



## Staying Safe on the Internet



Mark Schulman

# Your Presenter



- Mark Schulman
- IT professional for almost 40 years
- No affiliation with any product

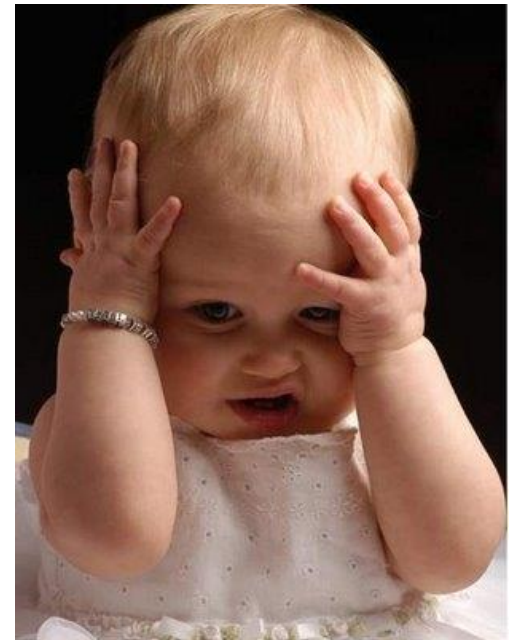
# What We'll Talk About

- Passwords
- Email Safety
- Staying Safe in Public
- Shopping Safety
- Odds n' Ends



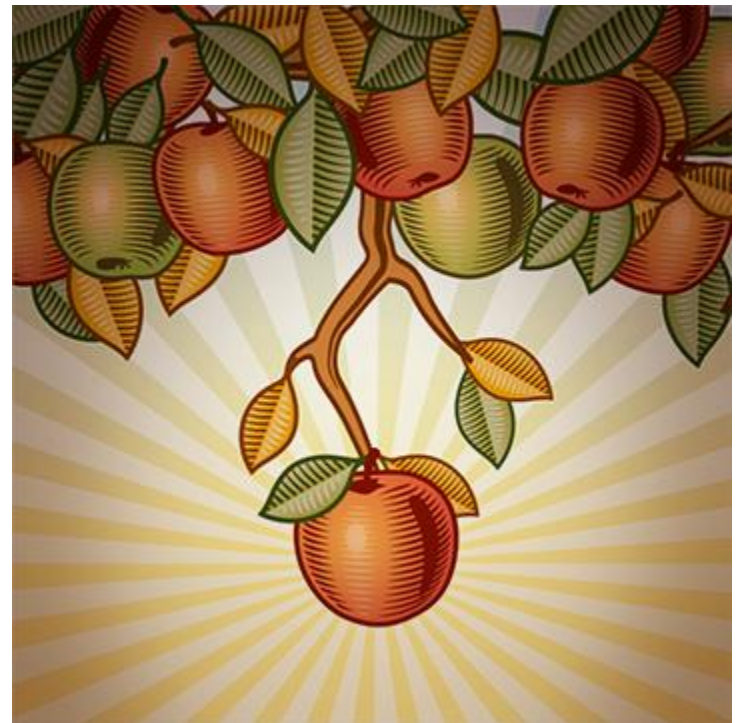
# This Stuff Isn't Entirely Easy

- Computer security seems inscrutable
- Bad guys are really good at it
- How are you supposed to know?



# Easier Stuff

- We're going for the low-hanging fruit



# Passwords



# Passwords

- Passwords are the keys that open your online identity
- A compromised password can be disastrous



# Top 10 Password Tips

- Hackers are really good at guessing passwords
- Here's the usual advice
- The Top 10 Password Tips (except there are only 6 of them) ...





## Password Tip #6

6. Don't write down passwords

... might be willing to give on this one

## Password Tip #5

### 5. Don't use words or names



jruqibn



tablespoon

## Password Tip #4

### 4. Use a variety of characters



pr6TZ&4



twiuzg

## Password Tip #3

### 3. Make your passwords as long as possible



whethersnowbyrest



dog

## Password Tip #2

### 2. Don't use personal information



4073662041



max

# Password Tip #1

1. Use a different password everywhere

## Bonus Tip - Laptop Users

- Beware passwords that are easy to spot as you type



???

