

Forum:[Hack Forums](#)

Thread: [Perfect Security Idea](#)

Omniscient - June 27, 2011, 3:46 pm

I finally just came up with a perfect security idea.

A secondary email address that's non-changeable and encrypted in the database.

The secondary email if used will reset the password.

It's perfect as long as members remember their secondary email addy.

I can't work on this idea now but I think it's a real winner.

Too many members come up with ideas that they aren't aware are either difficult to implement or would cause more problems than help.

hxxkd - June 27, 2011, 3:47 pm

Sounds good Omni! I hope it keeps hackers away.

hxxkd

EDIT:

Sorry for LQP but I had to be the first person to post :).

King - June 27, 2011, 3:48 pm

I think that it's a good idea, Omni.

But, I guess, there are some better ideas, imo.

Edit: You're right. This is the best possible idea that doesn't require a lot of work.

Moralitas - June 27, 2011, 3:48 pm

But what if someone gets access to an account before the user had added this? Like the day you add it to the site.

Edit: Quote:Too many members come up with ideas that they aren't aware are either difficult to implement or would cause more problems than help. Too many members don't search, nor think before suggesting. That section needs some kind of additional feature like an approval system, and after the approval, administrators look at it.

eight - June 27, 2011, 3:49 pm

I like it, the only problem is the remembering part for members.

I recommend they write in notepad and just save it.

RDCA - June 27, 2011, 3:50 pm

Couldn't this screw over an account though? What if the "hacker" sets his email as the second email. Then he will have constant over right.

Riggs - June 27, 2011, 3:50 pm

I'd give Omni a Blue Peter badge if he new what it was.

S70N3R - June 27, 2011, 3:50 pm

Just say the users Secondary email is compromised?

Mr Kewl - June 27, 2011, 3:51 pm

This sounds really good.

And Suggestion : Make a secondary account use only for HF>

Nov - June 27, 2011, 3:51 pm

Something like the gmail system? That would be good. Just today I forgot my gmail password and would have been in trouble on for having a secondary email.

JrSadFish - June 27, 2011, 3:53 pm

sounds cool. But a bit confusing.

Moralitas - June 27, 2011, 3:54 pm

(Jun 27, 2011 03:53 PM)JrSadFish Wrote: [\[CITE\]](#) sounds cool. But a bit confusing. You will have the ability to reset the password with that secondary e-mail. The secondary e-mail cannot be changed, and it cannot be viewed because it's encrypted. No matter what happens, if you're the original owner, you will get access to the account.

King - June 27, 2011, 3:55 pm

(Jun 27, 2011 03:54 PM)Peter Chao Wrote: [\[CITE\]](#) You will have the ability to reset the password with that secondary e-mail. The secondary e-mail cannot be changed, and it cannot be viewed because it's encrypted. No matter what happens, if you're the original owner, you will get access to the account. But, you stated something important in your previous post.

What if the hacker sets-up that email?

?????-?u??? - June 27, 2011, 3:56 pm

Couldn't you implement a required secondary password, that can only be entered via on-site keyboard?

Thatd made account stealing nearly impossible.

BaussHacker - June 27, 2011, 4:01 pm

I thought there already was something like this.

Anyways, that's a good idea and I will look forward to it.

But I'm already secured like this, at least for my mail. As I got 3 emails connected to it.

Moralitas - June 27, 2011, 4:02 pm

(Jun 27, 2011 03:56 PM)Nibbles Wrote: [\[CITE\]](#) Couldn't you implement a required secondary password, that can only be entered via on-site keyboard?

Thatd made account stealing nearly impossible. Here's what I like about that, if you're key logged, other user won't be able to see that. If you're ratted, user may not see it either if the keyboard doesn't show last pressed button, and if you're fast enough, the mouse will be at another key.

This is a good idea for a 'pin', but not a secondary password. This pin would be like the previous secret answer, would need it to change password, etc.. The pin can be user desired since it's hard to remember pins generated by the computer, especially when they contain letters.

Edit: Thanks Nibble, implying this on my site, lol. Have to see how a on-site keyboard would work.

