

1 July 2009

By: Lucian Constantin, Web News Editor



The necessity of password field masking placed under doubt  
Apple (for MacOS X-themed login prompt)

## [Masking Passwords: Good or Bad Debate](#)

### *Computer experts argue over the pros and cons of the practice*

Various experts in areas such as usability, cryptography and security entered a debate over the necessity of masking passwords, a standard practice dating back to the beginning of the Internet. People on both sides of the barricade bring compelling arguments to the table.

The practice of masking passwords is so common and dates so far back, that many users might not even realize what it means or that there is an alternative to it. It involves replacing passwords, or, better said, access codes, with a string of asterisks or bullets.

The issue of whether passwords should continue to be hidden in web forms or not was brought up by world-renowned web usability expert Jakob Nielsen, who considers it an unnecessary legacy design. "Password masking has become common for no reasons other than (a) it's easy to do, and (b) it was the default in the Web's early days," he [claims](#).

Mr. Nielsen argues that, "There's usually nobody looking over your shoulder when you log in to a website. It's just you, sitting all alone in your office, suffering reduced usability to protect against a non-issue." According to him, this outdated convention raises several problems.

First of all, he explains that, by not being able to see what is being typed in a form field, the chance of errors occurring increases, which ultimately leaves users frustrated. Furthermore, this decrease in confidence causes users to choose overly simple passwords or resort to copy-pasting them from a file, both actions reflecting "a true loss of security."

Cryptography guru Bruce Schneier agrees with Nielsen and [maintains](#) that, "Shoulder surfing isn't very common, and cleartext passwords greatly reduces [sic.] errors. It has long annoyed me when I can't see what I type: in Windows logins, in PGP, and so on." In order to clarify, he stresses that, "I'm not talking about PIN masking on public terminals like ATMs. I'm talking about password masking on personal computers."

Jakob Nielsen has also considered scenarios where users are exposed to the prying eyes of bystanders, such as in Internet cafes. His solution to this is "offering them a checkbox to have their passwords masked." He goes on to note that, "For high-risk applications, such as bank accounts, you might even check this box by default."

Graham Cluley, senior technology consultant at Sophos, joins the discussion, [saying](#) that, "I'm afraid that wise as these two gents are, I have to disagree with them." The security expert notes that the additional checkbox might lead to "awkward social positions," like when logging in from a friend's computer, without wanting them to see your password.

Mr. Cluley also brings forth other scenarios where password masking should be a must, like when an IT staffer needs to log in on your work computer with an admin password in order to fix something with you being present. "I bet I'm not the only one to be sitting in a completely open plan building - anyone could be passing by and looking over my shoulder," he also points out.

Additionally, the security researcher notes that the masking of password fields is actually

performed by browsers and not websites. "If there were an option to display password input fields as cleartext rather than asterisks, then that should be set in the user's browser not decided by individual websites," he concludes.

Trend Micro's Solutions Architect, Rik Ferguson, feels the same as Mr. Cluley about this. "The vast majority of the global office population are definitely not fortunate enough to be sitting secure in their own private office," he [writes](#). "Even if it were true that shoulder-surfing is not common, isn't that partly because it serves little purpose when passwords are masked? Chicken or egg Mr. Schneier, Mr. Nielsen?" the researcher rhetorically asks.

Mr. Ferguson goes on to point out that, "Password masking is also an effective method of defeating malware, which is designed to take snapshots of the users screen, which has long been a way that banking Trojans have overcome virtual or on-screen keyboards."

Both sides made good points, however, so far one thing is clear - this is a sensitive issue that should be carefully analyzed. Even Mr. Nielsen is aware that security should outweigh comfort. "In cases where there's a tension between security and usability, sometimes security should win," he writes.

As usual, we encourage you to comment on subjects of significant public interest, such as this one.