

# Welcome

to

# Email Security Practices

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

# 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 - Overview 1 of 4
- **Email Security Practices** today's topic
- Password Management – Practical Strategies 3 of 4
- File Encryption, Cloud Security & Public Wi-Fi 4 of 4

# Agenda

## Email security practices

- Why do we need protection?
- Fundamentals of email security
- How to spot “dangerous” emails

**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](#)



# Security Training - Email Safety Principles

## How to evaluate “bad” emails

### 1. Safety principle # 1 - Unsolicited vs. Solicited

- Unsolicited means unrequested and unexpected – even from a known source
- Even if you know the sender, is anything unusual about THIS email? (hover over sender name to confirm email address)
- Caution: Brief emails from “known” persons – Why? Malware frequently delivered from familiar name, short “to” list, single link

### 2. Safety Principle #2 - Antenna up!

- Does anything seem amiss? STOP – Do you need to click this now?
- Evaluate time of day, recipient list, brief content, out-of-character - uncertain why *this* person would send this content?
- Any misspellings? Grammar mistakes? Unusual phrasing? Unusual colors? Formatting? Font variations?

### 3. Safety Principle #3 - Don't get your news from email

- Beware current events/product releases (Olympics, disasters, holiday messages, celebrity news, Apple/Tesla product releases)
- Beware Social media – Popular sites are rife with phishing scams – Don't believe your friends are foolproof
- Does anything seem “too good to be true?” Does the content make you curious? (Ask yourself, who wants to make you curious?)

**Antenna up!** Scammers are very intentional in creating elaborate ruses – think twice and be very cautious

# Security Training - Email Safety Principles

## How to evaluate “bad” emails

### 4. Safety principle # 4 – Careful with Unsubscribe

- DON'T: Use “Unsubscribe” unless you are CERTAIN the source is credible. Instead, in Outlook, right click, choose “Junk”, then “Block Sender”
- Scammers use “unsubscribe” to 1) confirm your email address is real, and/or 2) initiate an attack
- Antenna up! Scammers are very intentional in creating elaborate ruses – think twice and be very cautious

### 5. Safety Principle # 5 – Know how to evaluate true vs. fake URLs

- Careful with fake DNS Domain Names
- Most important URL analysis skill – Know how to evaluate “bad” URL Domain Name
- URL is made up of:

URL protocol moniker (https://) - Everything up to and including first double slashes

DNS hostname (www.) - Starts after first double slashes, ends after first period

**DNS Domain Name - Starts after first period, ends before first single slash**



**Summary: Antenna up!** Scammers are very intentional in creating elaborate ruses – think twice and be very cautious

# Security Training – Other Email Safety Principles

Don't act without careful consideration

## Email Security Settings

- **Turn on Multifactor Authentication** on your email – and anywhere available (bank apps, investment logins)
- M365 – Implement MS Defender for Office 365 (formerly ATP) – “click” protection - \$2/mo
- M355 – Corporate accounts - Set “Transport rule” to block auto-forwarded emails – avoids Spear Phishing

## Links – Before you click

- Hover over link, checking spellings, unexpected content, added extensions (amex.us.com) (ups.pickup.com)
- If you think a request may be legit – instead of clicking link, go to vendor site and login (no copy/paste)

## Recent hacker spoofs

- Get ready! Tax season is coming - Login to confirm your IRS account now; Reset your IRS Pin#; Problem with your W-2
- Office 365 password for youemail@yourdomain expires today. Click here to Keep Current Password
- Text alerts – You receive text “Google has detected unusual activity” – reset your password – Never click on text alerts
- Apple/MS 365/Gmail account needs renewal/password reset, Resume attached, Word attachments = Ransomware
- Never respond if asked to click link for “confirmation” or “reset”, even if they know last 4 of CC#, last 4 of SS#
- If you have ANY concern you've made a mistake – change your password



# Security “Warning” Emails

## Security alert – login limit reached

Email Preview - Incorrect Password Limit Reached

From: [services@amazon-security.net](mailto:services@amazon-security.net)  
Reply-to: [services@amazon-security.net](mailto:services@amazon-security.net)  
Subject: Incorrect Password Limit Reached

[Send me a test email](#)  
[Toggle red flags](#)

**amazon** Your Account | [Amazon.com](#)

Message From Customer Service


Hello, customer,

You have entered the wrong password too many times. As a security precaution, we need more information from you. Once you've confirmed you own this account, we'll walk you through some steps to make your account more secure.

