Welcome

File Encryption, Cloud Security & Public Wi-Fi

Protecting Important Personal Information

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

Cybersecurity 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 Information - Overview	available on Foster & Motley website
• Email Security Practices	available on Foster & Motley website
• Password Management – Practical Strategies	available on Foster & Motley website
• **File Encryption, Cloud Security & Public Wi-Fi**	today's topic

Foster & Motley
FOSTERING LIFE'S WEALTH

Agenda

File Encryption, Cloud Security & Public Wi-Fi

Protecting Important Personal Information

- When and why file encryption is important
- How to protect personal files “at rest” that include PHI or PII (SS#’s, CC#’s passwords, etc.)
- How and why to protect sensitive files during transmission
- Using the cloud securely
- Using public Wi-Fi securely

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 businesses & professionals

Foster & Motley
FOSTERING LIFE'S WEALTH

Why do we need protection?

The Internet Today is a Dangerous Place

- Increasingly, PCs & Macs are being infected with malware that steals passwords and copies data
- New key logging & phishing attacks change constantly – Bad guys are motivated and *relentless*
- Victims are NOT notified (SolarWinds attack) – Keystroke-logging malware may be active on millions of PCs

Email Addresses and Passwords Are For Sale

- 6.2 Billion emails are available for sale on the Darkweb
- 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 orgs - Microsoft, Cisco, US Gov, DOD, DOJ…
- List of biggest breaches can be found at: https://haveibeenpwned.com/

Foster & Motley
FOSTERING LIFE'S WEALTH

Protect (Encrypt) Important Documents “at rest”

What is File Encryption?

- Encryption is a term describing data that can’t be read without a private “key”
- Encrypted data is garbled so that if opened it can’t be easily read or interpreted
- Encryption security varies based on technology used AND based on length of “key” (the password)
- Long non-dictionary passwords are encouraged. Length is the enemy of hacker decryption software

What Files Should Be Encrypted and Why?

- Encrypt sensitive files containing Personally Identifiable Information (PII) or Protected Health Info (PHI)
- From whom are you protecting info? Future hackers – YES (and maybe from IT support, children, etc.)

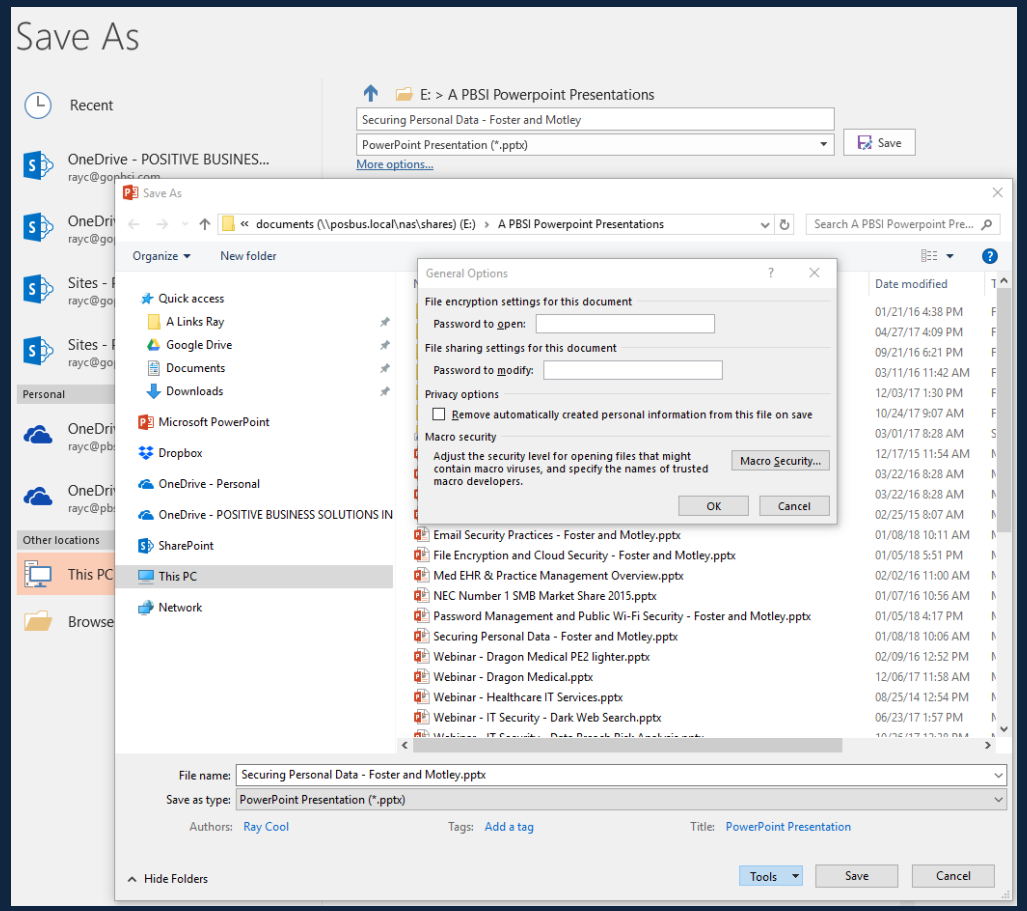
Encrypt Important Files “at Rest”

