

# Welcome

To

## Password Management – Practical Strategies

Hosted by:



Content by:



Presenter: Ray Cool, CEO  
PBSI Technology Solutions  
Webinar will begin at 1:00

# Welcome

to

## Cybersecurity Education Series

Hosted by Foster & Motley

Content provided by PBSI Technology Solutions

### Series Goals

- Educate listeners how to protect electronic valuables
- Improve knowledge about electronic security
- Provide practical information about what to change and how to do so

### Topic Summaries

- Securing Personal Information
- Email Security Practices
- **Password Management – Practical Strategies**
- File Encryption, Cloud Security & Public Wi-Fi

available on Foster & Motley website

available on Foster & Motley website

**today's topic**

4 of 4

# Agenda

## Password Management – Practical Strategies

### Today's Agenda

- Why does password security demand our attention?
- Password guidelines
- Benefits of using a Password Manager
- Create a system to remember unique passwords
- Alternatives to a Password Manager
- Demonstration of LastPass setup

**PBSI Technology Solutions**  
*"IT Security Specialists"*

## Who is PBSI?

- Technology Services provider for hundreds of clients in the tri-state including Foster & Motley
- Experienced – 75% of staff have 10+ years experience w/PBSI
- Proactive IT security monitoring for businesses & professionals

# Why do we need protection?

## The Internet Today is a Dangerous Place

- Increasingly, PCs are being infected with malware that steals passwords and copies data
- New keylogging and phishing attacks are changing constantly – Bad guys are smart, motivated and *relentless*
- The victim is typically NOT notified – Keylogging malware may be currently active on millions of unaware PCs

## Email Addresses and Passwords Are For Sale

- 6.2 Billion emails are available for sale on the Darkweb (was 2.7 Billion just 2 years ago)
- 1.2 Billion of them include exposed, cracked passwords
- Cisco, Microsoft, LinkedIn, Yahoo, Gmail, MySpace, DocuSign, Adobe, Dropbox, Tumblr and MANY others
- SolarWinds Orion hack compromises 250+ large organizations + US Gov, DOD, DOJ...
- [Secure Dark Web Exposed Password Check](#)



# Password Guidelines

## How to make my passwords safe



### 1. Keep my passwords private – and unique

- Don't reuse the same password on multiple sites. "Normal" passwords create a big security problem
- 1.2 Billion exposed email + pw combinations can be used on any bank or credit card site in the world
- If you have used a "normal" password in the past, change that password on all sites – today would be good...

### 2. Don't Store Important Passwords on your Web Browser

- Web browsers are wide open & exposed if a device is hacked – every browser password is available to a hacker
- Password Managers are protected by an added secure password, and all stored passwords are encrypted

### 3. Other Password Management Principles

- Enable two-factor authentication for all web accounts that offer it – especially important for email
- Password security – Never store written passwords anywhere around your desk or keyboard
- Don't use work email address for personal accounts & don't use same passwords on home & work accounts
- Find out if your passwords have been compromised – PBSI can do a darkweb search - free on request

### 4. Use a Password Manager

- LastPass, Dashlane, many others – Pick one - just do it!
- One commonly-missed benefit – losing a password might be costly - bitcoin-password could cost millions

# Create a System to Remember Unique Passwords

## Idea: Create a similar-but-different system for Remembering Passwords

- Choose a “normal” pw – but NEVER use it – just remember it
  - “normal” password - Include text portion and number portion
  - Example: “normal9” or “n9” = <mytext1234>
- Then: make notes to yourself that don’t expose the password, but make it knowable to you
  - Notes would impact text and number portion
  - For text portion change or capitalize: Ex: Cap 3<sup>rd</sup> would = myText1234
  - For number portion: Replace numbers, so n9 4433 would = mytext4433
  - Put it together: n9 Cap 2<sup>nd</sup> 6543 = mYtext6543
- Store your notes in a secure location (examples below)

# Demonstration

## Alternatives to a Password Manager

Alternatives If you don't use a password manager (none as secure as a password manager)

- **Alternatives – Highly recommend you encrypt (require a password to open)**
  - **OneNote** – If you use OneNote - Store passwords in an encrypted OneNote tab
  - **Word or Excel** - Encrypted Word or Excel document – stored in the cloud or locally – **use a long password**
  - **Email Contact Notes** (NOT encrypted) – Store your pw notes (never passwords themselves) in obscure contact
- **Handwritten passwords?** In today's world, this is simply not practical for most of us





# Use a Password Manager

## The best way to securely store passwords

### 1. LastPass Free Feature List (free)

- LastPass Free – provides encrypted secure password storage for all web logins
- Synchronizes across all devices (PCs, Laptops, Macs, Tablets, iPads, iPhones, & Android phones)
- Encrypts passwords at a very high level
- Autofills stored passwords on web sites
- Strong password generator
- Stores secure notes (addresses, garage opener codes, Wi-Fi passwords, etc.)