Qwazz - June 27, 2011, 4:05 pm

Sounds good to me. As long as we're safe thats what really matters.

Omniscient - June 27, 2011, 4:07 pm

Quote:Couldn't you implement a required secondary password, that can only be entered via on-site keyboard?

Thatd made account stealing nearly impossible.

WE already have that...secret word. Which is currently disabled while I help recover accounts.

ra1d - June 27, 2011, 4:08 pm

(Jun 27, 2011 03:56 PM)Nibbles Wrote: [\[CITE\]](#) Couldn't you implement a required secondary password, that can only be entered via on-site keyboard?

Thatd made account stealing nearly impossible.

This is possibly the most secure way.

2buckz - June 27, 2011, 4:08 pm

Good idea honestly - it'd work out perfectly.

Moralitas - June 27, 2011, 4:09 pm

(Jun 27, 2011 04:07 PM)Omniscient Wrote: [\[CITE\]](#) WE already have that...secret word. Which is currently disabled while I help recover accounts.If you're keylogged, the cracker may get the answer to the secret word. If that's replaced with an on-site keyboard, it's better.

King - June 27, 2011, 4:10 pm

(Jun 27, 2011 04:09 PM)Peter Chao Wrote: [\[CITE\]](#) If you're keylogged, the cracker may get the answer to the secret word. If that's replaced with an on-site keyboard, it's better.Why don't you use Keyscrambler?

Check the thread in my sig. It contains a lot of precious information.

Moralitas - June 27, 2011, 4:11 pm

(Jun 27, 2011 04:10 PM)-BoodyE- Wrote: [\[CITE\]](#) Why don't you use Keyscrambler?

Check the thread in my sig. It contains a lot of precious information.Have you ever tested it yourself? Keylog yourself while you have Keyscrambler.

ra1d - June 27, 2011, 4:11 pm

(Jun 27, 2011 04:07 PM)Omniscient Wrote: [\[CITE\]](#) WE already have that...secret word. Which is currently disabled while I help recover accounts.

I think you misunderstood he's suggestion.

What he is trying to say is that we need a secondary password in order to change the originally password.

But the secondary password can only be entered via a keyboard that is on the website.

Just like on Liberty Reserve.

Picture example: [\(Click to View\)](#)

[img]http://i.min.us/ibDO4e.png[/img]

idonotcare - June 27, 2011, 4:12 pm

Make a pin and a master pin.

Pin = Chaning password and e-mail

Master Pin = Changing master encrypted e-mail

King - June 27, 2011, 4:13 pm

(Jun 27, 2011 04:11 PM)Peter Chao Wrote: [\[CITE\]](#) Have you ever tested it yourself? Keylog yourself while you have Keyscrambler.

It works in Firefox, IE and a few other programs. You have to purchase premium in order to make it to work in all the programs.

It's proved to be working.

Zeon - June 27, 2011, 4:14 pm

What if the attacker gains access to the secondary email though?

ra1d - June 27, 2011, 4:15 pm

(Jun 27, 2011 04:13 PM)-BoodyE- Wrote: [\[CITE\]](#) It works in Firefox, IE and a few other programs. You have to purchase premium in order to make it to work in all the programs.

It's proven to be working.

Not everyone have the funds to buy such software.

King - June 27, 2011, 4:17 pm

(Jun 27, 2011 04:15 PM)Rand0m™ Wrote: [\[CITE\]](#) Not everyone have the funds to buy such software.

You can get it for free. It will still work with IE and Firefox.

Chutiya hun mien - June 27, 2011, 4:17 pm

What if a hacker still has access to some account and sets it up, the real owner is then fucked? Why not keep security questions? Just send the security question set up link to the EMAILS of current users so they are the ones who set them up and recover their accounts when ever they lose access to them.

Etheryte - June 27, 2011, 4:35 pm

Secondary email somehow being compromised, might be through other means, not through the site, e.g. the member getting infected, would thus result in the account being compromised permanently?

I fail to see how this is a perfect solution.

Asatru - June 27, 2011, 4:37 pm

That sounds like a really good idea and no I'm not ass kissing.