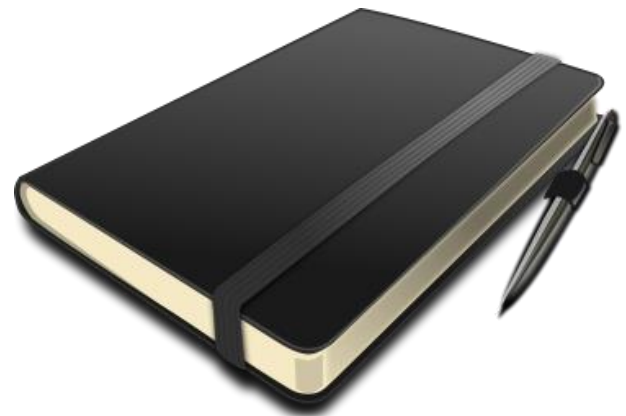
- How can I possibly follow all those rules?





# Less-Acceptable Method

- Write them down in a notebook (even though we said not to)
- Better to follow the other rules
- Protect the notebook very carefully:
  - Must never leave the house
  - Make it inconspicuous
  - Hide if possible



# Better Method

- Password manager



# Password Managers

- Programs that store all your passwords
- Unlocked by a single password
- Enables you to use very good passwords (it'll make them up for you)
- Will type your passwords for you
- You only have to remember one password, so *make it a good one!*
- Example: LastPass

LastPass



The Last Password You'll Ever Need.

# Demonstration



# LastPass

# 2-Factor Identification

- Security factors:
  - Something you know
  - Something you have
  - Something you are
- Whenever possible, use two-factor identification
- Some inconvenience, but far safer



# Demonstration



## 2-Factor Authentication

# Prepare

- Have a list of passwords to change if you lose your phone or laptop
  - email
  - Facebook
  - Amazon (Kindle)
  - etc.



# Email Safety





# Email Safety

Major concerns:

- Avoiding phishing attacks
- Avoiding viruses & spyware
- Reducing SPAM



# Phishing Attacks

- Phishing: Mean people trying to convince you to give up personal information
- Typically email from financial institutions asking you to “confirm” your account information
- No self-respecting institution needs you to confirm your information



CC:

From: "security" <security@boa.com>  Add to Address Book  Add Mobile Alert

Subject: Your Online is Blocked

Date: Sat, 29 Sep 2007 14:23:31 +0200



---

## Your Online Banking is Blocked

---

Dear Customer,

We recently reviewed your account, and suspect that your [Bank of America](#) account may have been accessed by an unauthorized third party. Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your online account access, we need you to confirm your account, to do so we need you to follow the link below and proceed to confirm your information:

[https://www.bankofamerica.com/cgi-bin/imcprd.dll/Ctrl.jsp?BV\\_UseBVCookie=yes](https://www.bankofamerica.com/cgi-bin/imcprd.dll/Ctrl.jsp?BV_UseBVCookie=yes)


Tank you for your patience as we work together to protect your account.

Sincerely,  
[Bank of America](#) Customer Service

**\*Important\***

Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.

---

[Bank of America](#), N.A. Member FDIC. [Equal Housing Lender](#) 

© 2007 Bank of America Corporation. All rights reserved.

# Phishing Give-a-way

- Missing “To:” address
- Grammar and spelling errors
- Fake links

To restore your online account access, we need you to confirm your account, to do so we need you to follow the link below and proceed to confirm your information:

[https://www.bankofamerica.com/cgi-bin/imcpprd.dll/Ctrl.jsp?BV\\_UseBVCookie=yes](https://www.bankofamerica.com/cgi-bin/imcpprd.dll/Ctrl.jsp?BV_UseBVCookie=yes)

Tank you for your patience as we work together to protect your account.

Sincerely,  
Bank of America Customer Service

**\*Important\***

Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.

---

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 

© 2007 Bank of America Corporation. All rights reserved.

<http://elportaldepeten.com/galeria/sql/cancel.php>

# What to Do

- Almost all requests to “confirm” information are bogus
- Never click on a link in a suspicious email
- Call the institution



# A Non-Self-Respecting Institution

- No self-respecting institution needs you to confirm your information.



