So all joking aside. I just wanted to take a moment to share a few thoughts on security. For years and years, us Mac users have been able to boast about not having viruses and for the most part, this is still true. However, the bad guys in the world are getting smarter. They don't necessarily need you to install something on your computer to get to your private data. There are other ways. It is time for us Mac users to begin to realize that we are not impervious to attack. As long as we're smart and follow a few simple rules we can continue with business as usual. There are however, times when our security or even identity is compromised. And I'm hearing of this more and more....

Hacked:

I was contacted by a client last week while she was on vacation with her family out North Carolina. She stated that she felt like her mobileme account had been broken in to. She said that all her devices and computer were reporting that the mobileme password was incorrect. When she tried to log in to me.com it would not take the password either. So she went to reset the password. When prompted for her date of birth, it wouldn't take that. So she was locked out of her own account. She then began to get reports from her friends and family that they were getting emails from her with the old "we're stuck in London and need money" trick except that the emails were coming from a yahoo account with her name in the prefix (almost identical to her mobileme name).

After she returned we met and I began with the obvious tests. I often encounter people who've forgotten their passwords (you know who you are) so I thought this was just a case of forgetfulness. But after digging around myself, I soon realized she was exactly right. It was clear her account had been broken into. I contacted Apple and we began the process of reseting the password. However, each time they asked me to provide some sort of identification Apple reported that my answer was wrong.

Her date of birth had been changed. Her secondary security question like "mom's maiden name" had been changed to "my favorite teacher". The address to the account had been changed. The credit card associated was no longer valid so we couldn't use that to convince Apple that we were who we said we were. Apple has to be absolutely sure before they can reset anyone's password. Every question they asked us to answer was wrong! It's like someone got her password and changed everything inside the account and come to find out, that is exactly what happened. The phone number to the account had been changed, the addresses, everything! Finally after much time with Apple we were able to see the exact time she stopped getting email (April 25th at 11:03pm) and they were able to see that there was massive activity on their end as well so that was enough to finally convince them we were telling the truth and that this account had been compromised. But here is where it really gets weird.

After Apple sent us a reset link, we were able to access the account and see what had been done. Someone had gone into her account, changed all the security questions, her birthday, addresses, phone numbers, and set the account to forward all her email to the yahoo account they created themselves then set the mobileme account to delete the email. So even after

regaining access to her account she had lost about a week's worth of email. Every email for the past week had been forwarded to this bogus yahoo account including the transcript of all the troubleshooting I did with Apple I asked be sent to us. So now the hacker had even more information including certain information of my own as I had to identify myself to Apple during the conversation with my own consultant ID. That transcript was sent to her email then forwarded to the hacker and deleted before she could even get it.

I decided to investigate a little further. We tried to gain access to the yahoo account which still exists and were able to get about 1/2 way in by using the same questions and answers they had changed her mobileme security settings to.

The only thing either of us can think could have allowed this to happen is that during the vacation they connected to an unsecured (open) wireless network for several days. This could have provided the opportunity needed to intercept the data on the network. This is extremely rare and the level of sophistication required to intercept packet information is not common knowledge but it can happen. Someone took over her identity for almost a week. Now you may be thinking, big deal. Email. Whoop de Doo. But this person also had access to all her contacts and calendars.

I've had a couple of other clients report that their friends are also getting emails via yahoo or aol that seem to come from them so this is obviously a new method that spammers are using and they're getting very good at it.

Ok, so what do we do now?

Let's go over a few things to consider going forward. I've put together a short list of 10 things to consider to continue to protect your privacy.

1. First, let's start being a bit more careful. I think the following may be safe to say that going forward: **try to avoid joining open wireless networks. Especially public ones. You never know who is listening.**

2. While there are still no major viruses out in the wild for the Mac, other pieces of software are starting to appear that claim to "help" your mac become more healthy. These are to be avoided.

3. Don't click on links in emails from people you weren't expecting an email from. If you feel that your bank is really trying to notify you about your account, then go to your browser and manually type in the address. Don't click on the link. These guys will do a very good job of disquising themselves as paypal, netflix, your local bank, a department store, or various other services you may do business with.

4. Don't use the cc field when sending bulk email. Use the bcc field. This will hide all your friend's emails from potential threats on other computers and it's just a nice thing to do.

5. Change your passwords from time to time and don't make it "password". Mixing letters and numbers is a great way to go. But you have to remember them!