Is that you?


Your action is required to help us to protect you Amazon account securely.

Thank you.  
Amazon.com



## Password Change Warning email

Password Report for Pbsinet at January 20, 2021, 10:54:06 AM

 Pbsinet/MS <[parts@tanakamusen.co.jp](mailto:parts@tanakamusen.co.jp)>  
To: Ray Cool

[Reply](#) [Reply All](#) [Forward](#) [...](#)


Wed 1/20/2021 1:54 PM

**Office 365**  
Hi [ray@pbsinet.com](mailto:ray@pbsinet.com),

Password for [ray@pbsinet.com](mailto:ray@pbsinet.com) expires today  
You can change your password or continue using current password.

[Keep Current Password](#)

Pbsinet Support



# Shipping emails

From: Fedex Support <pe...@iceweb.net> Sent: Fri 10/11/2013  
To: support@winpatrol.com  
Cc:  
Subject: Your Rewards Order Has Shipped  
Attachments:  Order history page.zip (107 KB)



## SHIPPING CONFIRMATION

My FedEx  
REWARDS

This is to confirm that one or more items in your order has been shipped. Note that multiple items in an order may be shipped separately.

You can review complete details of your order on the Order History page

Thanks for choosing FedEx.

**Order Confirmation Number:** 3477683

**Order Date:** 10/09/2013



This is an automatically generated email. Please do not reply to this email address.

Dear UPS Customer,

New invoice(s) are available for the consolidated payment plan(s) / account(s) enrolled in the UPS Billing Center  
Please view UPS Billing Center attach document to view and pay your invoice.

(c) 2012 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.

For more information on UPS's privacy practices, refer to the UPS Privacy Policy.

Please do not reply directly to this e-mail. UPS will not receive any reply message.

For questions or comments, visit Contact UPS.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

# Example of Ransomware email

From: Fax Message <[FaxMessage@eFaxOnline.com](mailto:FaxMessage@eFaxOnline.com)>  
Reply-to: Fax Message <[FaxMessage@eFaxOnline.com](mailto:FaxMessage@eFaxOnline.com)>  
Subject: Your Customer Has Sent An eFax message - 4 pages



Fax Message [Caller-ID: 998-566-9234]  
You have received a 4 pages fax.

\* The reference number for this fax is [AT-AT-99034jks03szl-AT-AT](#).

View this fax using your PDF reader.

[Click here to view this message](#)

Please visit [www.eFax.com/en/efax/twa/page/help](http://www.eFax.com/en/efax/twa/page/help) if you have any questions regarding this message or your service. Thank you for using the eFax service!

[Home](#) [Contact](#) [Login](#)

2017 j2 Global Communications, Inc. All rights reserved.

## Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **02/04/14 - 09:03** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: Windows XP (x32) First connect IP: [REDACTED]

[Refresh](#) [Payment](#) [FAQ](#) [My screen](#) [Test decrypt](#)

We are present a special software - CryptoDefense Decrypter - which is allow to decrypt and return control to all your encrypted files.  
**How to buy CryptoDefense decrypter?**



**1. You should register Bitcon wallet** ([click here for more information with pictures](#))

**2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

*Here are our recommendations:*

- [REDACTED] - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- [REDACTED] - An international directory of bitcoin exchanges.
- [REDACTED] - Recommended for fast, simple service.
- [REDACTED] - Bitcoin exchange based in the United States. (Highly rated).
- [REDACTED] - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- [REDACTED] - allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.

**3. Send 1.09 BTC to Bitcoin address:** [REDACTED] [Get QR code](#)

**4. Enter the Transaction ID and select amount:**

[Clear](#)

**Note:** Transaction ID - you can find in detailed info about transaction you made.


**5. Please check the payment information and click "PAY".**

[PAY](#)

# Fake News Email

Current event – Actual “fake” news

From: NBC <[nbcnews@nbcalerts.com](mailto:nbcnews@nbcalerts.com)>  
Reply-to: NBC <[nbcnews@nbcalerts.com](mailto:nbcnews@nbcalerts.com)>  
Subject: [Breaking News: Charlottesville Driver Acquitted Immediately by Grand Jury](#)




**BREAKING NEWS:**

**James Alex Fields, who drove his car into a crowd protesting a far-right event in Charlottesville, [was acquitted by a Grand Jury this morning](#).**

The decision was announced by a representative of the Grand Jury, who stated that the incident was believed to be "accidental". Fields' act killed one person and injured many others during the controversial protest. See the video of the announcement [here](#).

