

Forum:[Hack Forums](#)

Thread: [What other security measures should I take?](#)

Cabinet - October 6, 2016, 1:37 pm

This is a brief list of things I have already done:

Set up an Electrum wallet under a proxy

Set up a Skype under a proxy

Started using a deep web email address

Set up a basic system to protect my passwords (they are all randomly generated and stored in a password protected encrypted archive off-site, the password to the archive being randomly generated and rather long)

Started using Tor for everything that Tor would be appropriate for

Put a password on my computer (can't believe I didn't have one before)

Started putting my computer to sleep every time I step away from it

Got a new anti-virus (Malware-Bytes, as opposed to AVG)

Any other measures I could take?

Cimex - October 6, 2016, 1:42 pm

It all depends on your security focus... are you just protecting yourself from users of the internet, or government etc?

JUAN9087™ - October 6, 2016, 1:44 pm

Are you posting this with your actual ip and computer did you created this account with your actual internet ip?

Faith Connors - October 6, 2016, 1:44 pm

That sounds a little overkill except for the randomly generated passwords and stuff like that, wonder what you're doing. Ah, don't answer that, it's none of my business.

Anyway, yeah Sigaint is a good email provider but so is Protonmail, if you want to use clearnet and still maintain really high security.

I'd suggest setting up either XMPP or Ricochet instead of using email for everything, as IM is generally faster than email (Ricochet is probably safer than XMPP although both are good) and Skype probably isn't the most secure thing for IM.

MWB is a good AV, but it's really for scanning stuff rather than live protection. Avira is a good free AV that keeps scanning your system constantly and it's not very intrusive. ESET is probably my fave antivirus but it does cost if you have a few bucks to choke up.

Uhh, maybe you'd want to encrypt your drives if you haven't already, Bitlocker or something like Truecrypt 7.1a (DO NOT USE ANY VERSION AFTER OR BEFORE THIS, ANYTHING NEWER IS

COMPROMISED) or use Veracrypt to create your own virtual encrypted drive.

Cabinet - October 6, 2016, 1:59 pm

(Oct 6, 2016 01:42 PM)Cimex Wrote: [\[CITE\]](#) It all depends on your security focus... are you just protecting yourself from users of the internet, or government etc?

I want to be secure all around, but mostly from other people. I don't think I could be a big target for the government, but of course I don't want to eliminate any options.

(Oct 6, 2016 01:44 PM)JUAN9087™ Wrote: [\[CITE\]](#) Are you posting this with your actual ip and computer did you created this account with your actual internet ip?

Yeah I'm using my real IP for Hackforums and other personal stuff. Should I be using public wifi or something?

(Oct 6, 2016 01:44 PM)Faith Connors Wrote: [\[CITE\]](#) That sounds a little overkill except for the randomly generated passwords and stuff like that, wonder what you're doing. Ah, don't answer that, it's none of my business.

Anyway, yeah Sigaint is a good email provider but so is Protonmail, if you want to use clearnet and still maintain really high security.

I'd suggest setting up either XMPP or Ricochet instead of using email for everything, as IM is generally faster than email (Ricochet is probably safer than XMPP although both are good) and Skype probably isn't the most secure thing for IM.

MWB is a good AV, but it's really for scanning stuff rather than live protection. Avira is a good free AV that keeps scanning your system constantly and it's not very intrusive. ESET is probably my fave antivirus but it does cost if you have a few bucks to choke up.

Uhh, maybe you'd want to encrypt your drives if you haven't already, Bitlocker or something like Truecrypt 7.1a (DO NOT USE ANY VERSION AFTER OR BEFORE THIS, ANYTHING NEWER IS COMPROMISED) or use Veracrypt to create your own virtual encrypted drive.

Ahh but Skype is such a gold standard for communication here. Is it likely for any leaks to happen through Skype if I am using a proxy? I made sure I signed up through Tor and also used my Sigaint address for it. And I didn't dare to log in until the proxy was set up. But where could I get set up with XMPP?

Avira sounds like an interesting AV. How resource intensive is it? I only have a mobile Core 2 Duo so I have to watch out for that kind of stuff

And I'll consider using Truecrypt.

I was also wondering if there is any kind of dead man's switch programs out there? Something that prompts me every few hours or so and deletes certain files if I don't enter the correct password in time, or something similar.

ka\$h - October 6, 2016, 2:25 pm

You seem like you might be interested in tails Linux

Faith Connors - October 6, 2016, 2:26 pm

(Oct 6, 2016 01:59 PM)Cabinet Wrote: [\[CITE\]](#) Ahh but Skype is such a gold standard for communication here. Is it likely for any leaks to happen through Skype if I am using a proxy? I made sure I signed up through Tor and also used my Sigaint address for it. And I didn't dare to log in until the proxy was set up. But where could I get set up with XMPP?

Avira sounds like an interesting AV. How resource intensive is it? I only have a mobile Core 2 Duo so I have to watch out for that kind of stuff

And I'll consider using Truecrypt.

