

# Practical Approach for Better Cyber Security

Tom Ashoff  
Senior Vice President  
Engineering

# Who am I and why do I care?



- I build security products for a living
- You are my neighbors
- Your business and reputation are on the line
- SMB is a target rich environment
- And supply chain attacks are all the rage

Plus Mark asked me  
... and said there would be lunch.



# About ThreatQuotient

- **Founded 2013**

- Real users with unmet need

- **Leader In Emerging Market**

- Tier-1 customers with >400% growth rate

- **World-Class Team**

- Cisco
- SourceFire
- iSight
- Symantec
- General Dynamics



SOURCEfire



GENERAL DYNAMICS

- **Financially Strong**



- **Global Presence**

- Sales, Channel Partners, Technical Support

- **Local Development Center**

- Mount Airy

Maryland Center of Excellence!



# Awareness

- Assume you are vulnerable to attack
- Why am I a target?
- What is the most valuable thing to your business?
- Prepare for what can go wrong

- 
- Here are some practical steps  
Practice them, teach them, test them



# Lock It Up!

- Backup your data
- Encrypt your hard drives
- Turn on the firewall
- Your phone... passcode, auto-lock




# Lock It Down!

- Cable Modem
  - Turn off remote management
  - Change default network ID & password
  - Don't allow inbound connections
- Wi-Fi – Home or Office
  - Segregate your guests from employees
  - Strong passwords to join
  - Change them when you have departures
- Wi-Fi – Traveling
  - Don't connect to something you don't know
  - Verify with the owner the network & passcode



# Practice Safe Browsing

- HTTP vs HTTPS ... S stands for “something”
- HTTP = unsafe
- Personal data and HTTP are a *No No!*
- Pick the *right* browser
- I use Google Chrome for a reason
  - Lots of plugins to keep you safe
  - Popup & ad blockers, password safes, & HTTPS *always*
  - And they patch it frequently

 <https://www.msn.com>



chrome



# Patching

- Everything has vulnerabilities (bugs)
  - *TV, Smart Thermostats, Phone, Refrigerators, IOT*
- Know how to get updates
- Apply them on a regular basis
- Automatic checking & updating



# Email... Necessary Evil

- Using an email service? Good!
- Don't recognize the sender? Do Not Click!
- Hover over links before clicking
- Recognize phishing tactics
  - Grammar matters!
  - Verify that address!
  - Who needs that many gift cards?
  - And stop asking me for my phone number!



Hello Joyce  Spam x



John C [redacted] <cslemni@cox.net>

to me ▾

Mon, Mar 4, 11:01 AM (4 days ago)



## This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe



Joyce, got a moment? Give me your personal cell number as I need you to complete a task for me.  
Regards.

 Reply

 Forward



# Example From a Family Member

**From:** Katie Flanagan <dlhoffberg@aol.com>

**Sent:** Wednesday, February 6, 2019 9:27 AM

**To:** Tessa Ashoff <TASHoff@...org>

**Subject:** QUICK REPLY

Address is not from Katie or from her work domain

Subject implies urgency, this tactic is used to make you quickly react and possibly miss red flags

EXTERNAL EMAIL: Do not open attachments/click links if source is unknown.

Hi Tessa,

Got a moment?

Give me your personal cell number, I need you to complete a task for me.

Thanks,

Katie Flanagan

Sent from my ipad

Email system tells us that the sender is not from the organization

Improper grammar is a sign of Phishing

Is Katie known to send email from her iPad (incorrect capitalization) or other devices?

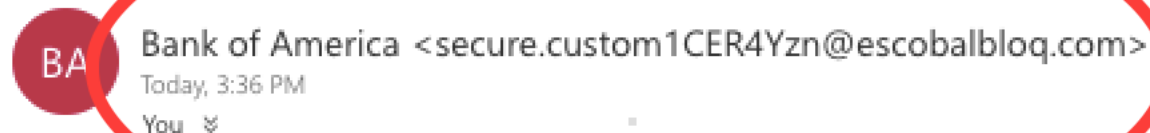


Account Alert: A New Update is Available



This looks serious and real!

Account Alert: A New Update is Available



### Security Alert

For security reasons, your account has been  
reviewed and confirm your personalized i

[Sign in to Update your Statements](#)

**Your security is important to us:** Sign in  
instructions that will be needed.

Please don't reply directly to this automatically generated email message. To ensure your safety, extra steps have  
been added to verify your identity.