# Email Viruses & Spyware

- Most common way to catch a virus: email attachments
- Photos (.jpg) are generally safe; anything else is suspect



# What to Do

- Never open attachments that you're not expecting
- Beware deceptive-looking filenames:  
**familyphoto.jpg.exe**
- Watch for unusual extensions (.scr)
- Especially dangerous: .exe, .com, .bat
- Never trust the "from" line in an email. Ever.
- Look for personalization, but even then ...  
TNO!

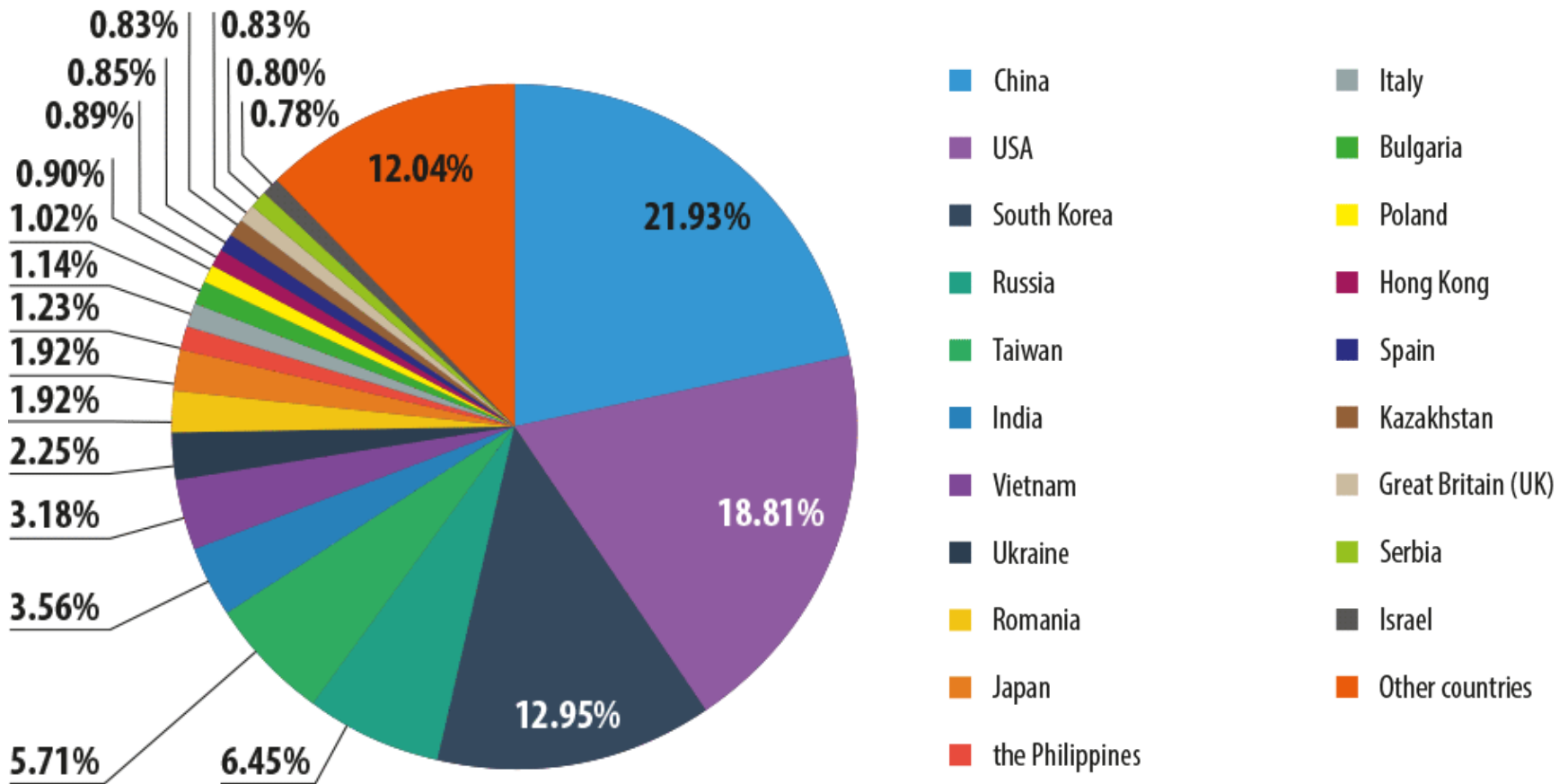


# SPAM

- Unsolicited advertisements
- Threatens the entire email infrastructure
- About 66% of email traffic is SPAM (1Q 2014)



