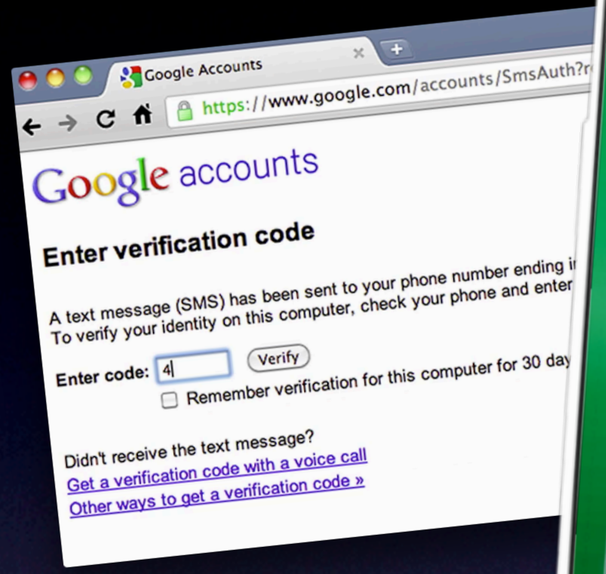
Cove Apple Club

August 8, 2012



Tonight's Topics

- Apple In The News
- Let's Get Serious About Security

AT&T Mobile Share

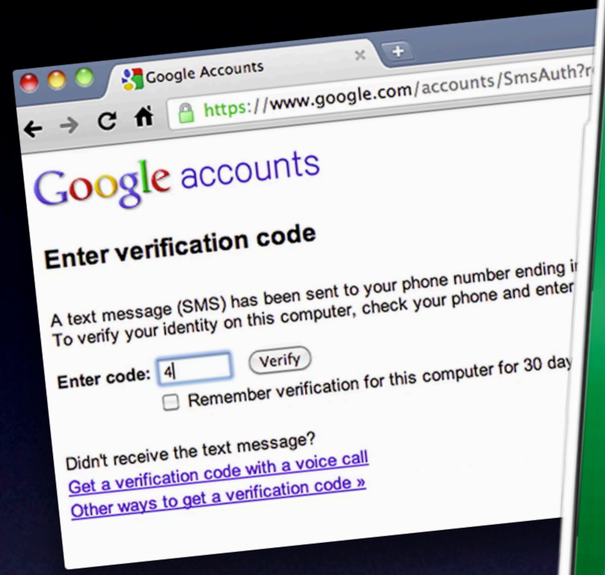
- Starts late this month -- exact date TBA
- Allows up to 10 devices on the same account to share a pool of mobile data gigabytes, along with unlimited talk & text
- Includes 3G and 4G smartphones and tablets
- Online calculator and other info online now at att.com/mobileshare

STEP 1: Choose your AT&T Mobile Share Plan	Per Month					
	1GB	4GB	6GB	10GB	15GB	20GB
Mobile Share with Unlimited Talk & Text	$40	$70	$90	$120	$160	$200
	+	+	+	+	+	+
Each Smartphone*	$45	$40	$35	$30	$30	$30

Apple vs. Samsung

- Court case underway for past ten days
- Not looking good for Samsung
- Apple is trying to protect its future

Let's Get Serious About Security



Mat Honan

- Wired and Gizmodo reporter and mid-level tech industry luminary
- As far from a clueless noob as anyone can be
- Had his digital life destroyed on Friday night

What Happened: Step 1

- Hackers used Honan's domain registration info to get his home address
- Honan's Gmail address is openly published
- Using only those two bits of freely available info, they could take over his entire digital life & wreak havoc on everything

What Happened: Step 2

- Hackers called Amazon and had them add a new credit card to Honan's account; used a fake number generated by algorithm; then hung up
- Called back, asked Amazon to set up a new email address on that same account; they already had all the info needed
- Used new email addy to do a password reset on Amazon; now have access to entire Amazon account, including last 4 digits of all credit cards associated with the account

What Happened: Step 3

- Info from prior steps ~~is~~ was all that's needed to get AppleCare to reset your passwords
- AppleCare generated a temporary password, and hackers used that to create their own passwords for Honan's iCloud account
- Proceeded to use "Find My..." feature to remote-wipe his iPhone, iPad & MacBook Pro & set un-do PIN Honan did not know

What Happened: Step 4

- Honan's Gmail address follows the same format as his iCloud @me.com address; his iCloud address was used as his recovery address for the Gmail account
- Hackers used Gmail's password reset function to gain ownership of his Gmail account
- From there, they took control of his Twitter account

Honan's Colossal Failures

- No backups! None!
- Weak, 7-year old passwords, although they did not figure into the takeover
- Daisy-chaining accounts together
- Using Find My iPhone/iPad/Mac with no backup
- Storing credit card info online with merchants
- Not using Google's 2-factor authentication for his mission-critical Gmail account

Apple/Amazon Failures

- Phone support system susceptible to social engineering
- Not following established account security procedures, i.e., secret question/answer mechanism
- Allowing phone-based access to sensitive account info like credit cards, passwords

Aftermath

- Both Apple and Amazon have shut down phone-based password recovery for now
- Both companies are investigating the vulns pointed out by Honan's case
- Expect some changes...