### 2. LastPass Premium Feature List (\$36 /yr)

- Emergency access contact
- Multifactor authentication

### 3. LastPass Families Feature List (\$48 /yr)

- Share DESIRED passwords (ex: Netflix, Amazon, Mobile wireless vendor)
- All other passwords remain private to each family member
- Cost – Add 5 more users to Premium for \$1 / mo total
- <https://www.lastpass.com/pricing>

# Demonstration

## LastPass

### 1. Create your account

- Install LastPass on your device – purchase direct from vendor site - [www.lastpass.com](http://www.lastpass.com)
- Set Master Password - Make it secure but not TOO long (8-10 char) (think: hundreds of times)  
Remember me (or remember login) = YES  
**Remember password = NO**  
YOU (not Foster & Motley) are the owner and manager of your LastPass and passwords

### 2. Set key security choices

- Set recovery mobile phone number
- Set secondary email address

### 3. Import passwords from your browser

### 4. Add 1 or more new site manually (login & password)

### 5. Add LastPass to your other devices

- App store – Download LastPass – then login – Do NOT create another account

# Demonstration

## Install LastPass

Purchase directly and install from vendor site  
[www.lastpass.com](https://www.lastpass.com)

Simplify your life.

LastPass remembers all your passwords, so you don't have to.

Get LastPass Free

[Upgrade to Premium for just \\$2/Month >](#)

# Demonstration

## Create your account Enter your Email and Master Password

### Get started with your email

Email address

janetlynnereed@gmail.com

☒ I agree to the [Terms](#) and [Privacy Policy](#)

[SIGN IN](#) [CREATE AN ACCOUNT](#)

janetlynnereed@gmail.com

New master password

..... [SHOW](#)

Confirm master password

..... [SHOW](#)

Password hint (optional)

In case you forget

[BACK](#) [NEXT](#)

### Leave yourself a lifeline

Since we can't reset your password, this reminder is your phone-a-friend... and that friend is you.


Make sure your reminder is clear to you, but don't include your password in it!

# Demonstration

## Account Settings - Phone Recovery

Account Recovery

Don't lose access to LastPass



We strongly recommend adding an account recovery phone number so you can access your account if you ever forget your master password.

Not Now

Add Number

Add Phone Number

Enter a phone number that can be used to help you get back into your account if you ever forget your password. Your phone number will only be used for the purposes of sending you a verification code for account recovery.

