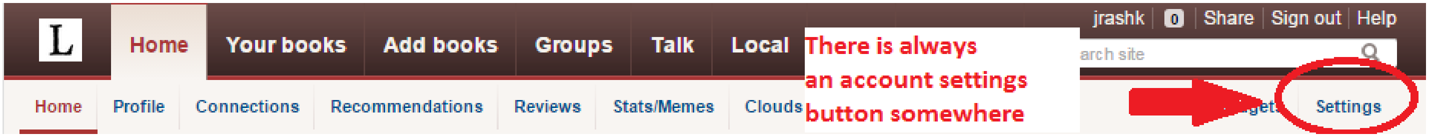
Privacy, Security, & Scam Defense

When using Social Media, The Web, and even E-Mail

Social Media & Privacy

- Yes this is one of those counterintuitive things.
- Every social media service has an area for you to manage your privacy settings.
- These settings allow you to manage who sees what information when they look at your profile
- Lets have a look at my LibraryThing account for an example.
(because I don't have a Facebook account …yes I know I'm not with it.)

LibraryThings' Privacy Settings



There is always an account settings button somewhere

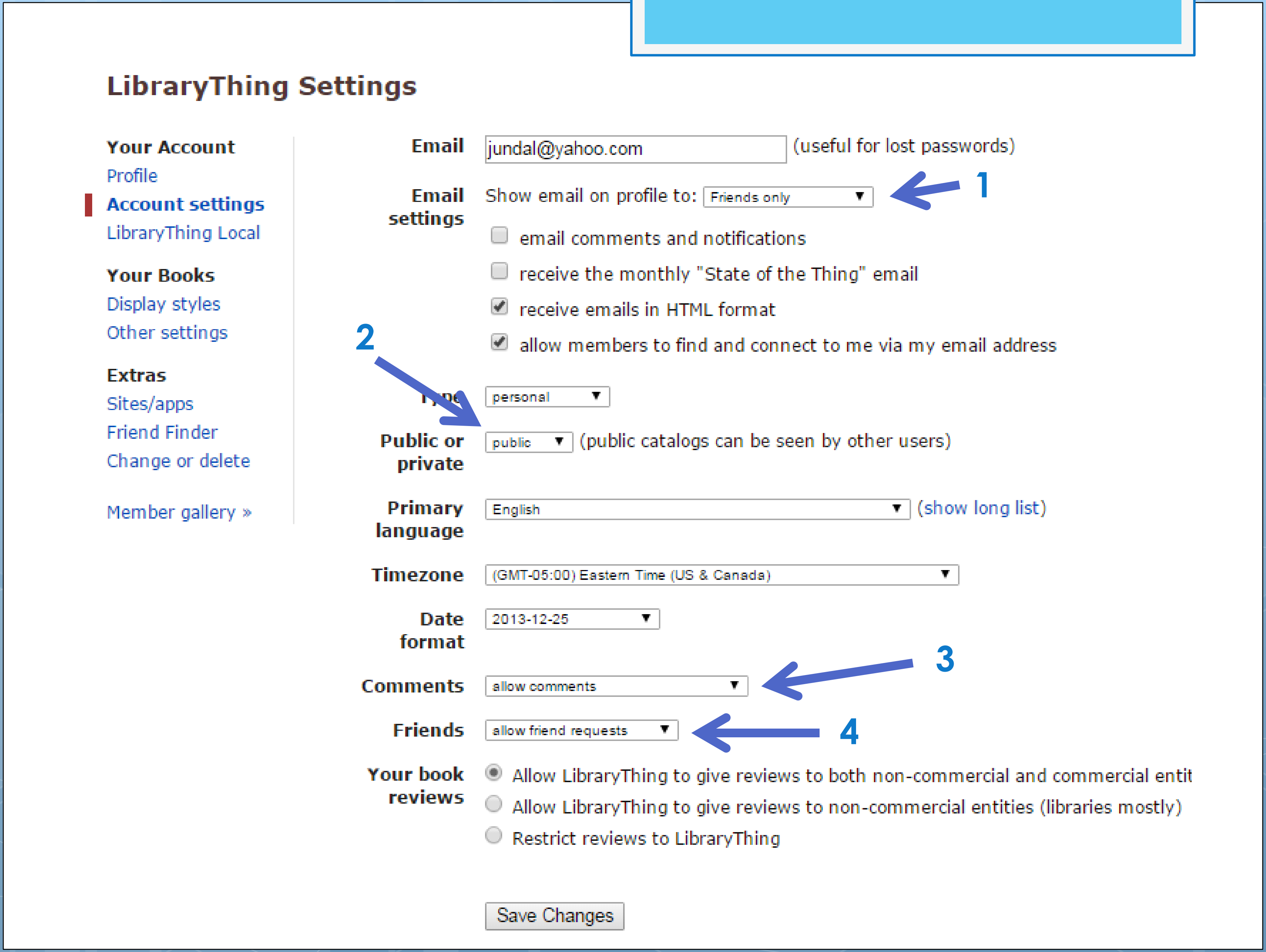
- Some social media / e-mail sites like to hide the settings' option for some reason.
- Keep an eye out for:

