) People whose preferred language was Korean or German chose the most secure passwords; those who spoke Indonesian the least. Passwords designed to hide sensitive information such as credit-card numbers were only slightly more secure than those protecting less important things, like access to games. "Nag screens" that told users they had chosen a weak password made virtually no difference. And users whose accounts had been hacked in the past did not make dramatically more secure choices than those who had never been hacked.

But it is the broader analysis of the sample that is of most interest to security researchers. For, despite their differences, the 70m users were still predictable enough that a generic password dictionary was effective against both the entire sample and any demographically organised slice of it. Mr Bonneau is blunt: "An attacker who can manage ten guesses per account...will compromise around 1% of accounts." And that, from the hacker's point of view, is a worthwhile outcome.

One obvious answer would be for sites to limit the number of guesses that can be made before access is blocked, as cash machines do. Yet whereas the biggest sites, such as Google and Microsoft, do take such measures (and more), many do not. A sample of 150 big websites examined in 2010 by Mr Bonneau and his colleague Soren Preibusch found that 126 made no attempt to limit guessing.

How this state of affairs arose is obscure. For some sites, laxity may be rational, since their passwords are not protecting anything particularly valuable, such as credit-card details. But password laxity imposes costs even on sites with good security, since people often use the same password for several different places.

One suggestion is that lax password security is a cultural remnant of the internet's innocent youth-an academic research network has few reasons to worry about hackers. Another possibility is that because many sites begin as cash-strapped start-ups, for which implementing extra password security would take up valuable programming time, they skimp on it at the beginning and then never bother to change. But whatever the reason, it behoves those unwilling to wait for websites to get their acts together to consider the alternatives to traditional passwords.

Skysail dactyl gimcrack golem

One such is multi-word passwords called passphrases. Using several words instead of one means an attacker has to guess more letters, which creates more security-but only if the phrase chosen is not one likely to turn up, through familiar usage, in a dictionary of phrases. Which, of course, it often is.

Mr Bonneau and his colleague Ekaterina Shutova have analysed a real-world passphrase system employed by Amazon, an online retailer that allowed its American users to employ passphrases between October 2009 and February 2012. They ••

• found that, although passphrases do offer better security than passwords, they are not as good as had been hoped. A phrase of four or five randomly chosen words (for instance, the headline above) is fairly secure. But remembering several such phrases is no easier than remembering several randomly chosen passwords. Once again, the need for memorability is a boon to attackers. By scraping the internet for lists of things like film titles, sporting phrases and slang, Mr Bonneau and Dr Shutova were able to construct a 20,656-word dictionary that unlocked 1.13% of the accounts in Amazon's database.

The researchers also suspected that even those who do not use famous phrases would still prefer patterns found in natural language over true randomness. So they compared their collection of passphrases with two-word phrases extracted at random from the British National Corpus (a loom-word sample of English maintained by Oxford University Press), and from the Google NGram Corpus (harvested from the internet by that firm's web-crawlers). Sure enough, they found considerable overlap between structures common in ordinary English and the phrases chosen by Amazon's users. Some 13% of the adjective-noun constructions ("beautiful woman") which the researchers tried were on the money, as were 5% of adverb-verb mixes ("probably keep").

Matéria

One way round that is to combine the ideas of a password and a passphrase into a so-called mnemonic password. This is a string of apparent gibberish which is not actually too hard to remember. It can be formed, for example, by using the first letter of each word in a phrase, varying upper and lower case, and substituting some symbols for others-"8" for "B", for instance. C'itaMcoTtit8" is thus a mnemonic contraction of the text in these brackets.) Even mnemonic passwords, however, are not invulnerable. A study published in 2006 cracked 4% of the mnemonics in a sample using a dictionary based on song lyrics, film titles and the like.

The upshot is that there is probably no right answer. All security is irritating (ask anyone who flies regularly), and there is a constant tension between people's desire to be safe and their desire for things to be simple. While that tension persists, the hacker will always get through.

Fonte: The Economist, London, v. 402, n. 8777, p. 81-82, 24 a 30 Mar. 2012.