Account recovery phone number

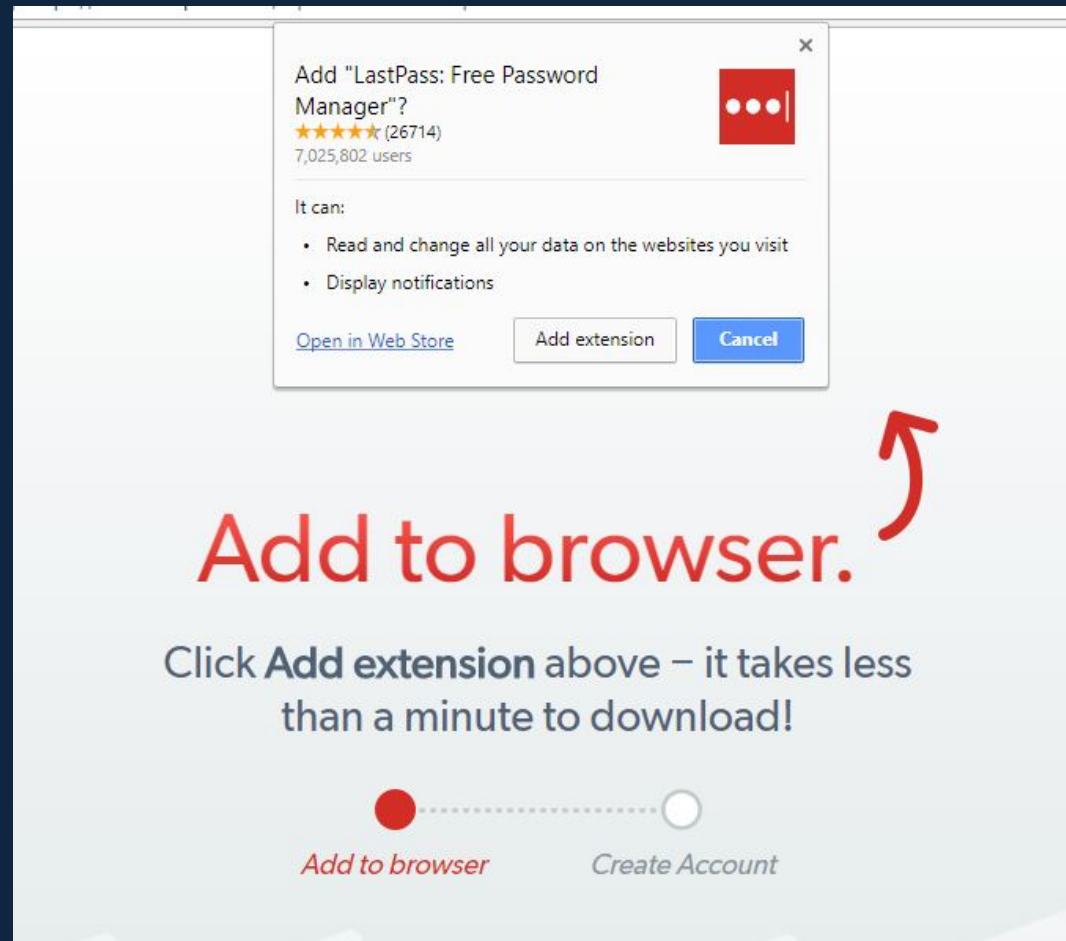
United States(+1)