Bank of America Email, 9<sup>th</sup> Floor NC1-028-09-02, 150 N College St., Charlotte, NC 28255.  
Please do NOT send any physical mail to this address, especially mail containing sensitive  
information.

Need to get in touch? Simply visit our [Contact Us](#) page for multiple ways to connect. Please do  
not reply to this email, as email replies are not monitored.

Read more about [Privacy & Security](#).

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)  
©2018 Bank of America Corporation. All rights reserved.



✓ Junk Email

From



Bank of America  
info@adden.fr

Date

☒ All

☐ This week

☐ Last week

☐ This month

☐ Select range

From

Sun 11/4/2018



To

Bank of America 

## Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNT

**IP-Conflict detected on your account**

Dear Valued Customer,

We're letting you know that we've detected multiple IP-Conflict on your online account, which will result to restrictions and closure of your online account. Kindly verify your account below to ensure the safety of your assets and online account.

For verification click <http://www.bankofamerica.com/verify> to restore and ensure the safety of your Account .

Sun 11/4/2018



## Security Checkpoint

To confirm the authenticity of me  
You last signed in to Online Bar

civilwarmerchandise.com/system/logs/valdiate/BOAlastest/login.php

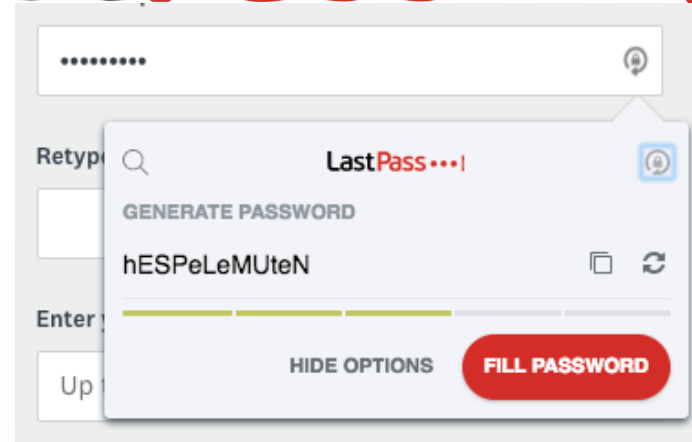
number. Always look for ver



# Passwords & Multi-Factor Authentication

# LastPass...

- Sharing isn't caring
- Different passwords
- Strong passwords
- How good is your memory?
  - LastPass or OnePassword
- Tokens, BioMetrics, Dual-factor Authentication
  - Google Authenticator as example
  - Text authentication codes



**Two Factor Authentication**



# Summary

- Awareness & Training (challenge your team)
- Backup and Encrypt your data
- Lockdown your Wi-Fi
- Lockdown permissions on your modem, laptop & mobile devices
- Know where and what you're surfing
- Exercise caution when dealing with email
- Get a password manager.... please!



## CYBER TIPS FOR YOUR BUSINESS

- **Assess risk and identify weaknesses** – If your sensitive information is linked to the Internet, then make sure you understand how it's being protected.
- **Create a contingency plan** – Establish security practices and policies to protect your organization's sensitive information and its employees, patrons, and stakeholders.
- **Educate employees** – Make sure that employees are routinely educated about new and emerging cyber threats and how to protect your organization's data. Hold them accountable to the Internet security policies and procedures, and require that they use strong passwords and regularly change them.
- **Back up critical information** – Establish a schedule to perform critical data backups to ensure that critical data is not lost in the event of a cyber attack or natural disaster. Store all backups in remote locations away from the office, and encrypt sensitive data about the organization and its customers. Invest in data loss protection software and use two-factor authentication where possible.
- **Secure your Internet connection** – Use and regularly update antivirus software and antispyware on all computers. Automate patch deployments across your organization, use a firewall, encrypt data in transit, and hide your Wi-Fi network. Protect all pages on your public-facing websites.
- **Create a continuity plan** – A continuity plan ensures that of nature, accidents, and technological or attack-related emergencies. Business functions can continue to be performed during a wide range of emergencies, including localized acts templates for this type of plan at <http://www.fema.gov/planning-templates>.