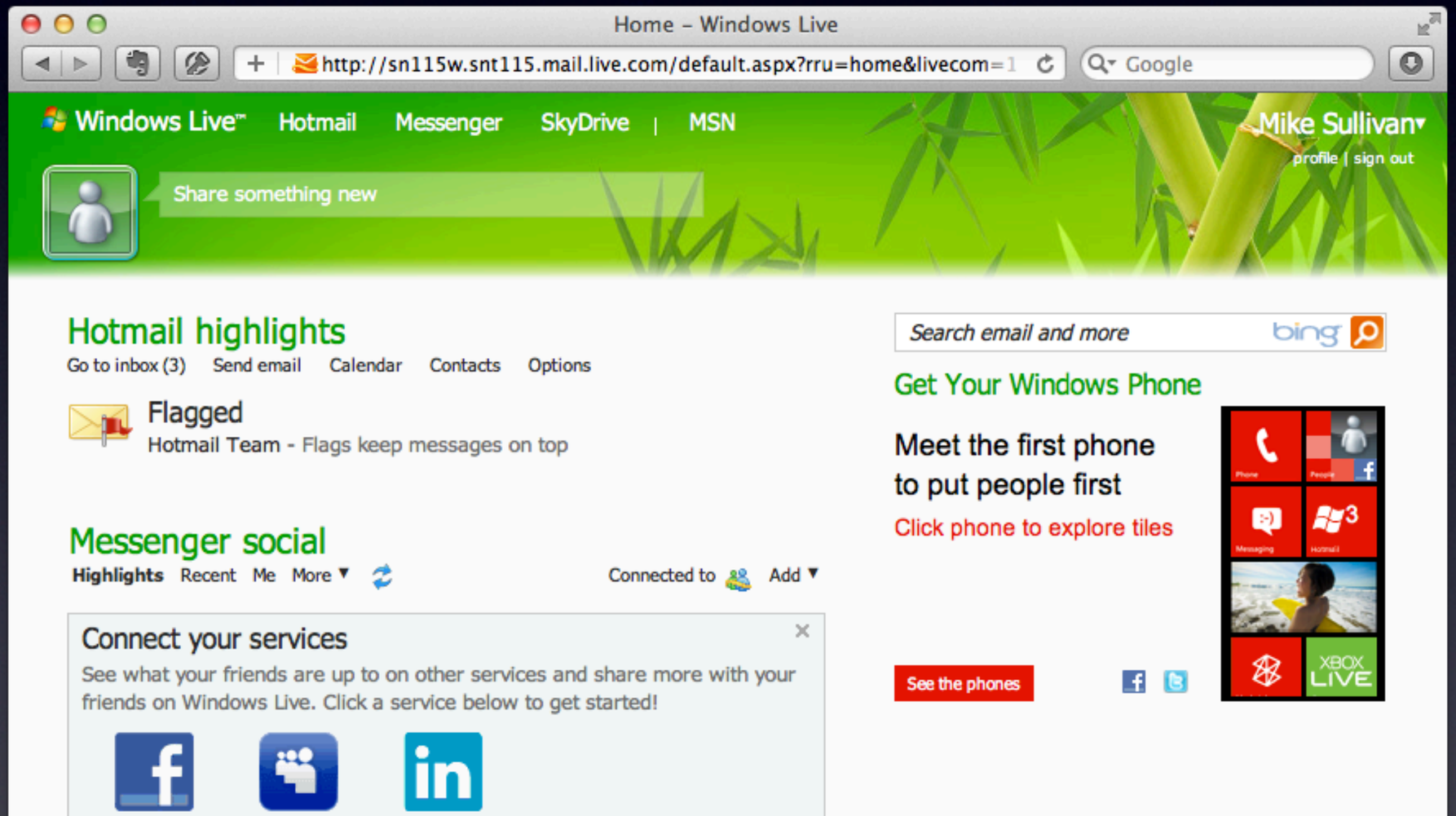
Obvious Lessons

- Have backups!
  - Local: Time Machine/Carbon Copy Cloner/SuperDuper
  - Off-site: BackBlaze/Carbonite/Mozy
- Use strong, long, unique, non-dictionary passwords on all your logins
- Employ a password manager like 1Password to manage & fill them all
- Do not store credit card info with ANY merchant or provider, ever, period, no matter what.