Moralitas - June 27, 2011, 4:38 pm

(Jun 27, 2011 04:35 PM)Etheryte Wrote: [\[CITE\]](#) Secondary email somehow being compromised, might be through other means, not through the site, e.g. the member getting infected, would thus result in the account being compromised permanently?

I fail to see how this is a perfect solution. Only the user that set the mail knows it's a secondary e-mail to reset. I assume it will not send a confirmation to the e-mail saying this is your secondary e-mail for HackForums.

Kotei - June 27, 2011, 4:39 pm

Will the secondary email be displayed in UserCP? Because if it is, someone that has access to someone else's account can simply find that email, then try to crack it or steal it, then they are fucked all the same.

Moralitas - June 27, 2011, 4:39 pm

No it won't, otherwise it's pointless. It will be encrypted in the database.

-Dartz - June 27, 2011, 4:40 pm

(Jun 27, 2011 03:46 PM)Omniscient Wrote: [\[CITE\]](#) I finally just came up with a perfect security idea.

A secondary email address that's non-changeable and encrypted in the database.

The secondary email if used will reset the password.

It's perfect as long as members remember their secondary email addy.

I can't work on this idea now but I think it's a real winner.

Too many members come up with ideas that they aren't aware are either difficult to implement or would cause more problems than help.

Don't you think that has it's downside too?

Usually, if a HF account is hacked, it's RAted. A simple stealer / keylogger on most cases would make this security feature useless. Unless I'm thinking of this differently than you, it seems like it will only work against the hackers with little to no common sense.

SavageBoys - June 27, 2011, 4:47 pm

Sounds about right to me.

Use an alias/fake address/fake DOB then screenshot the info and save it to a flashdrive.

Then make two txtfiles one with the pass and the other with the email but instead of typing it IN the textfile put the info as the name and rename the extension .password and .email and place them on said flashdrive.

At least thats what I did.

Can't steal info from a piece of hardware thats not connected.

Dolus - June 27, 2011, 4:52 pm

I'm not sure if these points have already been raised, discussed or answered but, I will put them out there none the less.

What happens when these non-changeable email accounts are compromised?

How will you encrypt the email and where will the encryption key be stored?

What is the difference between this and a normal email other than the email being stored under encryption?

I also don't understand the point of encrypting the email seeing as if I had access to the database I could just update the row to my own hash or, even better: edit the login script to capture and store login post data in the clear text form.

I will expand on this but, I am a little tired to think too deep.

Morchid - June 27, 2011, 4:55 pm

Seems to be a great idea. Hopefully we don't have to deal with this security problems again :)

PhirewireNET - June 27, 2011, 4:55 pm

Honestly if you are gonna implement this, i would have the secondary email something from you;

Hackmail.net or something; have it so you can't change its password or anything and it has to be attached to hackforums email.

Southern Proper - June 27, 2011, 4:56 pm

Sounds great! Simplicity at it's finest!

Maurice Moss - June 27, 2011, 4:58 pm

I remember someone made a post that each user should have a username and a display name, and you can only log in with the username. That sounded like a good idea imo.

Kenji Harima - June 27, 2011, 5:00 pm

Well instead of a secondary email why not have it send a sms to a phone number or something? Emails can always be hacked.

Maurice Moss - June 27, 2011, 5:01 pm

(Jun 27, 2011 05:00 PM)Micro Life Wrote: [\[CITE\]](#) Well instead of a secondary email why not have it send a sms to a phone number or something? Emails can always be hacked.

Not everyone has a cell phone.

Skyset - June 27, 2011, 5:06 pm

An alternative e-mail is always good, as well as a security question. You should add both. =)

Godsent - June 27, 2011, 5:06 pm

Very good idea,
I'd like to see this put in action.

.[Preservation]. - June 27, 2011, 5:15 pm

I think the secondary email is close to flawless, if implemented in the account creation process. I'm not sure how hard that would be to implement, but it would protect new members quite well.

To everyone asking what would happen if the secondary email was compromised. First, I would imagine that this email would ONLY be used for this purpose. If a hacker we're to aim at hackforums, or more likely a specific member and got a keylogger or a rat onto the member's computer it wouldn't do them any good, as the user would never access the email. Second the database was hacked again, they would just have email addresses they couldn't do anything with.