# Where is It From?



# The SPAM Hit Parade

- Stock is about to skyrocket
- Financial institution suspended your account
- Package couldn't be delivered
- Nigerian prince(ss)



# SPAM Do's and Don'ts

- Never respond
- Don't click unsubscribe links
- Don't fall for the scams



# SPAM Strategies

- Be careful giving out your email address
- Don't give out other people's addresses
- Don't post your email address online
- Use disposable email addresses



# Disposable Email Addresses

- Unique email address that you give to a website or company
- Forwards to your “real” email address
- If you get SPAM’ed ...
  - you know who did it
  - you can turn it off
- Example: 33mail.com
- For other alternatives, Google “disposable email”



# Demonstration



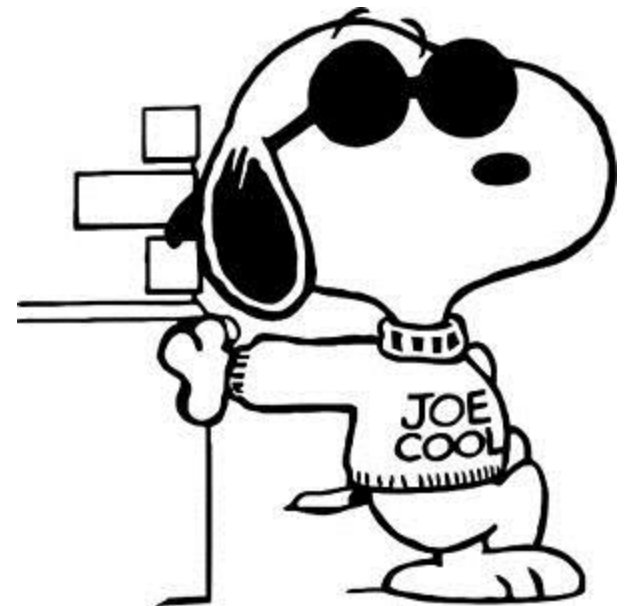
33mail.com

# An Extra Level of Cool

- Your own email domain

[bill@johnsonfamily.net](mailto:bill@johnsonfamily.net)

- Costs \$9 - \$15 / year
- Create as many addresses in your domain as you want
- Topic for another time ...





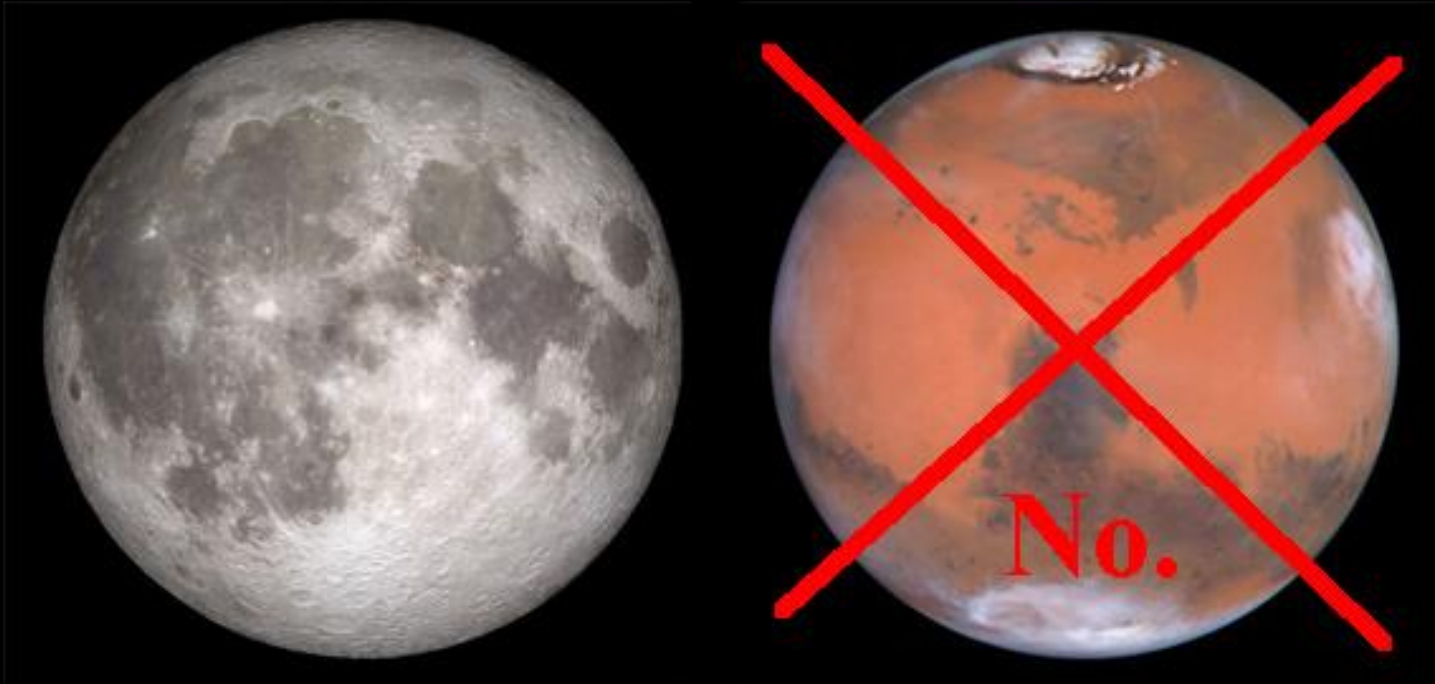
## And While We're on the Subject ...