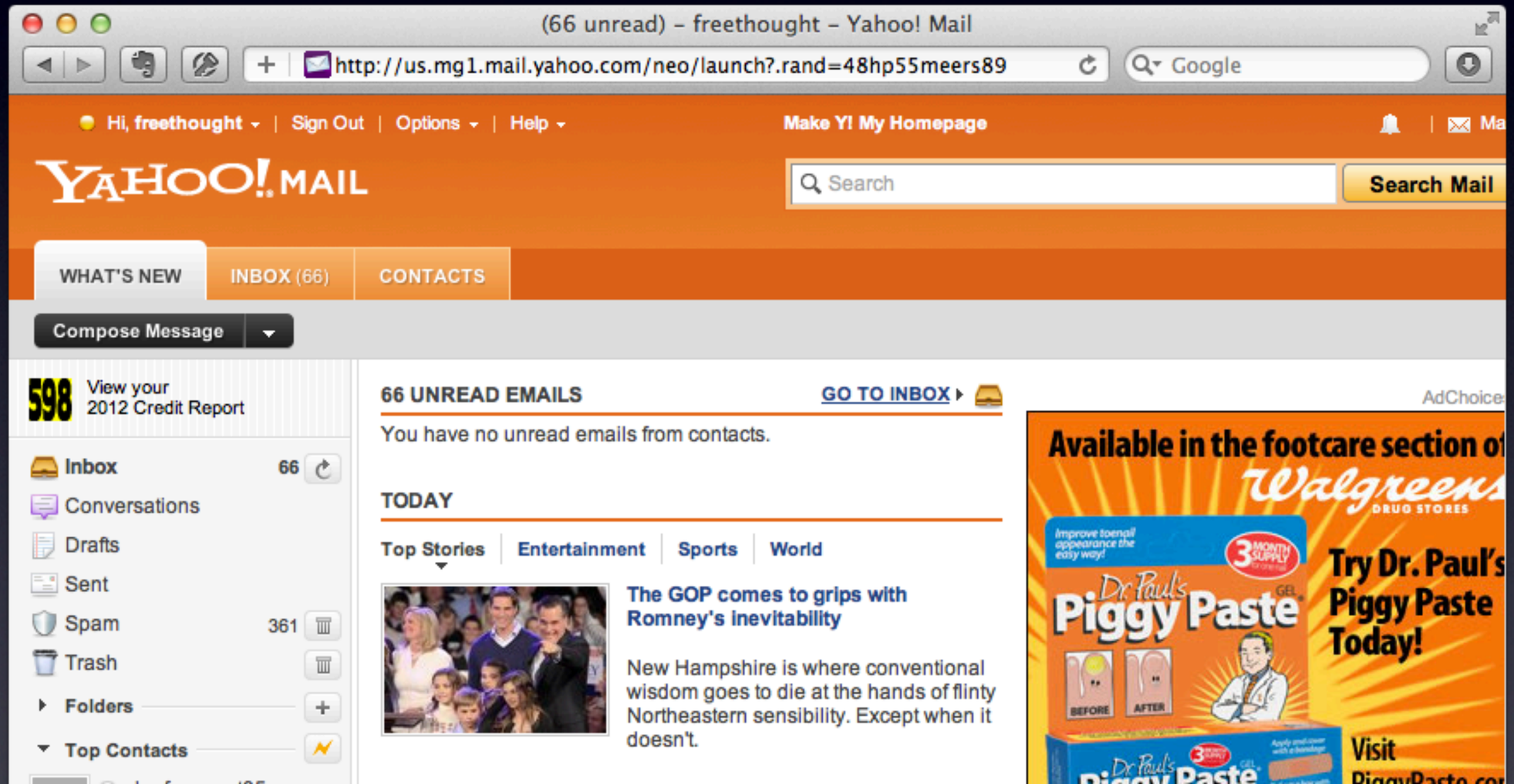
Obvious Lessons

- Do not use a similar email addy for your recovery addy
  - My iCloud email is my main email account
  - mikesullivan@me.com ≠ My Gmail address, which is used only for Google services & emergency recovery
- Get off of crappy, free, insecure email systems: AOL, Yahoo!, Hotmail -- if you're not paying for it, they are paying for you