- MS Office - Most files can be encrypted – simply by adding a password
- Password protection = encryption

Foster & Motley
FOSTERING LIFE'S WEALTH

Demonstration

How to Encrypt a file



Foster & Motley
FOSTERING LIFE'S WEALTH

Protect (Encrypt) Sensitive During Transmission

Email - Encrypt Sensitive Files or Content Sent via Email – 3 Choices

- **Encrypt the email**
  - Requires purchase of an email encryption tool (option: Virtru for gmail is free)
- **Encrypt the attachment(s)**
  - Encrypt the document(s) – then attach to an email
  - Important - provide password to the recipient using different medium (text, voice or separate encrypted email)
- **Use a secured file sharing site** – like Foster & Motley's **ShareFile**
  - Go to website, login, look for file upload, and you'll be prompted to select file(s) to upload
  - File sharing links are automatically encrypted (presuming you know and trust the site)

Foster & Motley
FOSTERING LIFE'S WEALTH

Managing Location of Files and Folders

Know where documents are stored

Microsoft Office default save-as location is either C:\Documents, or OneDrive

- But – other apps (scans, photos, faxes) are not consistent
- When saving files, use “save-as” instead of “save” to know the location of file
- This “save-as” greatly increases the likelihood of success of controlling document location
- Beware file names starting with “Copy of….” – That will almost certainly create a duplicate copy

Idea: Keep documents with PII (Personally Identifiable Information) in a separate folder

- To setup a sub-folder – right click, add “folder”; name the folder (i.e.: Documents \ Tax Information)

Foster & Motley
FOSTERING LIFE'S WEALTH

Using Cloud Storage Securely

When and why is it best to use cloud storage?

- **When to consider cloud storage?**
  - Multi-location access - Home and other locations
  - Multi-device access (PC /laptop /iPhone /iPad)
  - Critical need for availability (when my network or PC are down)
  - Concerned about local PC backup
  - Concerned about reliability – Remove files from uncertain IT environment

- **Which Vendor?**
  - Most of us: Microsoft OneDrive (included with Microsoft 365) or Google Drive
  - If you wish: Apple iCloud, Amazon, Adobe, Dropbox, Box, others

- **Do I need to encrypt cloud files?**
  - Files with sensitive data, including PII or PHI – Recommended, subject to risk-tolerance
  - For highly sensitive information stored in the Cloud – use a long password

Foster & Motley
FOSTERING LIFE'S WEALTH

Principles for Safe use of Public Wi-Fi

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

- Prompting for public Wi-Fi password does NOT mean the connection is secure
- Wi-Fi is secure ONLY when you are using a VPN or Password Manager
- 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 VPN or Password Manager to login (I use Nord VPN)**
- **Solution: Use Cellular – Cellular traffic is always encrypted** (Simply turn Wi-Fi off)

Foster & Motley
FOSTERING LIFE'S WEALTH

Today's Summary

File Encryption, Cloud Security & Public Wi-Fi

Document Security

- Encrypt files "at rest" that include protected information (SS#s, CC#s, DOBs, Account#s, DL#s)
- Email - Encrypt files during transmission that contain PII or PHI

Use the Cloud securely

- Be cautious when storing sensitive information in the cloud

Careful on Public Wi-Fi

- On public Wi-Fi, NEVER visit sites requiring login and password – Unless using a VPN
- Cellular traffic is always encrypted & safe

Foster & Motley
FOSTERING LIFE'S WEALTH

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

Foster & Motley
FOSTERING LIFE'S WEALTH

Webinar Summary

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

Included Handouts

"MS Office & Pdf File Encryption"

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
Data Breach Risk Scan (up to 3 PCs/Macs), scheduled during daytime	$ 200 one time
Security Risk Assessment– includes above Risk Scan, adding personal security review by phone & direct connect	$ 325 one time (adds $125)
Online Security Monitoring, Antivirus, Patch Management, Vulnerability Scans (up to 3 PCs/Macs)	$ 225 / yr up to 3 PCs/Macs
Online Security Monitoring, Antivirus, Patch Mgnt, Vulnerability S. (up to 3 PCs/Macs) w/S1 Ransomware Protect	$ 325 / yr up to 3 PCs/Macs
Online Backup with redundant local encrypted backup (per PC or Mac)	$ 115 / yr per PC/Mac
Concierge Security Services – Your own personal security advisor included at no cost with any of above services	included with any of above

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

Webinar Summary

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

Foster & Motley
FOSTERING LIFE'S WEALTH