⚙ A Gear Icon

☰ The Three Bars Icon
AKA:
The Hamburger Icon

● ● ● The Three Dots Icon

- One of these is bound to take you to a screen like this.



LibraryThing Settings

Email jundal@yahoo.com (useful for lost passwords)

Email settings Show email on profile to: Friends only ▼

□ email comments and notifications

□ receive the monthly "State of the Thing" email

☑ receive emails in HTML format

☑ allow members to find and connect to me via my email address

Type personal ▼

Public or private public ▼ (public catalogs can be seen by other users)

Primary language English ▼ (show long list)

Timezone (GMT-05:00) Eastern Time (US & Canada) ▼

Date format 2013-12-25 ▼

Comments allow comments ▼

Friends allow friend requests ▼

Your book reviews

● Allow LibraryThing to give reviews to both non-commercial and commercial entit

○ Allow LibraryThing to give reviews to non-commercial entities (libraries mostly)

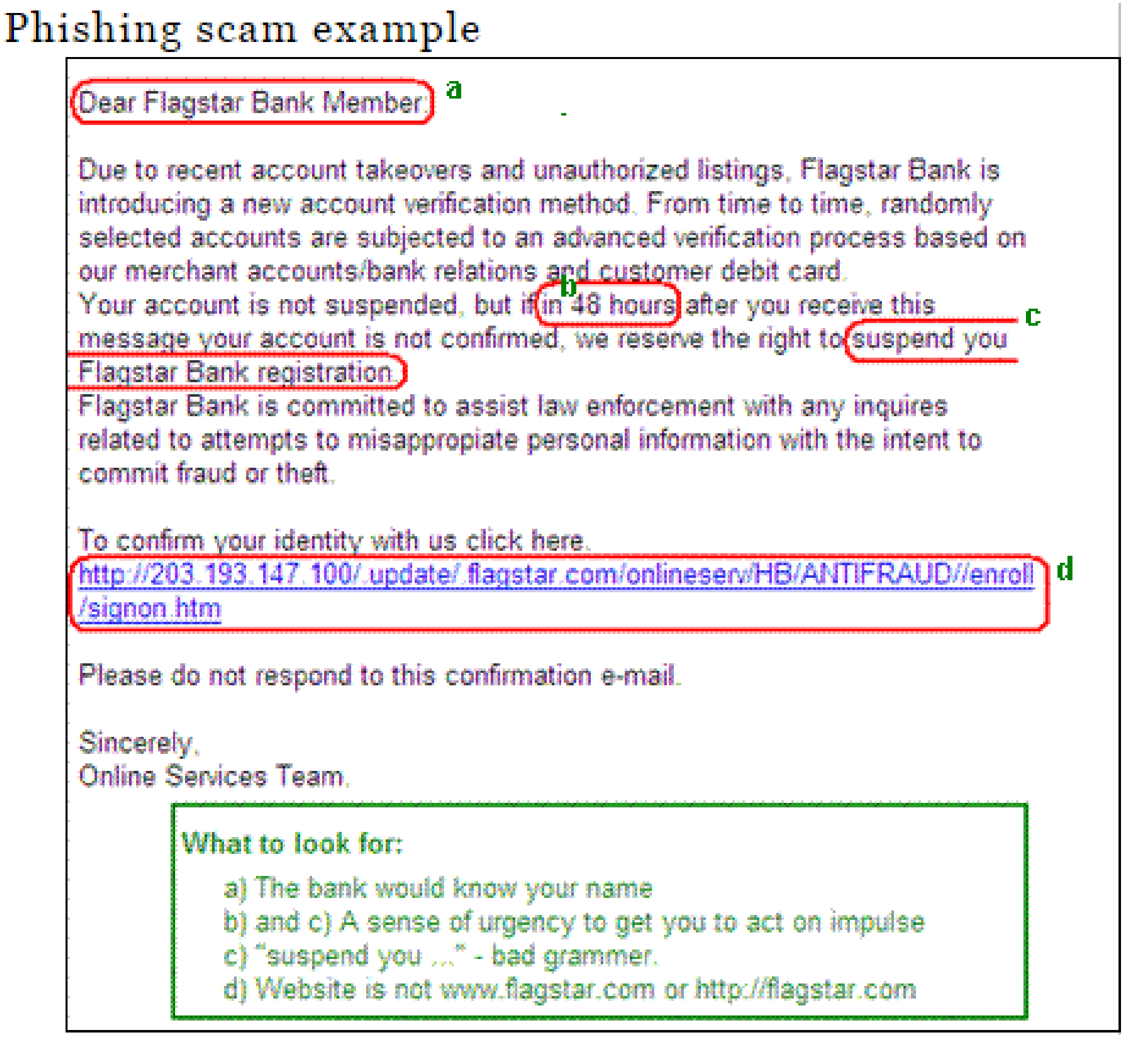
○ Restrict reviews to LibraryThing

Facebook Folks & Privacy

- Facebook is (currently) by far the largest social media site…that makes it target #1.
- The folks at Facebook know this and have made privacy & security a high priority.
- They have also set up a very nice set of tutorials That explain how your accounts privacy & security settings work. Complete with videos. https://www.facebook.com/about/basics
- If any Facebook folks care to comment on this you're welcome to do so.

On to
Scam Spotting & Defense

- The old saying **“If it sounds to good to be true it probably is.”** still holds true today.
- Companies you have accounts with (Cable, internet, phone, banks, etc…) know your name, phone #, and account info … they won’t ask you for it … especially by e-mail or website popup.
- Lets take a look at an example scam e-mail message.



Phishing scam example

Dear Flagstar Bank Member:

Due to recent account takeovers and unauthorized listings, Flagstar Bank is introducing a new account verification method. From time to time, randomly selected accounts are subjected to an advanced verification process based on our merchant accounts/bank relations and customer debit card.
Your account is not suspended, but if in 48 hours after you receive this message your account is not confirmed, we reserve the right to suspend you Flagstar Bank registration.
Flagstar Bank is committed to assist law enforcement with any inquires related to attempts to misappropiate personal information with the intent to commit fraud or theft.

To confirm your identity with us click here.
http://203.193.147.100/.update/.flagstar.com/onlineserv/HB/ANTIFRAUD//enroll/signon.htm

Please do not respond to this confirmation e-mail.