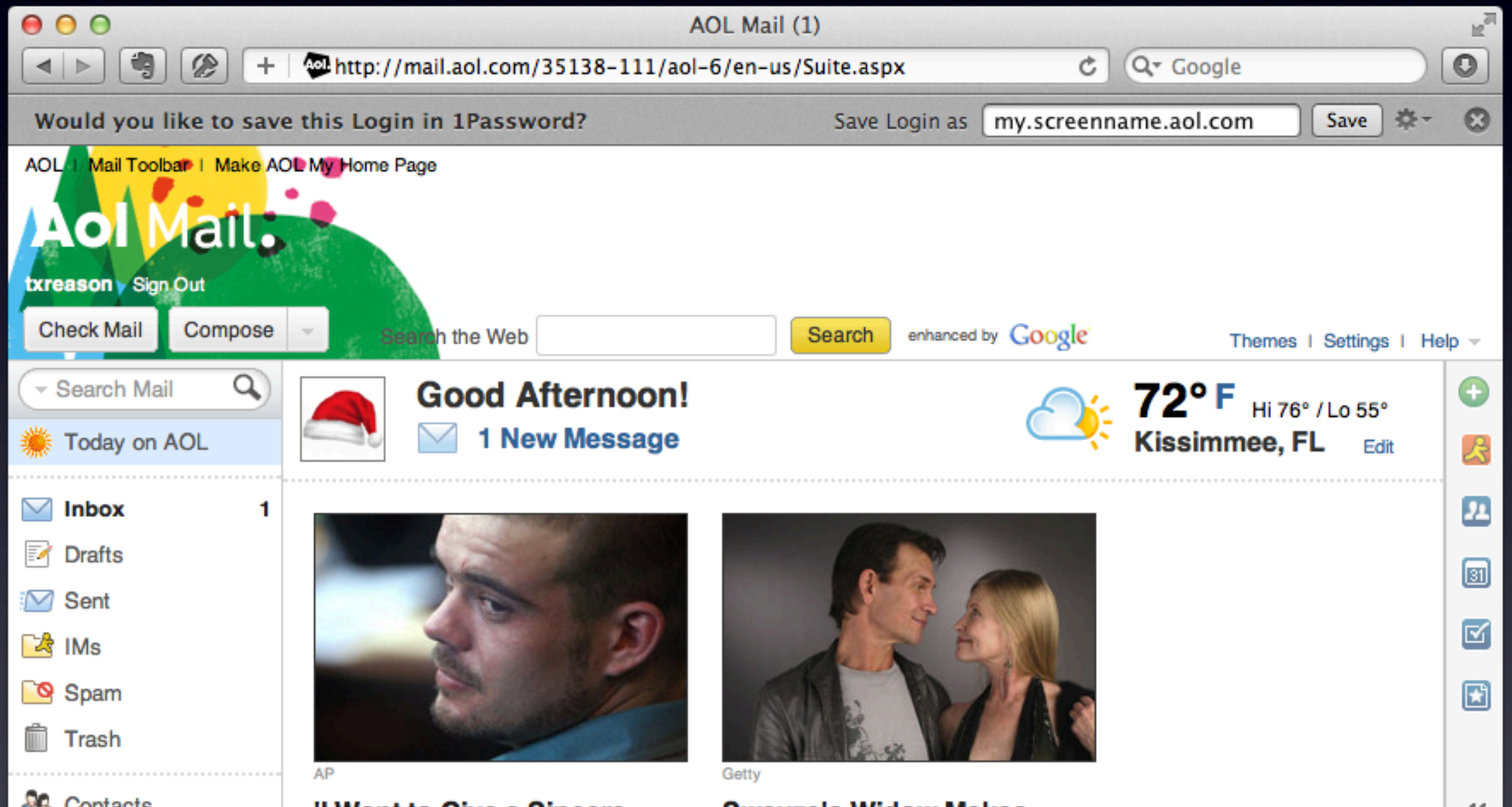
Hotmail/Live.com: Insecure



Yahoo! Mail: Insecure



AOL Mail: Insecure



Tonight's Stern Lecture

- **Backups**
- **Passwords**
- **Credit Cards**
- **2-Factor Auth for Google**

Backups


amazon
Mike's Amazon.com
Today's Deals
Gift Cards
Help
Shop by Department
Search
Electronics
2Tb hard disk
Go
All Electronics
Brands
Best Sellers
Audio & Home Theater
Camera & Photo
Car Electronics & GPS
Seagate Expansion 2 TB USB 3.0 Desktop External Hard Drive STBV2000100
by Seagate
(136 customer reviews)
Like (7)
Price: $119.99 & this item ships for FREE with Super Saver Shipping. Details
37 new from $116.42
Size: 2 TB
1 TB
2 TB
3 TB
In Stock.
Ships from and sold by Amazon.com.
Click for larger image and other views


Time Machine
Show All
Time Machine
OFF
ON
Click the lock to prevent further changes.
Backup – 1Tb Time Capsule
158 GB of 998 GB available
Oldest backup: May 30, 2012
Latest backup: Today, 11:06 AM
Next backup: Today, 12:56 PM
Select Disk...
Time Machine keeps:
• Hourly backups for the past 24 hours
• Daily backups for the past month
• Weekly backups for all previous months
The oldest backups are deleted when your disk becomes full.
Show Time Machine in menu bar
Options...

Q: ***What*** are the two kinds of hard disk drives?

- Those that *have* failed
- Those that *will* fail

Q: ***When*** Will Your Hard Drive Fail?

Only when it is
most inconvenient

Backups: Local

- There is no excuse
- If you can afford a Mac, you can afford an external backup hard disk

Local Backup: Time Machine

- Plug in, turn on, and forget about it
- Silent, automatic, comprehensive
- Has saved my bacon more than a few times

Other Local Backup Solutions

- **Carbon Copy Cloner**
- Automatic bit-for-bit bootable clone of your Macintosh HD
- $29.96; 30-day free trial
- Visit www.bombich.com

Other Local Backup Solutions

- **SuperDuper**
- Automatic bit-for-bit bootable clone of your Macintosh HD
- $27.95; 30-day free trial
- Visit www.shirt-pocket.com

Off-Site Backups

Off-Site Backups

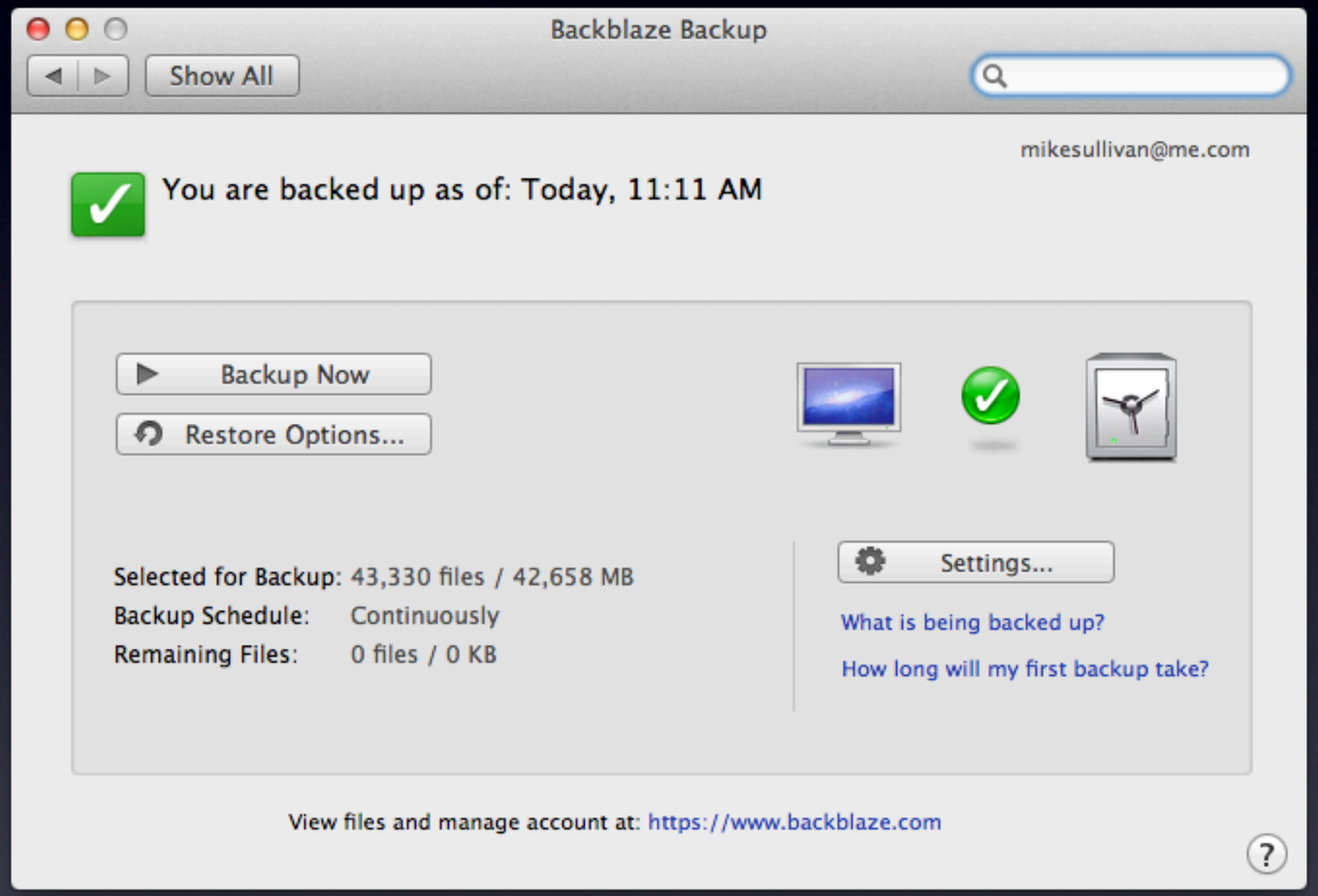
- We live in cardboard trailers...
- ...in an area with frequent lightning storms
- ...in FEMA Wind Zone III
- ...in an area with a history of hurricane activity
- ...in a region known for sinkholes.