[WATCH FOOTAGE OF THE CHARLOTTESVILLE INCIDENT HERE](#)




This email was sent to: [dainm@pbsinet.com](mailto:dainm@pbsinet.com)

This email was sent by:  
NBC News


[One Click Unsubscribe](#) | [Manage Your Subscription Preferences](#)

This never happened!

From: Fox News <[breakingnews@foxnewsalerts.com](mailto:breakingnews@foxnewsalerts.com)>  
Reply-to: Fox News <[breakingnews@foxnewsalerts.com](mailto:breakingnews@foxnewsalerts.com)>  
Subject: Fox News Alert: United Airlines CEO Oscar Munoz Resigns Amid Controversy



**BREAKING NEWS**  
**United Airlines CEO Oscar Munoz Resigns Amid Controversy**



United Airlines Head of Public Relations Terry Johnson announced today that United Airlines CEO Oscar Munoz resigned today amid the recent controversy where a passenger was violently dragged out of an airplane due to overbooking. He was criticized heavily for his response to the matter, blaming the victim for being disruptive and not following orders.

[Watch the announcement on FoxNews.com](#)

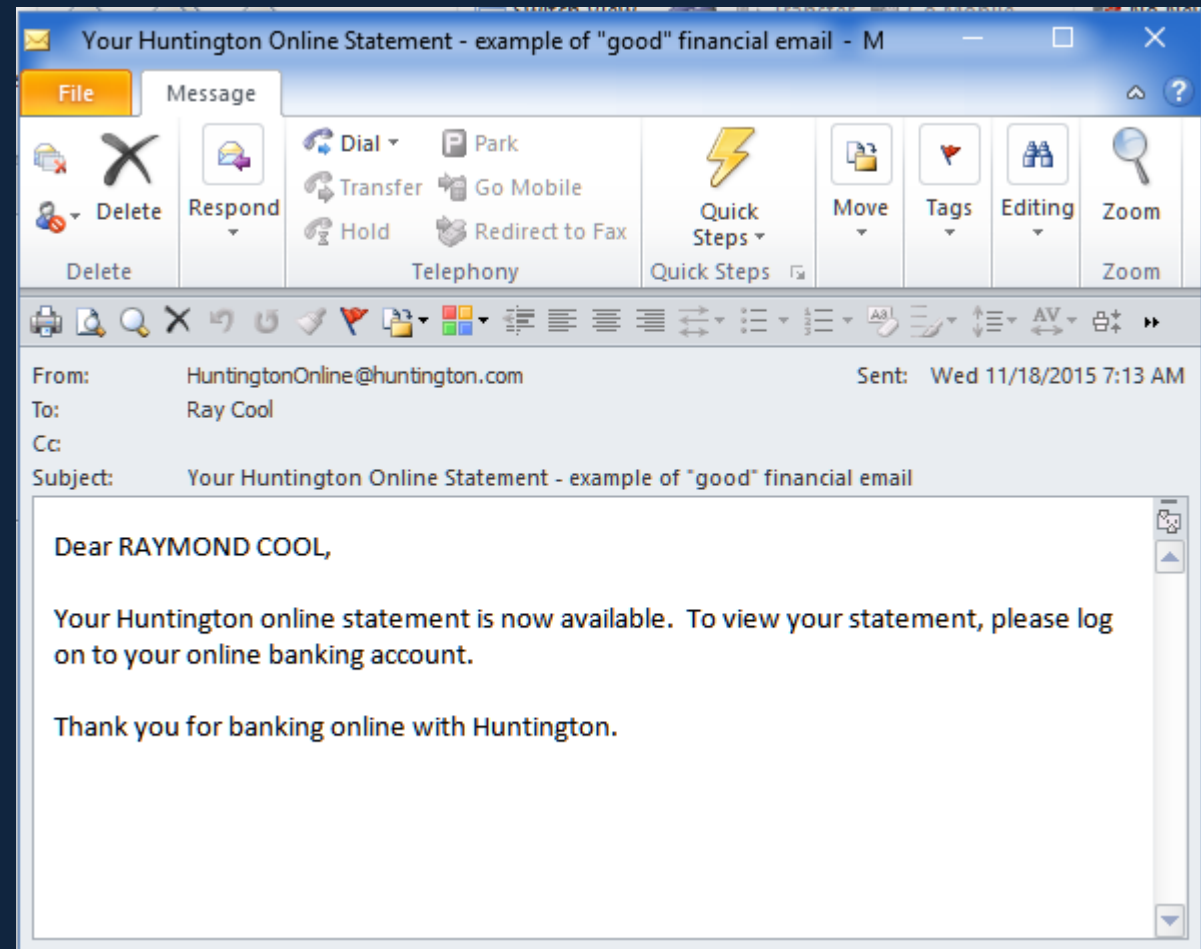
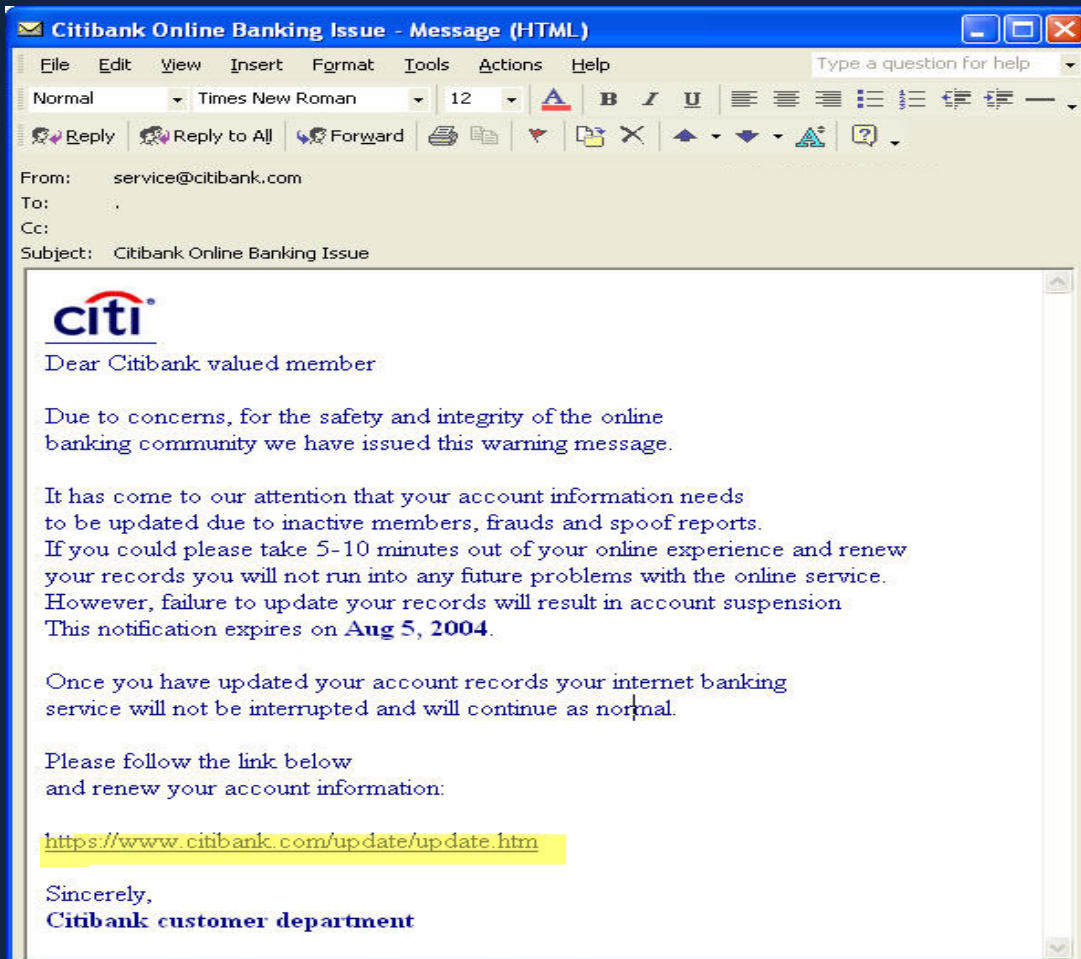
This email alert was sent to you due to your preferences. If you no longer wish to receive email alerts, please [unsubscribe here](#).