I was also wondering if there is any kind of dead man's switch programs out there? Something that prompts me every few hours or so and deletes certain files if I don't enter the correct password in time, or something similar.

Yeah, a lot of people here use skype because it's pretty much based on trust. You'll see guides hover around here on how to jack people's skype accounts or get them banned with very little effort, so yeah, don't give it to anyone you don't trust if you have any sensitive stuff in there.

As for setting up XMPP, all you need is a client for it and make sure it supports OTR (off-the-road, off-the-record) so Pidgin has support for it but right now I'm using Psi+ (make sure it's +) and I'm having no troubles. Then just find yourself a nice server/provider and sign up with them. Right now I'm on xmpp.jp but there are some ones with cooler names, like exploit.im or crimin.al

Avira is relatively resource intensive, but not sure how much. You can try it out and see how it works, I just like it because it's not intrusive at all.

As for a deadman's switch sort of thing, dunno if one exists but it can't be thaaaaat hard to make. Just set it up with your system's scheduler and it'll be good to go. Could very easily get annoying though.

zippy4blu - October 6, 2016, 3:16 pm

The password thing is an awesome idea, I would maybe require a bios password on boot for a little more physical security.

Ni??c??k - October 6, 2016, 3:20 pm

You should use Discord over Skype.

8lue7ornado - October 6, 2016, 3:29 pm

In addition you could use a live usb boot of whichever o.s. you want, there wouldn't be any kind of data saved within your pc and usb

I probably wouldn't use tor so often because of the end route, hard to trust on the onion route even tho it's really hard to be the last on purpose.. use duckduckgo.com or disconnect.com as search engine along with vpn that doesn't track logs (expressvpn one of them, a bit expensive tho)

M5DD - October 6, 2016, 3:34 pm

Stop using tor, it's pretty bad. Honestly you'll be better off with a bulletproof vpn that doesn't log.

Cabinet - October 6, 2016, 3:45 pm

(Oct 6, 2016 03:34 PM)M5DD Wrote: [\[CITE\]](#) Stop using tor, it's pretty bad. Honestly you'll be better off with a bulletproof vpn that doesn't log.

Lol you have to be trolling

Mi2414 - October 6, 2016, 3:48 pm

Discord is alot safer than skype, a good xmpp server is Null.Pm I know many who use it. Might also wanna encrypt your HDD an use 2fa with the App Authy.

M5DD - October 6, 2016, 3:50 pm

(Oct 6, 2016 03:45 PM)Cabinet Wrote: [\[CITE\]](#) Lol you have to be trolling

Nope, TOR sucks ass. Most of the nodes are owned by the feds and it's slow as fuck.

Cabinet - October 6, 2016, 4:05 pm

(Oct 6, 2016 03:50 PM)M5DD Wrote: [\[CITE\]](#) Nope, TOR sucks ass. Most of the nodes are owned by the feds and it's slow as fuck.

Even so, Tor was made with the thought of nodes being used to breach security in mind. I have a child-like understanding of networking, so correct me if I'm wrong here. But no agency has the time or the money to decrypt every packet going through Tor nodes. And seeing how you would have to buy a lot of hardware and hire a lot of employees to do that kind of work, I'm sure someone would pick up on that paper trail and blow a whistle.

M5DD - October 6, 2016, 4:32 pm

(Oct 6, 2016 04:05 PM)Cabinet Wrote: [\[CITE\]](#) Even so, Tor was made with the thought of nodes being used to breach security in mind. I have a child-like understanding of networking, so correct me if I'm wrong here. But no agency has the time or the money to decrypt every packet going through Tor nodes. And seeing how you would have to buy a lot of hardware and hire a lot of employees to do that kind of work, I'm sure someone would pick up on that paper trail and blow a whistle.

Quote:"Chloe set up a fake website with a Bitcoin theme, downloaded a complete list of exit nodes and then logged in to the honeypot site multiple times via Tor, using a different exit node and a unique password each time.

Crucially the usernames and passwords were sent over regular HTTP rather than encrypted HTTPS so that when Tor's layers of encryption were peeled back they were visible in the stream of traffic.

If the login attempts had gone unobserved and unabused then the total number of website visits and log in attempts recorded by the honeypot should have matched the number performed by Chloe exactly.

They didn't.

After a month of testing there were over 600 unexplained page visits, 12 failed log-in attempts and 16 successful ones that hadn't come from Chloe.

The passwords were not stored anywhere and were far too difficult to guess so if they were indeed stolen, they were stolen by somebody snooping on-the-wire."

Quote:"Dan Egerstad proved then that exit nodes were a fine place to spy on people and his research convinced him in 2007, long before Snowden, that governments were funding expensive, high bandwidth exit nodes for exactly that purpose."

just saying

Cabinet - October 6, 2016, 5:00 pm

That's interesting. I'd like to see someone more experienced than us fact/reality check that though.