Welcome

Password Management & Public Wi-Fi Security

Hosted by:

Foster & Motley
FOSTERING LIFE'S WEALTH

Content by:

PBSI Technology Solutions
800-626-2306-Toll Free 513-772-2255-Local

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

Foster & Motley
FOSTERING LIFE'S WEALTH

Welcome

Foster & Motley Clients

to

Security Education Series

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 Data	available on Foster & Motley website
• Email Security Practices	available on Foster & Motley website
• File Encryption & Cloud Security	available on Foster & Motley website
• **Password Management & Public Wi-Fi**	today's topic

Foster & Motley
FOSTERING LIFE'S WEALTH

Agenda

Password Management & Public Wi-Fi Security

Tools for managing passwords and internet security

- Why does password security demand our attention?
- Password guidelines
- Understanding the dangers of public Wi-Fi
- Benefits of using a Password Manager

Foster & Motley
FOSTERING LIFE'S WEALTH

PBSI Technology Solutions
"IT Security Specialists"

Who is PBSI?

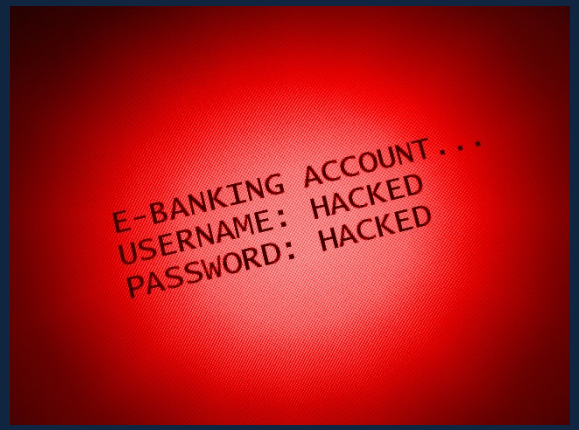
- Technology Services provider for hundreds of clients in the tri-state including Foster & Motley
- Experienced – 75% of staff have 10+ years experience w/PBSI
- Proactive IT security monitoring for home and business

Foster & Motley
FOSTERING LIFE'S WEALTH

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



Darkweb Exposed Password Check

- 2.7 Billion emails are available for sale on the Darkweb
- 1.2 Billion of them include exposed, cracked passwords
- LinkedIn, Yahoo, Gmail, DocuSign, Adobe, Dropbox, Tumblr, MySpace and 30 others
- Experian – smaller than ALL of the above breaches in 2017
- Secure Dark Web Exposed Password Check.

Foster & Motley
FOSTERING LIFE'S WEALTH

Password Guidelines

How to make my passwords safe

1. **Change your passwords – today would be a good idea…**
   - Change passwords on a regular basis
   - Don't use "normal" or "easy" passwords (ex: Be yourself; everyone else is taken – By;eeit!)

2. **Don't reuse WORK passwords on personal sites, and vice-versa**
   - Use different password wherever you store credit card information

3. **Use a secure password manager**
   - LastPass ($24/yr) or Dashlane ($39/yr) or similar – these provide VPN security and encryption for stored passwords
   - Why? Manual password management is inevitably unsafe

4. **Enable two-factor authentication for all web accounts that offer it**
   - Yes, it's a hassle, but it works

6. **Find out if your passwords have been compromised**
   - PBSI can check organization domains, or lists of individual email addresses or https://haveibeenpwned.com/

Foster & Motley
FOSTERING LIFE'S WEALTH

Principles for Safe use of Public Wi-Fi

Well known "hosts" do NOT equate to "secure" hosts

Public Wi-Fi is NOT secure

- On public Wi-Fi, NEVER visit sites requiring login and password – Unless using a VPN
- NOT Secure: Starbucks, Marriott, Delta, airlines, hotels, restaurants, guest Wi-Fi at your attorney, CPA, etc.
- Passwords hacks are common on public Wi-Fi – banking on "presumed trust" of the host – using free hacking tools
- Beware Fake Wi-Fi – "Google Starbucks" ("Trump WiFi" scammed 1,000 RNC attendees)