Just my two cents.

robife - June 27, 2011, 5:19 pm

More secure it will be by phone, SMS. something like facebook.

?Dunsparth - June 27, 2011, 5:26 pm

Wow amazing idea.

Good thoughts omni.
Keep up the good work

Barneyyz™ - June 27, 2011, 5:29 pm

That's a not too bad idea Omnomin, but what if those secondary emails get compromised? doubting they will, but surely there is a small chance?

Quote:What he is trying to say is that we need a secondary password in order to change the originally password.

That's secret word. You can't change your email OR password without secret word. It's a second password to secure account info. Members often forget it though.

Quote:But the secondary password can only be entered via a keyboard that is on the website. Not sure I want to deal with that.

Quote:What if the attacker gains access to the secondary email though?

What if someone puts a gun to your head and makes you tell. I can't prevent everything. What I can do is find reasonable solutions that will benefit account security without causing more problems then they solve.

Quote:Secondary email somehow being compromised, might be through other means, not through the site, e.g. the member getting infected, would thus result in the account being compromised permanently?

And how would they know the secondary email? Sorry but if people here can't keep a secret email secret. That's not my problem. It will be encrypted in the database making it very difficult to decrypt as email addresses in general are many characters.

And this is a safety net. It's not a 100% security solution.

For the secondary email to work you will need to enter it along with your uid. If there is a match I'll have a password reset occur. However it's unlikely I'll even have a success/fail message.

Quote:Will the secondary email be displayed in UserCP?

No. Completely encrypted and not changable in usercp. You set it and don't forget it.

Quote:Usually, if a HF account is hacked, it's RATed. A simple stealer / keylogger on most cases would make this security feature useless.

Again I can't protect members from all contingencies.

Quote:What happens when these non-changeable email accounts are compromised?

What happens now when an account is compromised? You contact staff.

The issue is allowing members more ways to identify when their accounts are stolen and then methods to recover themselves. the secret word was helpful but apparently members are too lazy to remember them.

I can't be your fucking brains and personal security guard.

Quote:What is the difference between this and a normal email other than the email being stored under encryption?

If your account is stolen and your email is compromised. I'm hoping your smart enough to keep your secondary email secret and use it from a secured computer. You can then do a PW reset to your secondary and regain the account. Is this 100%? No, but it's a chance.

Quote:Well instead of a secondary email why not have it send a sms to a phone number or something? Emails can always be hacked.

Who's going to pay the SMS fees? And not everyone wants to enter their cell in the DB. To be honest I don't even want that info. Oh the horror if we're compromised and your cell is exposed.

Quote:That's a not too bad idea Omnomni, but what if those secondary emails get compromised? doubting they will, but surely there is a small chance?

Always a chance. I think the benefits outweigh the negatives. And I'm fairly certain I can code this in a reasonable time. There is that to consider. It's not enough to come up with great ideas. You have to think of ideas practically and how they'd be implemented.

No point in saying...I'm adding SMS, extra password, extra email, onscreen keyboard, and blah blah blah if it takes me 2 years to implement.

Positive - June 27, 2011, 5:39 pm

(Jun 27, 2011 03:46 PM)Omniscient Wrote: [\[CITE\]](#) I finally just came up with a perfect security idea.

A secondary email address that's non-changeable and encrypted in the database.

The secondary email if used will reset the password.

It's perfect as long as members remember their secondary email addy.

I can't work on this idea now but I think it's a real winner.

Too many members come up with ideas that they aren't aware are either difficult to implement or would cause more problems than help.

Sounds like a good idea sir.

I mean, I would have it to where it still shows the primary in the usercp, but you can password reset with the secondary email.

-- Positive --

Elite Hacker 69 - June 27, 2011, 5:46 pm

Isn't there some kind of security system you could sell out to people that were unsure of if they could keep their details secure?

FamousMassacre - June 27, 2011, 6:05 pm

(Jun 27, 2011 03:46 PM)Omniscient Wrote: [\[CITE\]](#) I finally just came up with a perfect security idea.

