Forgot Password Discussion

The two cases both demonstrate vulnerability, but the vulnerability they show can be classified to be different. In the first case we can say there is a vulnerability in procedure and implementation that is by clicking on forgot password, there should be some form of identification done to verify if the subject is indeed the true user, and then an authentication process in terms of personal questions or some other unique verification then the password can be sent. In the second case the vulnerability is in design. If the user inputs a new form of identification, he can be linked to a subject, which might not be the true subject. Another flaw is the attacker could reset your password before you even know you have an email, because the system allows it. Thus if the attacker have the ability to pass these; ask users to complete a CAPTCHA, to demonstrate that they are human, ask users to enter a PIN which is sent to their personal e-mail address or mobile phone, require use of another technology, such as a one-time-password token, or leverage biometrics, such as a voice print. If in both cases the system will be vulnerable.