- Don't believe everything you read or see in an email
- Emails and photos are easily faked
- My favorites ...



# Favorite Fake #1

Mars the size of the moon



## Favorite Fake #2

Israeli spy satellite captures shuttle Columbia exploding



## And While We're on the Subject ...

Don't forward emails unless you've researched them

- [snopes.com](http://snopes.com)
- [truthorfact.com](http://truthorfact.com)
- Google: topic + "hoax"



# Staying Safe in Public



## Tip 1 – Understand the Risks

- Public Wifi is great, but ...
- Very difficult to be completely safe on public Wifi
- Beware where you go



## Tip 2 - https

- Make sure the address bar says “https”



## Tip 3 - SSID

- Make sure you know the correct network name (SSID)





# Pop Quiz

- What is the SSID for  ?

CFYMCA-Guest

## Tip 4 – If You Must

- If you must access sensitive sites on a public Wifi, use a Virtual Private Network (VPN)
- Example: VyprVPN (\$6.67/month)



# Shopping Safely



# Shopping Online

- Many people wrongly fear online shopping
- Often safer than brick-and-mortar
- All that's required: a little common sense



# Online Shopping Do's & Don'ts

- Always use a credit card or PayPal tied to a credit card
- Do your research – products and companies!  
Don't be fooled by a flashy website
- Shop internationally with caution
- If it sounds too good ...
- Search for scams if the company is unfamiliar
- Understand return policies



# Odds n' Ends



# Watch the Kids

- Kids tend to ...
  - go to web sites they shouldn't
  - download software indiscriminately
  - use unsafe software



# Quiz

1. What browser comes on every Windows PC?
2. What browser do a majority of people use?
3. What browser is the equivalent of painting a target on your back?





Answer



Internet Explorer

# Don't Use Internet Explorer



Firefox

[firefox.com](https://www.firefox.com)



Internet  
Explorer



Google  
Chrome

[google.com/chrome](https://www.google.com/chrome)

# Viruses

- You must run an antivirus program
- Best: Norton Antivirus. Best free: AVG or Avast
- Getting rid of spyware or viruses is difficult -- sometimes impossible -- prevention is the key



# Malware Bytes

- No virus program catches everything
- Extra protection: run the free version of MalwareBytes frequently
- [www.malwarebytes.org](http://www.malwarebytes.org)




# Latest Scam

- Microsoft calling
  - Microsoft will never call you
  - Been around since 2009
  - Objective: Get you to buy worthless “protection”, clean out your bank account, or infect your computer



# Questions?





Presentation and notes at:  
<http://mark.schulmans.com>

Contact me at:  
mark @ schulmans . com