Forced Alpha-Numeric User IDs

Asked 16 years, 3 months ago   Modified 8 years, 1 month ago

Viewed 722 times

▲

3

▼

🔖

🕘

I am a programmer at a financial institute. I have recently been told to enforce that all new user id's to have at least one alpha and one numeric. I immediately thought that this was a horrible idea and I would rather not implement it, as I believe this is an anti-feature and of poor user experience. The problem is that I don't have a good case for not implementing this requirement.

Do you think this is a good requirement?

Do you have any good reasons not to do it?

Do you know of any research that I could reference.

> Edit: This is **not** in regards to the password. We already have similar requirements for that, which I am not opposed to.

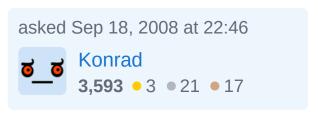`security` `web-applications` `finance` `user-experience`

Share

Improve this question

Follow

Do you mean the username or password when you say "userID?" – ine Sep 18, 2008 at 22:48

Username, we already have similar (however more strict) requirements for the password. – Konrad Sep 18, 2008 at 22:56

9 Answers

Sorted by: Highest score (default) ⇕

▲

4

▼

🔖

✓

🕓

One argument against this is that many usernames / ids in other areas do not require numeric components. It's more likely that users will be better able to remember user ids that they have used elsewhere -- and that is more likely if they do not need to include numerics.
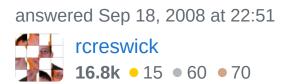
Furthermore, depending on the system, the user ids may work well as defaults when connecting to external systems (ssh behaves this way under unix-like systems). In this case, it is clearly beneficial to have one ID that is shared between systems.

Using the same ID in multiple places improves consistency, which is a well-known aspect of good software interfaces. It's not too difficult to show that the way people interact with a system *is* a user-interface, and should adhere to (at least some) of the well-known interface guidelines. (Obviously ideas like keyboard

shortcuts are meaningless if you're considering the interactions between multiple, possibly unknown, systems, but aspects such as consistency *do* apply.)

Edit: I'm assuming that this discussion is about usernames or publicly visible IDs, *NOT* something that pertains directly to security, such as passwords.

Share Improve this answer

Follow

I would begin by asking them for their specific reasons behind this. Once you have a list of bullet points and the reasons why, it's easier to refute or provide alternatives.

4

As for general ideas:

- This is opinion, but adding a numeral to a username won't necessarily increase security. People write down usernames on post it notes, most users will just add a '1' to the beginning or end of their username, making it easy to guess.

- From a usability standpoint, this is bad as it breaks the norm. Forcing them to add a numeral to their username will just lead to the above point. They will simply add a '1' to the end or beginning of their username.

Remember, the more complex an authentication system is, the more likely a general user is to find ways to

circumvent it and make their link in the chain weak.

Share   Improve this answer

Follow

UserIDs? Requiring passwords to be alphanumeric is generally a good idea, since it makes them more resistant to a dictionary attack. It doesn't really make any sense for usernames. The whole point of having a name/password combo is that the name part doesn't have to be kept secret.

Share   Improve this answer

Follow

If you're working at a financial institution, there are probably regulations about this sort of thing, so it's most likely out of your hands. But one thing you can do is make it clear to the user when he has entered an invalid ID. And don't wait until he clicks submit; show some kind of message right next to the field, and update it as he types.

Share   Improve this answer

Follow

A few of the answers above have a counter-argument: If the users pick the same username they use on the other sites, then they are also likely to pick the same or similar passwords for the financial site, lowering security.

A reason not to do it: If you impose more restrictions than they are used to on the users, they will start writing down the login information, and that's an obvious loss of security.

Both of the bank accounts I have require an alphanumeric username and two passwords for the online login. One of them also has a image I have to remember. The two passwords have to change once a month or so. Therefore, I have all the login information right here on a text file. (Even looking at it doesn't make any sense; I'll have to go down to the bank and reset my passwords again. That's a grand total of 7 password resets for 6 logins. Talk about security, not even *I* can access my account.)

Share   Improve this answer

Follow

answered Sep 19, 2008 at 7:16

aib
46.8k ● 10 ● 74 ● 79

it's good if it's in their password (as alas, financial companies like to deny you this security right [i'm talking to you american express]).

username, i say no, unless they want to.
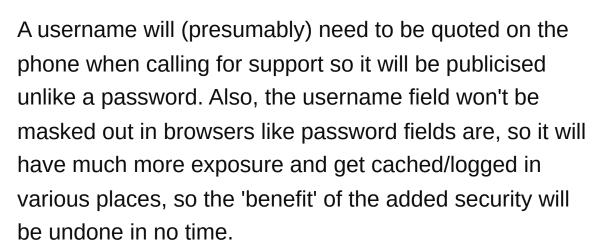
Share   Improve this answer

Follow

Interesting, I don't have that problem with Amex
– Luke Bennett Sep 18, 2008 at 22:50

0

A username will (presumably) need to be quoted on the phone when calling for support so it will be publicised unlike a password. Also, the username field won't be masked out in browsers like password fields are, so it will have much more exposure and get cached/logged in various places, so the 'benefit' of the added security will be undone in no time.

And the more difficult you make things, the more likely a user is to write it down somewhere which again undermines security (same applies for password policies actually, but that's another story!)

Share   Improve this answer

Follow

0

I also work at a financial institution and our usernames (both real people and production IDs) are all lowercase, alphabetical, up to 8 characters and I've never considered it a problem... avoids the confusion of 0 vs O, 1 vs I, and

8 vs B - unless you work for the same company as me and are about to implement a new policy...

Share Improve this answer

Follow

answered Sep 18, 2008 at 23:21

mxsscott

403 ● 3 ● 8

Adding any feature adds costs. It will take time now to build and test it, and in the future to support it. No feature should be built without a really good reason.

This feature is pointless. Usernames are not supposed to be kept secret, so having strong usernames has no advantage. It is probably worth spending time making passwords (or other authentication factors) strong, but users should be able to communicate their username to other users without that being a security risk.

If your application imposes extra constraints on the choice of user ID then some of your users will have a different user ID for your application than for the other applications in your environment. Note: I'm assuming that this is an internal application (for use by employees) rather than in Internet-facing application.

Having inconsistent usernames adds a number of specific risks:

1. It will make the audit trail harder to follow (a serious security risk).

2. It may add cost if you later start using single sign on.

3. It will cause a bad user experience as users have to remember that this application uses a weird username.