

## Passwords reconsidered

IT security has its fair share of cherished beliefs that happen to be wrong. One of the most pernicious of these is the myth that conventional passwords are good for securing Internet access. They're not, and this realization is spreading, though a little knowledge can be a dangerous thing. Common "password-strengthening" measures can actually reduce security in online logins.

### Password guessing

Password security and usability tend to conflict, and users usually favour usability over security. A common practice is to impose rules specifying minimum password length and complexity. Password guessing becomes a game of iterating through all possibilities allowed by these constraints, like clicking through every setting of a combination lock until it opens. The search space for a four-digit numeric PIN consists of 10,000 possibilities, while that for a non-case-sensitive ten-character alphanumeric password it is 3,656,158 billion. Superficially the longer password looks like a better security bet.

However, in 1959 the psychologist George Miller observed that people can only retain about seven chunks of information in working memory. Subsequent research suggests this number is actually closer to four. As passwords get longer and more arbitrarily structured, so it becomes cognitively harder to analyse them into a few memorable chunks.

### Password disclosure

Increasing the structural complexity of online passwords adds little to security and can actually trigger their disclosure. Authentication guru Richard Smith examined workplaces to see if he could find employees' passwords written under their mouse mats or elsewhere amongst desktop items. Alarming, he discovered written passwords at up to 39% of workstations, with the higher incidences reflecting the memorization difficulty of those companies' specific password policies.

It isn't just human memory limitations that facilitate password disclosure. Research has shown that the best visual deception phishing attacks can fool even the most sophisticated users. Conventional 'password-strengthening' measures offer no added protection whatsoever against social engineering phishing attacks.

Keystroke-logging viruses and physical keyloggers don't even require users to be careless. Undetected, they monitor keyboard input, collecting login credentials. A 'strong' twelve-character alphanumeric and special characters password provides no more protection than a four digit PIN against a well-constructed phishing or keystroke-logging attack.

### Password shareability

Password structure constraints need to be relegated to the second tier of security checklist items. Beyond four or five character length, password guessability has always been a questionable security criterion in applications that lock users out after a few failed attempts. In today's threat landscape, it is *shareability* that defines a password's security. A solution that allows passwords to be shared, accidentally or deliberately, with an unauthorized party is asking for trouble.

Even the number of authentication factors must be subordinated to shareability. Though conventional wisdom tells us that security increases as authentication factors are added, this is almost always contingent on user behaviour and/or the security of the input infrastructure. A two-factor Internet login solution fails the shareability test if the credentials can be hijacked at point of entry by a fake website or a Trojan virus.

Online services need password solutions that correctly diagnose the core requirement of password security as *low shareability*. Low shareability solutions provide each user with a unique login environment, without which their password cannot readily be entered, or even expressed. Tricerion's SafeLogin solution passes the low shareability test with flying colours. Very easy to understand and use, its innovative patented login offers outstanding protection against all known online authentication risks.