Off-Site Backups

- There is no excuse
- If you can afford a Mac and a high-speed Internet connection, you can afford an off-site backup plan
- It's your belt-and-suspenders form of cheap insurance against the unthinkable

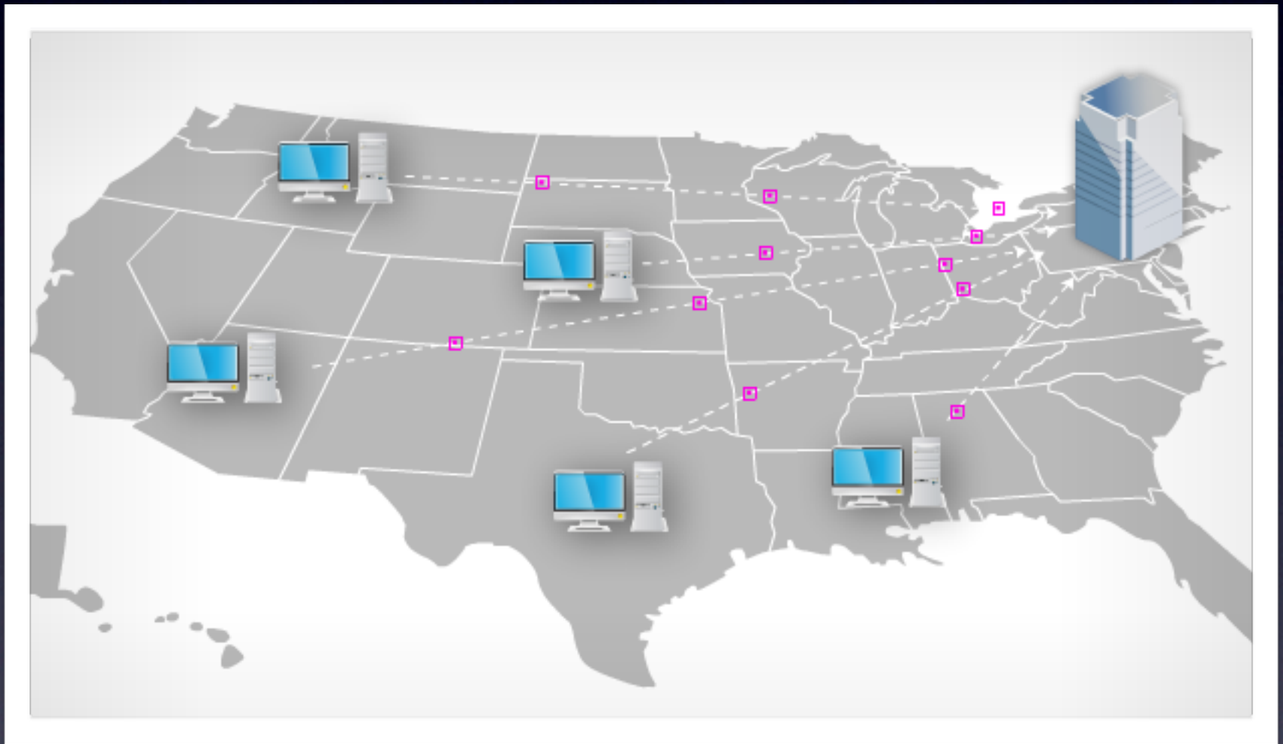
Off-Site Backups: BackBlaze

- ***Unlimited*** off-site backup of your ***entire*** Mac for $5/month or **$50/year**
- Automatic, silent, continuous, comprehensive
- Restore online or from an HD they will ship you
- Visit backblaze.com