Send Test Code

\*Message and Data Rates May Apply

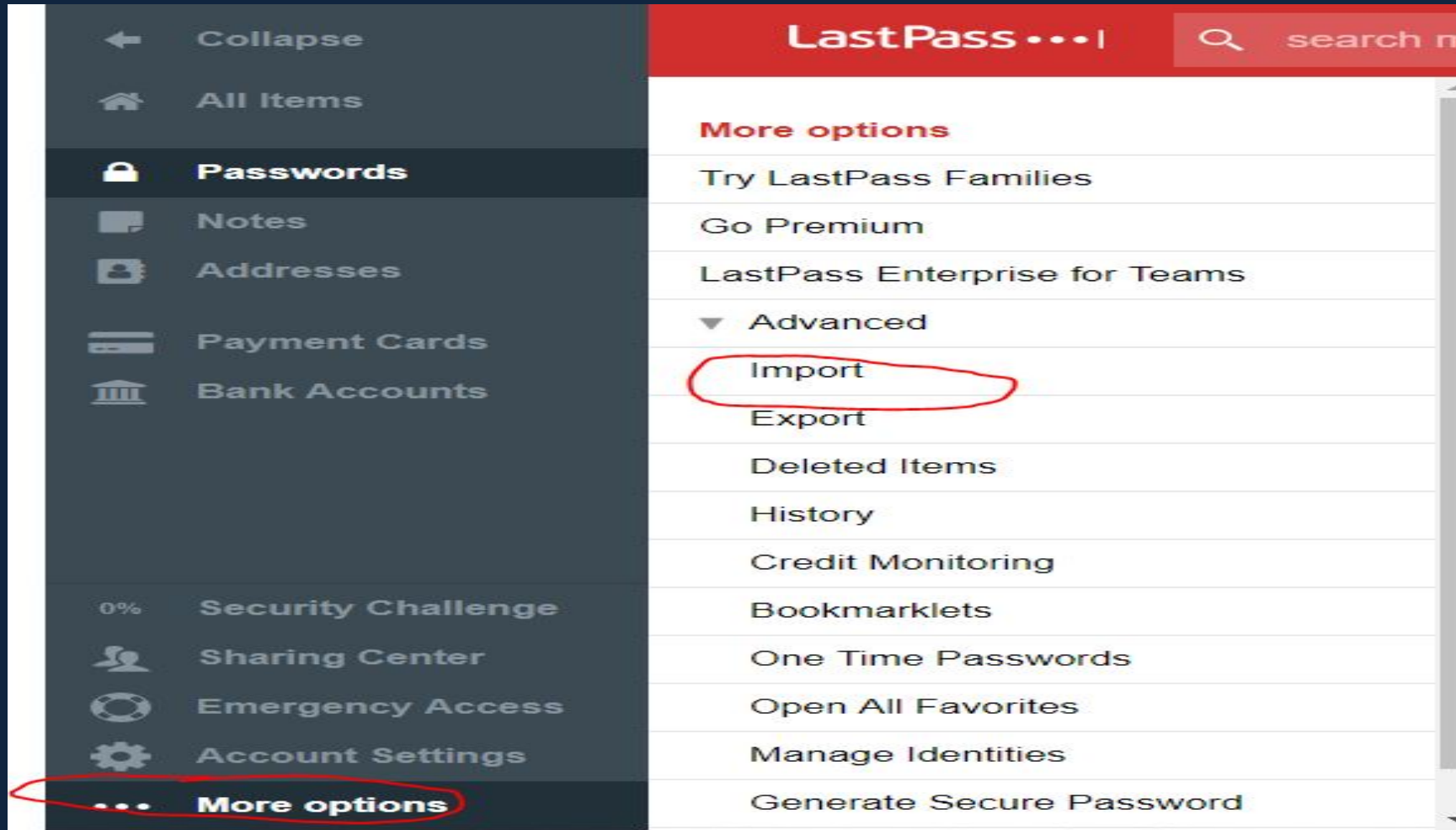
# Demonstration

## Add Browser Extension



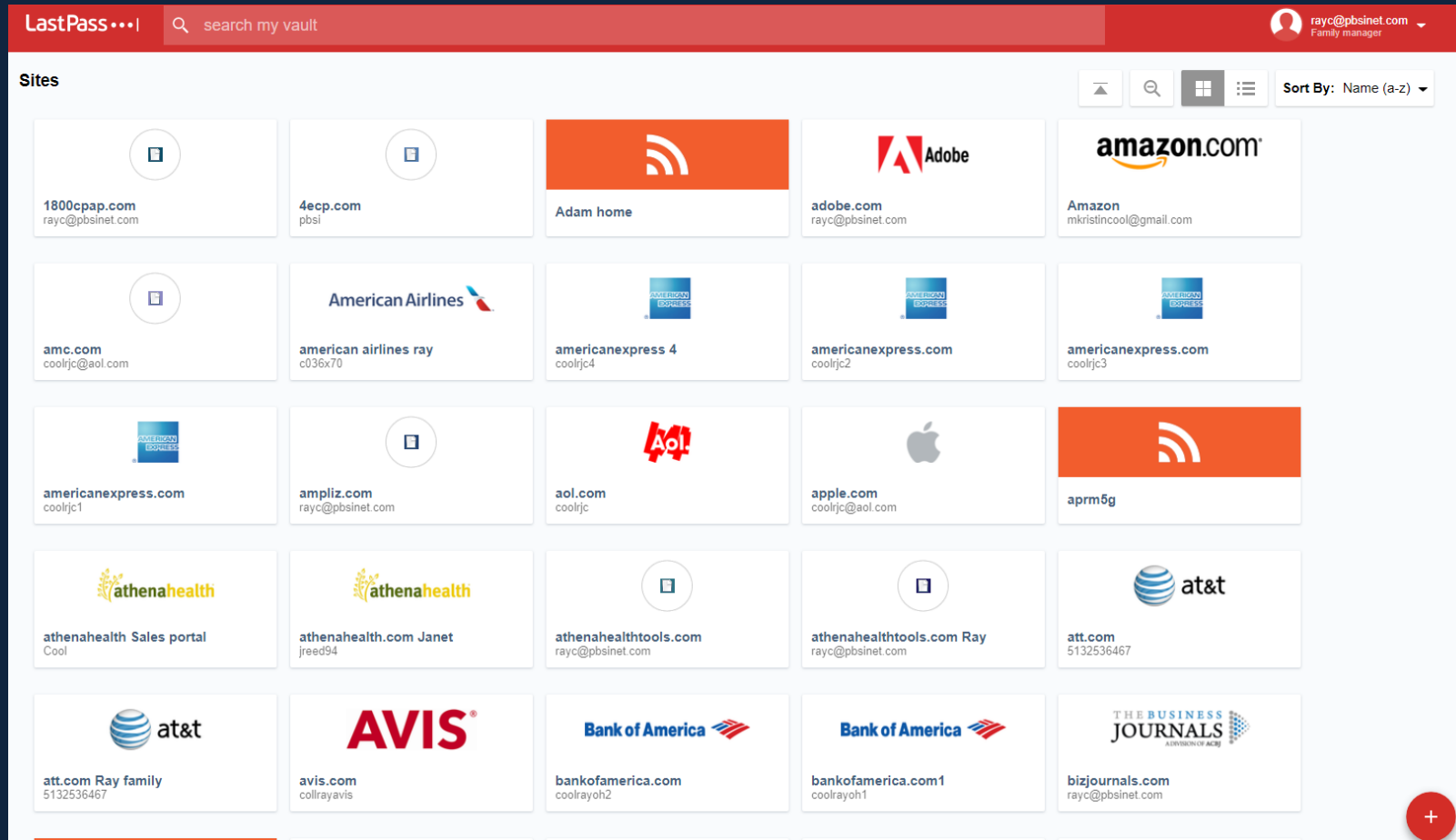
# Demonstration

## Import Browser Passwords



# Demonstration

## Manually add a New Site & Password





# Demonstration

## Add a New Site & Password

Add Site

LastPass...|

URL:

https://www.amazon.com

Name:

Amazon

Folder:

Shopping

Username:

username

Password:

.....

Notes:

Advanced Settings:

☐ Require Password Reprompt

☐ Autologin

☐ Disable AutoFill

Cancel

Save

# Summary – Managing Passwords

## Password Management Principles

Don't reuse the same password on multiple sites

Don't Store Important Passwords on your Web Browser

Change reused passwords – today would be a good idea...

Enable two-factor authentication for all web accounts that offer it

Find out if your passwords have been compromised – PBSI will check for free

## Options for Managing Passwords

Encrypted Word document

Encrypted OneNote Tab

Use a Password Manager

# Summary - Essentials of Securing Personal Information

## Establish protection from the “open” internet

- Use secure passwords to protect your Wi-Fi & IoT (Internet of Things) devices – and keep firmware updated

## Secure your Desktops, Laptops & Files

- Antivirus & Malware protection – Use non-free antivirus, auto updated without manual intervention, daily vulnerability scanning w/alerts
- Patch Management - Security issues frequently related to un-updated software patches
- Automate Your Backup – multi-location, locally encrypted, redundant

## Email Security

- 5 principles of secure email evaluation
- Turn on Multifactor Authentication

## Password Management

- Don't use common passwords on multiple sites
- Use a password manager or another secure option

## Beware public Wi-Fi

- No passwords on Public Wi-Fi - If logging in with password , use a password manager or VPN tool, or use cellular