6. While it's a pain, use the password lock on your phone or iPad or phone. Do it now! Even I have your info on my phone. I have where you live, your phone number, maybe a note

about your computer or account. You better believe I password protect my phone and computer and you should to.

7. Don't use Norton Antivirus, VirusBarrier or any other virus protection. Do use common sense. These are not yet necessary. In fact, it's in their interest to convince you there *are* viruses because that means their sales will increase.

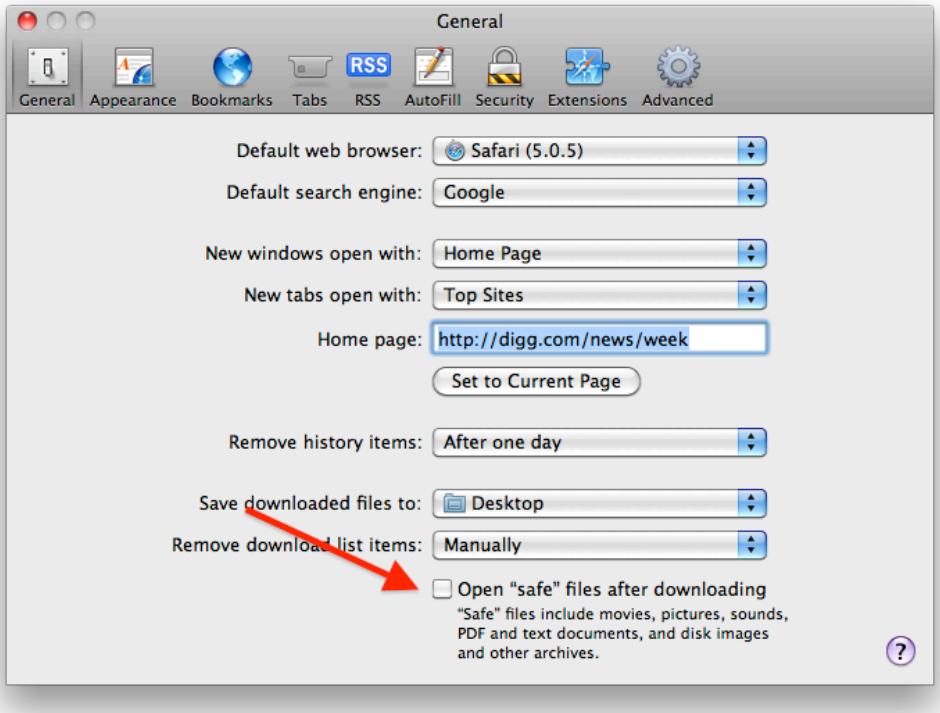
WARNING: If you feel you are just a very basic user then you may want to **STOP** reading here and jump to the last paragraph because things are going to get a little technical from here on out.

*****Advanced*****

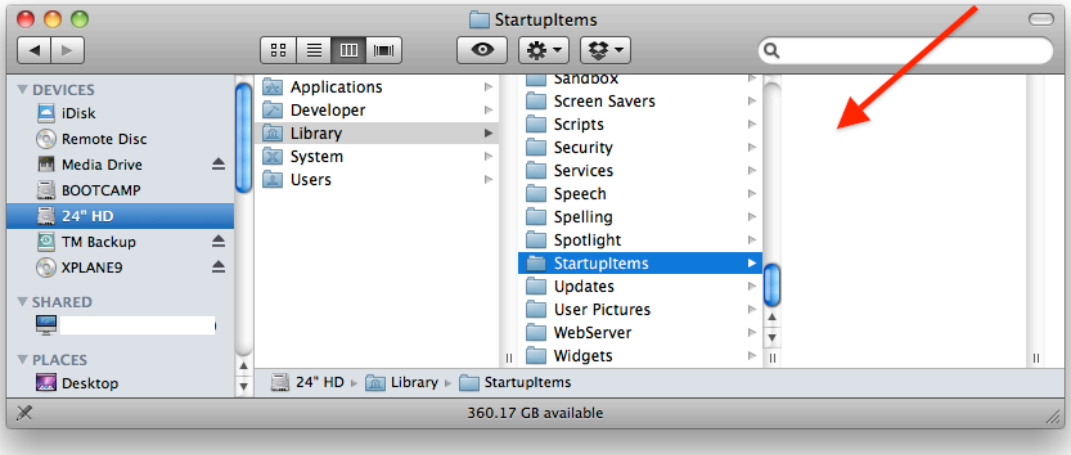
8. Avoid anything called "MACDefender". It's a scam. If anything prompts you to install it and asks for your password, if you didn't download it, don't input your password to authorize it to install. I'm not talking about installing a print driver or a program you downloaded yourself. If you go download Google Earth and it prompts you for your password, that's different. I'm talking about being prompted out of nowhere. Think before you install. A good article on it can be found here.