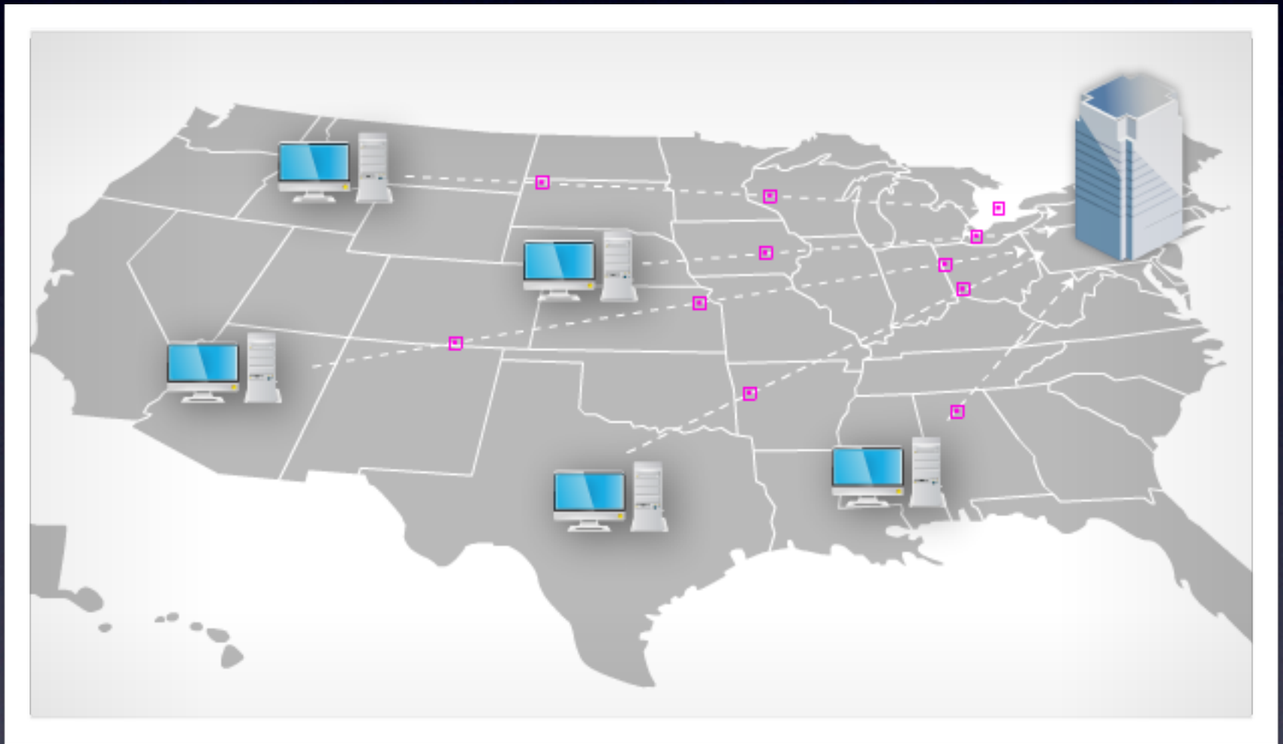
Off-Site Backups: Carbonite

- Unlimited off-site, online backup of your entire Mac for $59/year
- Not as fully-featured as BackBlaze; some features available for Windows only
- Visit carbonite.com



Off-Site Backups: Mozy

- 50Gb @ $6/month;
  125Gb @ $9.99/month
- Restore online or via mailed DVD
- Visit mozy.com



Just Pick One.

Do it... **TODAY.**

Passwords

We've Seen This Movie Before

- January, 2009
- May, 2010
- March, 2011
- February, 2012

Two-Pronged Strategy

- You create one strong, long, unguessable, non-dictionary master password for your four mission-critical systems:
  - Your Mac's boot-up password / admin account
  - Your main email address (iCloud / Gmail / etc.)
  - Your Dropbox account
  - Your Apple ID (same as iCloud / Gmail in most cases)

Two-Pronged Strategy

- You use a password manager, like **1 Password**, to create, manage, fill-in and remember **EVERY OTHER PASSWORD** you need
- **Every password is UNIQUE, LONG, STRONG, UNGUESSABLE and NOT IN THE DICTIONARY**

Most Passwords Are Too Short

- 3- and 4-character passwords can be broken almost instantly
- 4-character lower-case alphanumeric password = 36^4 = 1,679,616 possible combinations = a few seconds, max, of CPU / GPU time on a modern desktop computer
- 8-character lower-case alphanumeric + symbols password = 30 bits of strength or about 1,000,000,000 combinations & permutations. 16 minutes to crack using a desktop computer. [1]
- 12-character lower-case alphanumeric password = 36^{12} = 4,738,381,300,000,000,000,000,000,000 combinations = 7,000,000 years to crack on a desktop computer. [1]

Source: NIST

“I use it for everything!”

- Just helped a friend here in the Cove
- Had the SAME password for **EVERYTHING**: email, finance, banking, ecommerce, etc.
- The password they are using is:
  - A common two-syllable English word
  - ...that appears in the first 20 pages of the dictionary
  - ...that is uniquely associated with their hometown!