A secondary email address that's non-changeable and encrypted in the database.

The secondary email if used will reset the password.

It's perfect as long as members remember their secondary email addy.

I can't work on this idea now but I think it's a real winner.

Too many members come up with ideas that they aren't aware are either difficult to implement or would cause more problems than help.

I use my Hackforums address for my email, so basically the same thing?

.Astro - June 27, 2011, 6:13 pm

I was just thinking of this, except mine was to use a dummy email address for show, while the real email address is hidden.

?Cooldude? - June 27, 2011, 11:36 pm

Omni, what's the point in having to enter your UID along with the secondary email address?

wia - June 28, 2011, 2:11 am

Just hash the emails next time. If you don't mass mail no problem. A second email is silly because if your second email gets compromised or you lose access you can't change it.

Venom Page - June 28, 2011, 4:11 am

(Jun 27, 2011 03:50 PM)S70N3R Wrote: [\[CITE\]](#) Just say the users Secondary email is compromised?

Well, if I get Omni's idea right, you hash the mail as well, so if you reset your password using your secondary mail, it just checks if the hash of this mail is in the database, that way the secondary mail is never actually stored in the database, just it's hash.

nanobyter - June 28, 2011, 4:57 am

Bro I can try to help :) I know HTML css and getting good at php you know :)
or you could tell me what to do and 2 people better than one
not now though VACATION! I see a lot of comments about being keylogged and about people knowing your second e-mail common he's trying his best if omni wanted to he wouldn't give us this but he does!

I don't know why people worry about keyloggers and Rats (I was only ratted once when I was 10) but my e-mails never been hacked or I've lost accounts except that one time and I only lost my pass and when I feel something is wrong I change my pass e-mail and stuff COMMON SENSE!

I always say if you get hacked it's because you were stupid and didn't make sure it was clean (not every case though) and if this happens just go to White Hat Section when I feel like I need a check I go check there or run my AV so guys please not that hard -.-

Elite Hacker 69 - June 28, 2011, 5:41 am

Omni you should require a symbol in passwords.

SavageBoys - June 28, 2011, 6:13 am

(Jun 28, 2011 05:41 AM)BLX Wrote: [\[CITE\]](#) Omni you should require a symbol in passwords.
Yeah a strong combination is always a pass with uppercase/lowercase/numbers/symbols.

h0lmeZ - June 28, 2011, 6:43 am

I like the login system from Liberty Reserve with the PINs which you can only enter with the mouse to prevent keylogging.

lovemaster - June 28, 2011, 7:11 am

lol we need this, somebody tried to reset my password twice hahah
if my email gets hacked, i wont be able to get my account back, so implement this Idea quick

hope we can be safer for the future

Omniscient - June 28, 2011, 10:32 am

Quote:Omni, what's the point in having to enter your UID along with the secondary email address?
This would ensure the uid would be known and that it's not just random guessing. So let's say your secondary was compromised somehow. The person who stole the account would need to know that it's your account.

Also I'm going to figure out a way to do reminders every few months for members to check their current emails and possibly change their passwords. It's insane the amount of people who have email addresses here that are no longer valid or accessible. If people had their emails then a mass password change would be no big deal. Instead I have hundreds saying they can't remember their

HF email or they lost access. It's uncool.

King James - June 28, 2011, 10:47 am

I've got a few possible additions:

Warning screens. Tell them not to login to that e-mail frequently, and to create and maintain it on a computer you're 100% sure is safe.

Explain it can't be removed, altered or anything.

If you still get complaints from people messing up their emails, then we have some real idiots here ?.

fiddy % - June 28, 2011, 11:53 am

Sounds very reasonable. I don't see how this won't be secure.

pr0t0typ3 - June 28, 2011, 12:03 pm

I don't think it is a good idea, because if you loose your secondary email for some reason you are not able to change it or reset the password.

?Cooldude? - June 28, 2011, 12:04 pm

(Jun 28, 2011 10:32 AM)Omniscient Wrote: [\[CITE\]](#) This would ensure the uid would be known and that it's not just random guessing. So let's say your secondary was compromised somehow. The person who stole the account would need to know that it's your account.