How to know when Wi-Fi is secure

- Does requiring of a public Wi-Fi password ensure security? – No
- Wi-Fi is secure ONLY when you are using a Password Manager or VPN – Virtual Private Network
- VPN establishes a point-to-point encrypted "private" channel between you and one other party

How to safely use public WiFi

- Safe: Google searches are fine on public Wi-Fi – but STOP if prompted for a pw (Uber, Yelp, restaurant orders…)
- Solution: Use a Password Manager to login, or a VPN tool like Hotspot Shield VPN (free or $ 40/ yr)

Foster & Motley
FOSTERING LIFE'S WEALTH

Use a Password Manager

Tools for Protecting and Storing Passwords

1. Use a secure password manager

- LastPass ($24 /yr) or Dashlane ($39/yr) or similar – provide VPN security and encryption for all web logins
  - Encryption - All passwords and credentials are encrypted at a very high level
  - Auto-synchronization of passwords across all PCs, laptops, Macs, Androids, iPhones, iPads
  - Auto-fill passwords for login to stored websites
  - What they don't do – Don't store login/passwords for apps – only browsers

2. Ideas beyond a password manager for storing passwords safely

- Store passwords in an encrypted document, and store this locally or in the cloud – **use a complex password**
- Microsoft OneNote encrypted tab – Office 365 version ONLY - synchronizes across all PCs, laptops, Macs, iPxx, Androids
- Handwritten passwords? In today's world, this is simply not practical for most of us

Foster & Motley
FOSTERING LIFE'S WEALTH

Summary - Essentials of Securing Personal Information

Secure your Desktops & Laptops

- Antivirus & Malware protection – auto updated without manual intervention, daily vulnerability scanning
- Desktop Patch Management - Security issues frequently related to un-updated software patches
- Wireless Security – ensure latest encryption, control password access

Encrypt sensitive files

- Encrypt files “at rest” that include protected information (SS#s, CC#s, DOBs)
- Encrypt files with personal information during transmission

Backup on an automated schedule

- Don’t let lack of knowledge or attention put you at risk. Use an encrypted backup as a ransomware protection.

Beware public Wi-Fi

- No passwords on Public Wi-Fi - If logging in with password , use a password manager or VPN tool, or use trusted app (Bank app)

Know if your PCs are safe

- Online security monitoring

Training - Encourage every family member to learn secure behavior

- Learn the essentials of safety using email and web browsing

Foster & Motley
FOSTERING LIFE'S WEALTH

Webinar Summary

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

Included Handouts

"IT Security – What each of us need to know" and "How to evaluate dangerous emails"

How can PBSI help you? - Concierge IT Security Services

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

	Cost for F&M Client
Security Risk Assessment and in-person security training – one-on-one, scheduled during daytime	$ 325 one time
Antivirus, Online Monitoring, Patch Management, Vulnerability Scanning (up to 3 PCs/Macs)	$ 225 / yr
Data Breach Risk Scanning (up to 3 PCs/Macs)	$ 75 / yr
Online Backup with Ransomware protection (per PC)	$ 115 / yr
KnowBe4 Security Training – Ongoing phishing tests and security training emails (up to 3 emails)	$ 225 / yr

Webinar Follow-up

- Call or email questions, or free quotation (513) 772-2255 itservices@pbsinet.com
- Speaker contact Ray Cool, CEO (513) 924-3915 rayc@pbsinet.com

Upcoming Webinars

- Securing Personal Information available on Foster & Motley's website
- Email Security Practices available on Foster & Motley's website
- File Encryption & Cloud Security available on Foster & Motley's website
- **Password Management & Public Wi-Fi** today's topic

Foster & Motley
FOSTERING LIFE'S WEALTH