Yahoo announces innovative authentication mechanism Yahoo announced recently, a new method of authentication for its services that relies solely on an on-demand generated password that is sent to the user's mobile phone number.
This is not two-factor authentication (which Yahoo already had), but rather single-factor authentication where the single factor is the user's mobile phone.

Yahoo announced recently, a new method of authentication for its services that relies solely on an on-demand generated password that is sent to the user's mobile phone number. This is not two-factor authentication (which Yahoo already had), but rather single-factor authentication where the single factor is the user's mobile phone. It seems that if someone obtains temporary access to a user's unlocked phone they could generate a Yahoo one-time password that allows them to log in. CNET also reports that the temporary password is 4-characters long, though since it's temporary and Yahoo likely has anti-brute force protections that might not be a problem. *TK Keanini, CTO at Lancope advises that; "We need more innovation like this with authentication. Passwords are just pieces of information and in all these strategies, we want to make it useful for the shortest amount of time but not be an administrative burden. Yahoo knows that the most personal device on a person these days is their mobile phone and let's not stop here, let's keep innovating even more techniques to raise the cost to our attackers. While only leveraging a single factor (something you have - your phone), the security of the system will depend on how secure that device remains over time. We will see a major shift by the

attacker to target malware on these mobile platforms because of their larger role in the overall security of the individual. It is also important these days to ensure that the mobile account is secure because you don't want attackers changing features like call forwarding and other features that can put them in the middle of this communication stream." *Jared DeMott, principal security researcher at Bromium provided further ndorsements to this type of innovation, commenting that, "Passwords have been the weak link in many security incidents. Recall the celebrity pictures stolen a while back due to password resets. Even so, users have not rushed to the more secure two-factor authentication, because it is an extra step that they must do (or even know about, and know how to enable). Also, some users have expressed concern about providing a personal mobile number to ad companies like Yahoo!, Google, Facebook, etc. Either way, it seems most users will do only what is required by default. So if companies are serious about better login security, the default choice will need to be modified. In light of that, it is good to see Yahoo! trying to address the password problem. Potential drawbacks are of course: users without a txt/data mobile, lost phones, etc - could now cause new grief. But in engineering, it’s about balancing the gains against the losses. Time will tell if this is a better choice. Certainly when Yahoo! first started offering email, many users would not have had a mobile to do two-factor with. Now, many will. Times change. So must appropriate login measures. But balancing privacy, easy-of-use and recovery, against security is always the trick."