# Forum:Hack Forums

Thread: Change trust scan color

**Crystallize.** - *May 20, 2018, 11:32 am*
So what I mean is this:
http://prntscr.com/jkbzk3
My last 2FA Validation was long time ago I think that should be green and recent 2FA validations be red.Would be better for the eye imo.

**FamousHater** - *May 20, 2018, 11:33 am*
(May 20, 2018 11:32 AM)Crystallize. Wrote: *[CITE]* So what I mean is this:
http://prntscr.com/jkbzk3
My last 2FA Validation was long time ago I think that should be green and recent 2FA validations be red.Would be better for the eye imo.
i agree its pretty stupid to make it green only if u validate it every other day

**Vitani** - *May 20, 2018, 11:37 am*
Maybe the color yellow could be added for validations within the last week or so, but it doesn't really matter a lot. Not so much that it would require a change.

**Crystallize.** - *May 20, 2018, 11:43 am*
(May 20, 2018 11:37 AM)Vitani Wrote: *[CITE]* Maybe the color yellow could be added for validations within the last week or so, but it doesn't really matter a lot. Not so much that it would require a change.
Yeah but still why should it be red if I validated months ago... green would be better because it means that none else accesed it. :)

**4158996621556** - *May 20, 2018, 11:48 am*
we're not falling for your tricks.
guys dont deal with him as u can see from the trust scan his account is HACKED.
it doens't even match his ip which he registered this account 2 years ago!
deal with caution use middleman!

seriously though the 2fa thing, i always hated that.
like im always logged in, i dont have to login and confirm 2fa just for giggles cmon
plus the "matching registratoin ip"
USELESS! if someone registered in 2009, do you think they'll have the same ip? 2014? even a year.
theres no way youll always have the same ip.
or am i missing something

**webdev77** - *May 20, 2018, 11:54 am*
(May 20, 2018 11:32 AM)Crystallize. Wrote: *[CITE]* So what I mean is this:
http://prntscr.com/jkbzk3
My last 2FA Validation was long time ago I think that should be green and recent 2FA validations be red.Would be better for the eye imo.
No. Recent should remain green. Always require users to verify their account before dealing with them.

**Crystallize.** - *May 20, 2018, 12:07 pm*
(May 20, 2018 11:54 AM)webdev77 Wrote: [CITE] No. Recent should remain green. Always require users to verify their account before dealing with them.
Green is for good...

**FamousHater** - *May 20, 2018, 12:10 pm*
(May 20, 2018 11:54 AM)webdev77 Wrote: [CITE] No. Recent should remain green. Always require users to verify their account before dealing with them.
If i validate my account 2 days ago then why would it need to be red...

(May 20, 2018 11:48 AM)HackingDoge Wrote: [CITE] we're not falling for your tricks.
guys dont deal with him as u can see from the trust scan his account is HACKED.
it doens't even match his ip which he registered this account 2 years ago!
deal with caution use middleman!

seriously though the 2fa thing, i always hated that.
like im always logged in, i dont have to login and confirm 2fa just for giggles cmon
plus the "matching registratoin ip"
USELESS! if someone registered in 2009, do you think they'll have the same ip? 2014? even a year.
theres no way youll always have the same ip.
or am i missing something
lol u a fool

your lucky hf has 2fa as hf accounts used to be hacked all the time

**Xerotic** - *May 21, 2018, 2:11 pm*
That stat is used to help verify account ownership and you should consider the 2FA activation date as well.

Example:
2FA Enabled: 2015
Last 2FA Validation: Today (2018)

If you consider both of those stats then it is likely that the same user has had control of the account between the above dates.

Since online accounts can be compromised in many ways having different stats for different account security settings is important. The row that you want color switched is done in the "2FA Enabled" row. That shows length of time enabled. The latest 2FA validation is just that - proving that they have 2FA access as close to the time you are doing the deal as possible (aka: present time).

**Elitas** - *May 21, 2018, 3:01 pm*
(May 21, 2018 02:11 PM)Xerotic Wrote: [CITE] That stat is used to help verify account ownership and you should consider the 2FA activation date as well.

Example:
2FA Enabled: 2015
Last 2FA Validation: Today (2018)

If you consider both of those stats then it is likely that the same user has had control of the account between the above dates.

Since online accounts can be compromised in many ways having different stats for different account security settings is important. The row that you want color switched is done in the "2FA Enabled" row. That shows length of time enabled. The latest 2FA validation is just that - proving that they have 2FA access as close to the time you are doing the deal as possible (aka: present time).
To be fair, so long as the account has not been logged in with 2fa for a while, the only way it can be accessed it if the user's cookie has be stolen. In the event of a RAT or some sort of XSS attack, which isn't necessarily too common.

Honestly though, if a RAT is the case, it doesn't even matter if they validated their account recently, their cookie session/entire account is still at risk, and the same with an XSS attack all the same, the only difference is if someone has access to their account and then they logout and back in, they can change that.

I honestly fail to see any method of taking over someone's account without logging into it using their 2fa/user/pass (which is REALLY hard to get), in which their 2fa doesn't need to be validated. What I mean is, that assuming 2fa is safe, there aren't too many other attacks to takeover an account, and of those attack which do exist, confirming account ownership regularly with 2fa won't really change much at all.

Although I may not be thinking of the topic on a 'trust-level', as I guess there is an argument that is would make the user appear more trustworthy, but I am curious what potential untrustworthiness could come from not logging in with a 2fa regularly, certainly nothing which a malicious attacker could use..