Which password is stronger?

```
13 characters: d0g----------

12 characters: Pkz&1-*cH#8j
```

Answer: the longer one!

```
13 characters: d0g----------

12 characters: Pkz&1-*cH#8j
```

- The 13-character password is ***95 times harder*** to crack than the 12-character password, despite being MUCH easier to remember and type!
- See the effect of password length on attack vector search space at `https://www.grc.com/haystack.htm`

Master Password Strategy Ideas

- Your high school mascot plus your first home's house number, with a "digit of obfuscation"
- Example:
  - High school mascot: **Ferrets**
  - First home house number: **2756**
  - Digit of obfuscation: substitute second "e" in Ferrets for a **3**
- **Master password: Ferr3ts2756**

Master Password Strategy Ideas

- Your first pet's name ***intercut*** with the year you met your spouse, with a "digit of obfuscation"
- Example:
  - First pet's name: **Spot**
  - Year you met your spouse: **1979**
  - Digit of obfuscation: substitute the 'o' in Spot with a "**0**"
- **Master Password: S1p907t9**

Master Password Strategy Ideas

- The initial letters of the title of your favorite movie (or song), plus the year it was released, with a digit of obfuscation
- Example:
  - Favorite movie: **The Hunt for Red October**
  - Year it was released: **1990**
  - Digit of obfuscation: switch the "**f**" in "for" with a "**4**"
- Master password: **TH4RO1990**

Why These Work

- Unforgettable to you after just a short period of training
- Meaningless and random to everyone else
- ***Guaranteed unique in the world***
- ***Not found in any dictionary***
- Long enough to satisfy just about every password requirement
- Includes upper- and lower-case letters, one or more digits, and is not part of your name or email address

Now That You've Picked It...Get Some Extra Insurance

- Add something special to it to make it unique for each of the four mission-critical uses
- Example: add a "a" for "Apple;" a "g" for "Google;" etc.
- So, for your Apple ID, your password would be **aTH4RO1990**; for Google it would be **gTH4RO1990**; for Dropbox it would be **dTH4RO1990**
- So now, a breach or compromise in one will not spread to any of the others; also adds another character or two of complexity = manyfold increase in security

A funny thing happened on the way to the Cove Apple Club meeting...

[The Consumerist] Password Reset — Inbox

WordPress <wordpress@consumerist.com> August 8, 2012 11:03 AM
To: Mike Sullivan
[The Consumerist] Password Reset 4

Someone requested that the password be reset for the following account:

http://consumerist.com/

Username:

If this was a mistake, just ignore this email and nothing will happen.

To reset your password, visit the following address:

<http://consumerist.com/wp-login.php?action=rp&key=HA8YkUVwR3wcZb0bTReB&login=Freethought>

WordPress <wordpress@consumerist.com> August 8, 2012 10:52 AM
To: Mike Sullivan
[The Consumerist] Password Reset 3

Someone requested that the password be reset for the following account:

http://consumerist.com/

Username:

If this was a mistake, just ignore this email and nothing will happen.

The First 6 Characters of My Unique Consumerist Password Are:

YPz8Pr

...but there are 10 more characters
no one will ***ever*** know, ***including me***.

Credit Cards

It turns out, a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account. Once supplied, Apple will issue a temporary password, and that password grants access to iCloud.

That means the 16-year old kid who just took your credit card delivery order at Domino's has all the info he or anyone else needs to ruin your life and your credit.

DO NOT Store Credits Cards With Merchants, PERIOD

- It is simply not worth the risk
- Using 1Password, you can instantly fill-in your CC data with a single keystroke at the second it is needed, without ever storing it online anywhere
- Mat Honan's woes originated with the "last four digits" being an attack vector used to take over his identity

Question:

- When you pay with your credit card at WalMart, do you let them **keep** your credit card in their cash register when you leave?
- *Of course not!*
- So then why do you leave your credit card behind with online merchants?
- It's ***THE SAME THING!***

iTunes/App Store Purchases

- Do NOT keep a credit card on file with Apple in the iTunes Store, Mac App Store, or App Store
- Instead, buy iTunes gift cards (available absolutely everywhere) with cash or credit cards
- Use the “Redeem” function in the iTunes/App Store to deposit the value into your account

Account Information

Secure Connection

Apple ID Summary

Apple ID:		Edit ›
Payment Type:	No credit card on file.	Edit ›
Billing Address:		Edit ›
Country/Region:	United States	Change Country or Region ›
Apple ID Balance:	$0.71	

Account Information

Apple ID Summary

Apple ID:		Edit ›
Payment Type:	No credit card on file.	Edit ›
Billing Address:		Edit ›
Country/Region:	United States	Change C
Apple ID Balance:	$0.71	

amazon

Mike's Amazon.com | Today's Deals | Gift Cards | Help

Shop by
Department

Search All

Customer Service | Your Account | Your Orders | Returns Center | Manage Your Kindle