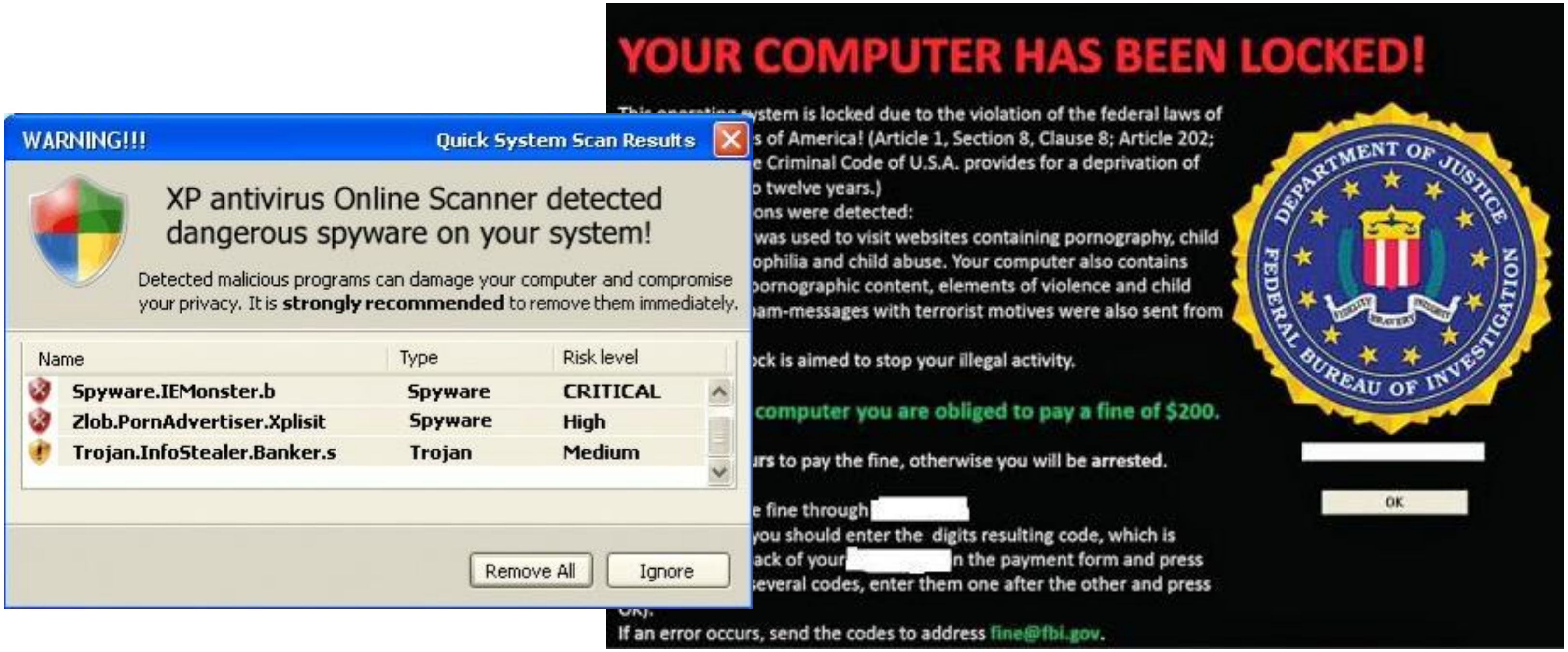
Sincerely,
Online Services Team.

What to look for:

a) The bank would know your name
b) and c) A sense of urgency to get you to act on impulse
c) "suspend you ..." - bad grammer.
d) Website is not www.flagstar.com or http://flagstar.com

- Thanks to Computers Confuse Me for the example: http://www.computersconfuseme.com/articles/phishing-scams/

Scareware: Don’t be afraid



WARNING!!! Quick System Scan Results

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of
s of America! (Article 1, Section 8, Clause 8; Article 202;
e Criminal Code of U.S.A. provides for a deprivation of
o twelve years.)
ons were detected:
was used to visit websites containing pornography, child
ophilia and child abuse. Your computer also contains
pornographic content, elements of violence and child
pam-messages with terrorist motives were also sent from

ock is aimed to stop your illegal activity.

computer you are obliged to pay a fine of $200.

urs to pay the fine, otherwise you will be arrested.

e fine through [redacted]
you should enter the digits resulting code, which is
ack of your [redacted] n the payment form and press
several codes, enter them one after the other and press
OK).
If an error occurs, send the codes to address fine@fbi.gov.

- Scareware is software that tries to scare you into doing something that you don’t want to do.

Tools To Protect You! And they are Free…yes Free!

- Avast = Antivirus
  - Avast is a free antivirus that has versions for all tech devices…including your smart phone.
  - Their free version defends you against computer Viruses and auto updates itself.
- MalwareBytes = Antispyware
  - Malwarebytes protects you from all those annoying pop-ups, page hijackers, and other garbage we don't like sneaking onto our computers. … Sorry no Mac version.

Tools To Protect You Cont.

- Windows Defender
  (AKA Windows Security Essentials) = Antispyware
  - Defender is Microsoft's free antispyware tool

Your probably wondering where to get these tools. Wonder no more.

- Avast: https://www.avast.com/en-us/index
- MalwareBytes: https://www.malwarebytes.org/
- Windows Defender: http://windows.microsoft.com/en-us/windows/security-essentials-download

Conclusion

- If you stop and really read before clicking you will notice when someone is trying to scam you.
- Don't Panic! It won't help so just stay calm and you'll do fine…computers can always be fixed.
- Keep your computers antivirus & malware protection updated, and run the scans at least once a month…or whenever you think you have a problem.
- When in doubt seek help from Google (or your friendly neighborhood librarian)…it's amazing how many of these things are reported by other people.

Any Questions???