9. There's a huge add campaign on the net right now for something called "Mac Keeper". My advice: Don't use it. It's preying on your fears that your mac has a virus! This is not the case. They just do a good job marketing. It claims to clean your Mac. Do not invest in this product.

10. Uncheck to automatically open downloaded files in Safari. Under preferences, go to the general tab and be sure to uncheck the following checkbox. (see below)



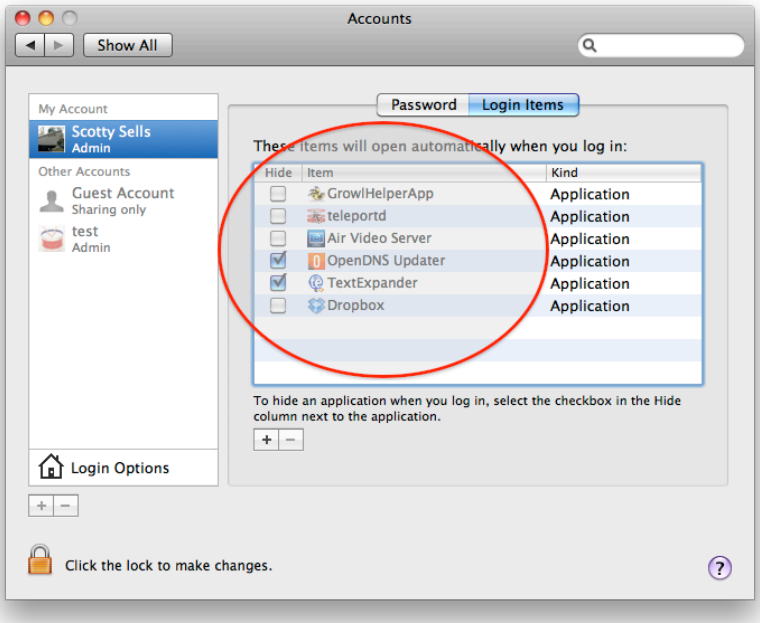
If you want to get technical, there are a couple places you can look in your Mac to be sure only what you *want* running, is running. For advanced users only: Go to /Library/Startup Items to see if there's anything in that folder. If you have a file there and you don't recognize a word in that filename then delete it.



Any file in that folder will run when you start your computer so that's a good place to look first. There are other places as well but it gets a little complicated. You can also check the LaunchAgents and LaunchDaemons folders however there are likely to be items there as well so you really need to know what you're doing before you start removing things randomly.

If you'd like to send me the name of the file and ask if it's a problem then you should feel free to do that or better yet, you can also join us on Mondays for Town Hall to ask about it as well! Note: HP often installs it's own software here (HP trap monitor). It's pointless so you can delete it.

You may *also* want to check your login items in system preferences to see what else is starting up when you log in.



Anything listed in the column shown here will launch at login. You'll most likely have some items but you'll want to ask yourself, "do I really want/need these starting up?". Many of you will see a file called "iTuneshelper". That's totally normal and there by default. You can leave it. As you see, I have several things running at login but have made the choice for those things to be there. Skype is famous for automatically adding itself to the list of startup items.

In Closing...

I don't mean to scare anyone. I just want everyone to continue to have a safe and happy Mac. My client's experience last week served as a wakeup call to me that even though we are on Macs we are not completely invulnerable to the bad guys of the world. Like I said, they are getting smarter all the time so we need to get smarter along with them.

One last thing. Apple is now providing a way for you to give feedback on your experience working with their consultants. If you would, please take a second to complete the feedback form on my services as a consultant with Apple. Click here to begin. It's a little long and you'll need to know your Apple ID to log in. Thanks so much!

Thanks for reading and remember, every hard drive dies so always backup.

Scotty Sells

_____
www.sellsconsulting.com
Consultants Network