Your Account > Edit or Delete a Payment Method

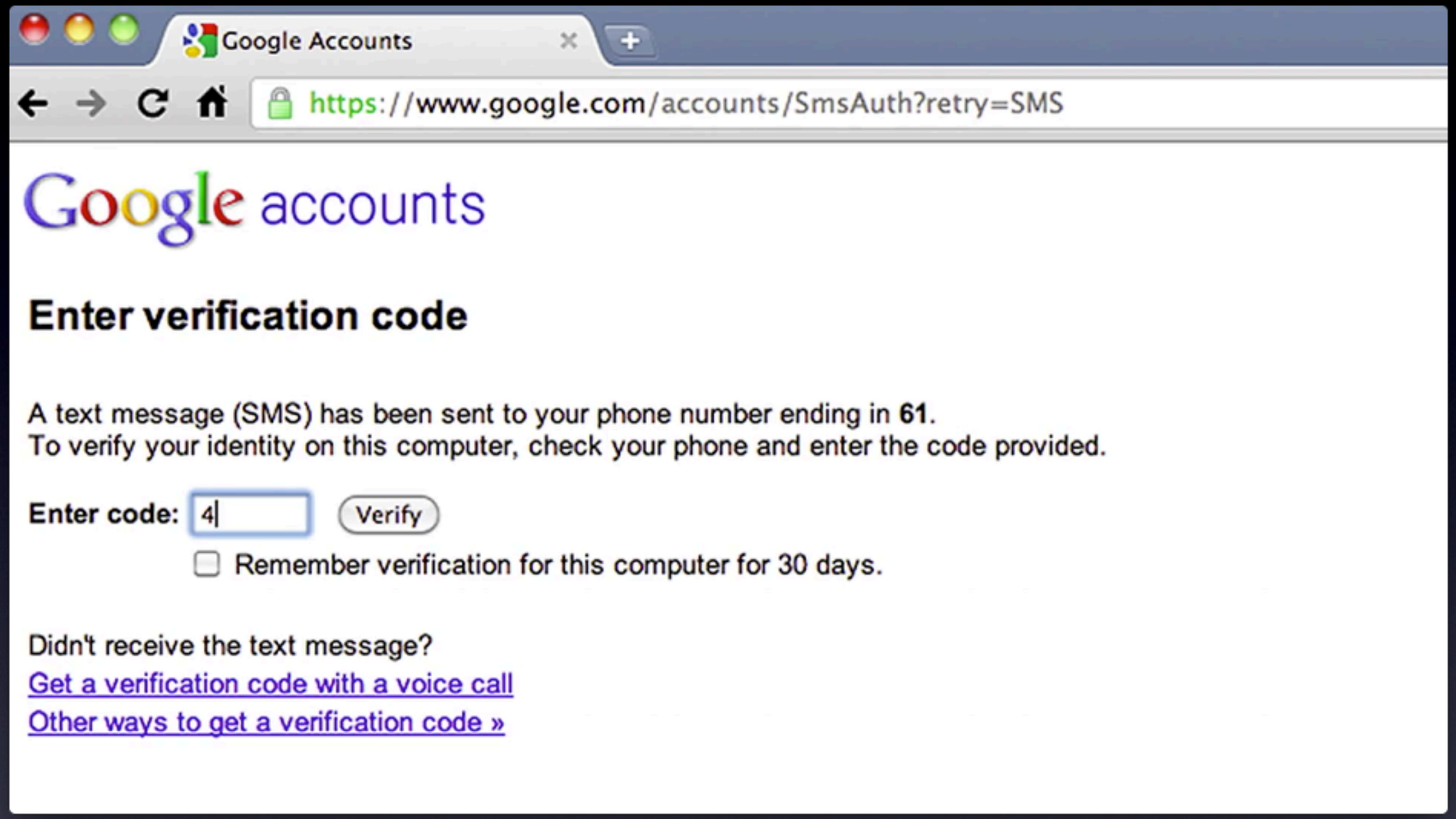
You currently have no payment methods in our system.

If you want to add a new credit or debit card to your account, click here.

Google 2-Factor Auth

If You Use Gmail for **ANYTHING**

- Turn on Google 2-Factor Authentication **TODAY**
- Ten minutes of pain for a whole lot of gain
- Free


Google Accounts
https://www.google.com/accounts/SmsAuth?retry=SMS
Google accounts
Enter verification code
A text message (SMS) has been sent to your phone number ending in 61.
To verify your identity on this computer, check your phone and enter the code provided.
Enter code:
4
Verify
Remember verification for this computer for 30 days.
Didn't receive the text message?
Get a verification code with a voice call
Other ways to get a verification code »

HOWTO Movie

Cove Apple Club – Shop!

coveappleclub.com/shop.html

Reader

Cove Apple Club

Have fun & do more with your Mac!

The next time you need some new Mac gear, start your online shopping session with the link to Amazon on this page. Your purchase will earn a little money for the Cove Apple Club, which we'll use to buy a new widescreen video projector for the club! We'll also update club members on the earnings every month.

So be sure to click the Amazon logo below when you need to shop for Mac products online...and "give back" to the Cove Apple Club -- without costing you an extra cent! Thanks!

On an iPhone or iPad? Amazon Banner above not displaying?
Click this link instead.

Earnings Report Totals

Glossary

July 25, 2012 to August 7, 2012

	Items Shipped	Revenue	Advertising Fees
Total Amazon.com Items Shipped	7	$134.59	$11.47
Total Third Party Items Shipped	7	$110.51	$5.93
Total Items Shipped	**14**	**$245.10**	**$17.40**
Total Items Returned	**0**	**$0.00**	**$0.00**
Total Refunds	**0**	**$0.00**	**$0.00**
TOTAL ADVERTISING FEES	**14**	**$245.10**	**$17.40**

Earnings Report Totals

Glossary

January 1, 2012 to August 7, 2012

	Items Shipped	Revenue	Advertising Fees
Total Amazon.com Items Shipped	92	$11,277.75	$493.49
Total Third Party Items Shipped	65	$1,928.76	$109.57
Total Items Shipped	**157**	**$13,206.51**	**$603.06**
Total Items Returned	**-2**	**-$200.00**	**-$8.00**
Total Refunds	**0**	**$0.00**	**$0.00**
TOTAL ADVERTISING FEES	**155**	**$13,006.51**	**$595.06**

AUG

22

Cove Apple Club

7:00 PM - 8:00 PM

Cove Apple Club

August 8, 2012