Ah right, I see. So an email sent to the secondary email wouldn't contain the users' username? That's a great idea to help prevent random attacks, although it wouldn't help with preventing targeted attacks. There would then be the problem of people not knowing their UIDs.

iPhone - June 28, 2011, 12:05 pm

Good idea, you should have known that early buddy.

KRB - June 28, 2011, 12:11 pm

Of all idea's presented of course omni's idea hits the spot :)

Hypnosis - June 28, 2011, 12:34 pm

Sounds like a plan to me.

Any date we could expect you to work on this?

Magnus - June 28, 2011, 1:02 pm

Maybe you can store the e-mails in a different table, something like hf_secaddy and do md5 salted encryption.

Debesten1 - June 28, 2011, 1:06 pm

If you are using this? What will help? If someone gets in the DB they will find this and decrypt it. Or you have to encrypt it in a language that you made by yourself?

iMario - June 28, 2011, 1:11 pm

I agree, this is a great idea, expect a lot of people forgetting their second email.

iHackForums - June 28, 2011, 1:13 pm

Sounds like a silly idea that email is just as hackable as the first even if it is encrypted after all they gain passwords mainly from stealers and keyloggers. so they will see a list of emails and just attempt with each email.. (Jun 28, 2011 01:06 PM)Debesten1 Wrote: [\[CITE\]](#) If you are using this? What will help? If someone gets in the DB they will find this and decrypt it.

Or you have to encrypt it in a language that you made by yourself?

Then they will get the encryption function and ofcourse there will be a decryption function and run it as if it was plain text...

USELESS IDEA!

Chancelor - June 28, 2011, 1:36 pm

Problem.. If the secondary email becomes compromised and your HF account info is changed then what.

Ninjury - June 28, 2011, 2:13 pm

Just say the word, and I will lay out the real perfect idea. Of which will not be hard to apply, nor cause a single problem for anyone.

DarkDelta - June 28, 2011, 2:44 pm

If you want to encrypt the emails, you can't send stuff to the emails unless you use a cipher, but then it is yet again crackable/decodeable

ElasticWeed - June 28, 2011, 3:10 pm

Sure would be nice as long as the E-mail address doesn't get hacked ^^

Cyber-Security - June 28, 2011, 3:50 pm

This is a really good idea. Good thinking Omni!

Number 1 - June 28, 2011, 4:01 pm

That's a good idea for now, But remember nothing is safe in the cyber world forever :)

Good luck Omni!

Jeimuzu - June 28, 2011, 4:24 pm

Nice work, sir!

This will stop those pesky hackers.

SIM-55193 - June 28, 2011, 5:06 pm

This is a really good idea. I like it.

Lith - June 28, 2011, 5:20 pm

What if they're compromised through a virus, wouldn't both of the emails get stolen?

Trojan - June 28, 2011, 5:20 pm

Well I'm glad that you're thinking of your own ideas Omnizzle.

lolsonlols - June 28, 2011, 5:39 pm

(Jun 28, 2011 05:20 PM)Unkn0wn Wrote: [\[CITE\]](#) What if they're compromised through a virus, wouldn't both of the emails get stolen?

I think SMS auth would be a good idea. Like google mail login 2-step login.

Lith - June 28, 2011, 7:15 pm

(Jun 28, 2011 05:39 PM)lolsonlols Wrote: [\[CITE\]](#) I think SMS auth would be a good idea. Like google mail login 2-step login.

That is pretty difficult to implement.

Kewlhotrod - June 28, 2011, 7:29 pm

This idea is for Ubers:

You could add a secondary e-Mail that is registered to their username at the time to your own personal e-Mail server (I.E. NOT a forward), and along with it a secret word. Only staff/moderators can check this e-Mail and verify the secret word as well, therefore making sure Ubers won't forget their e-Mail. I'm sure the verification can be made automatic with a few simple scripts, too.

Chamomile Tea - *June 28, 2011, 7:33 pm*

Great idea Omni, I hope you implement it as soon as possible.