## Know if your PCs & Macs are secure

- Consider online security monitoring – know if you have sleeping vulnerabilities

## Training - Encourage every family member to learn secure behavior

- Learn the essentials of safety – especially passwords, email and web browsing

# Webinar Summary

Thank you for your attendance  
Thank you to our friends at Foster & Motley

## Included Handout

“IT Security – Password Management Recommendations”

## How can PBSI help you? - Concierge IT Security Services

Pricing below has been discounted by 25% for Foster & Motley clients

Data Breach Risk Scan (up to 3 PCs/Macs), scheduled during daytime

Security Risk Assessment– includes above Risk Scan, adding personal security review by phone & direct connect

Online Security Monitoring, Antivirus, Patch Management, Vulnerability Scans (up to 3 PCs/Macs)

Online Security Monitoring, Antivirus, Patch Mgmt, Vulnerability S. (up to 3 PCs/Macs) w/S1 Ransomware Protect

Online Backup with redundant local encrypted backup (per PC or Mac)

Concierge Security Services – Your own personal security advisor included at no cost with any of above services

### Cost for F&M Client

\$ 200 one time

\$ 325 one time (adds \$125)

\$ 225 / yr up to 3 PCs/Macs

\$ 325 / yr up to 3 PCs/Macs

\$ 115 / yr per PC/Mac

included with any of above

## Webinar Follow-up

- Call or email questions, or request free quotation
- Speaker contact Ray Cool, CEO

(800) 626-2306

(513) 924-3915

[itservices@pbsinet.com](mailto:itservices@pbsinet.com)

[rayc@pbsinet.com](mailto:rayc@pbsinet.com)

## Upcoming Webinars

- Securing Personal Information
- Email Security Practices
- **Password Management – Practical Strategies**
- File Encryption, Cloud Security & Public Wi-Fi

available on Foster & Motley’s website

available on Foster & Motley’s website

**today’s topic**

Thursday February 18, 1:00 pm