# Banking Emails

“Bad” email (Link to website)

“Good” email (Tells me to login, no link)



# Emails from Trusted Sources

## Current event donation request

From: donations@goodwill-charities.net [Send me a test email](#)  
Reply-to: donations@goodwill-charities.net  
Subject: Donate Now to Wildfire Disaster Relief Efforts



Former San Francisco Mayor Frank Jordan visits the ashes of his home off Mark West Springs Road in Sonoma County, California. He and his wife Wendy Paskin-Jordan escaped from their home nearly a week prior, during the first moments of the firestorm. (Karl Mondon/ Bay Area News Group)



Considering the extent of the damage caused by these rapid wildfires, Goodwill is ready to provide physical, emotional and spiritual care to survivors and relief workers.

Goodwill disaster teams from across the country are mobilizing and, even after disaster response efforts are over, Goodwill will remain in communities impacted by these terrible fires, supporting long-term disaster recovery efforts and providing ongoing assistance to those in need.

Make your donation now to save lives and help the community recover from these disasters. Any amount will help.

**\$5 - \$10 - \$20 - \$50 - \$100 - \$250 - \$500 - \$1000**

## Missed phone call email

From: Pbsinet@711129-1419 <[redacted]>  
Sent: Tuesday, January 19, 2021 2:41 PM  
To: Ray Cool <[redacted]>  
Subject: \*\*\*MissedCall\*\*\*

Trusted sender.



Hello [raycool@pbsinet.com](mailto:raycool@pbsinet.com),

The below details are for the received voice-message.


Receiver:	<a href="mailto:raycool@pbsinet.com">raycool@pbsinet.com</a>
Date Modified:	19/01, 2020
Caller ID:	+1 965 *** ****
Duration:	<b>00m 26s</b>
Delivery Status:	<b>Successful</b>

Play **AUDIO MESSAGE**

# Signature and Credit Emails

## eSignature request


From: dn\_notify@sign-docusign.net [Send me a test email](#)  
Reply-to: dn\_notify@sign-docusign.net [Toggle red flags](#)  
Subject: A document for PBSI Positive Business Solutions to sign



Ben Hubbard sent you a document to review and sign.

[REVIEW DOCUMENT](#)

**Ben Hubbard**  
An envelope for signature for PBSI Positive Business Solutions

Powered by 

**Do Not Share This Email**  
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.


**Alternate Signing Method**  
Visit DocuSign.com, click 'Access Documents', and enter the security code:  
91A30983D57C4B3F97B19B56A5AFBCB92

**About Docu Sign**

## “Fix” your credit

Email Preview - Dain: Urgent Notice about Your Credit Score ✕

From: notifications@creditkar.ma [Send me a test email](#)  
Reply-to: notifications@creditkar.ma [Toggle red flags](#)  
Subject: Dain: Urgent Notice about Your Credit Score





Dain — your credit score was lowered.

Your credit score was lowered. Review your account now to ensure reports are accurate.

[See My New Scores](#)

We'll see you there  
**The Credit Karma Team**

---



To manage your Credit Karma emails, please go to your [Communication & Monitoring Preferences](#)

[Privacy Policy](#) [Terms of Use](#) [Unsubscribe](#)

Note: Never share your online banking or Credit Karma passwords with anyone, including us!

This message was sent to dainm@pbsinet.com. To manage the kinds of email you receive from Credit Karma, [click here](#).  
If you no longer wish to receive any emails from Credit Karma, [click here](#).

# Email Security Practices Summary

## Email Security Principles

- Email safety principle # 1 - Unsolicited vs. Solicited
- Email safety principle # 2 - Antenna up! – Do you need to click on this now?
- Email safety principle # 3 - Don't get your news from email
- Email safety principle # 4 - Careful with Unsubscribe
- Email safety principle # 5 - Learn how to evaluate URL for danger

## Email Security Settings

- Turn on Multifactor Authentication on your email – and anywhere available (bank apps, investment logins)
- M365 – Implement MS Defender for Office 365 (formerly ATP) – “click” protection - \$2/mo
- When in doubt – STOP – go to vendor web site directly



# Overall Summary - Essentials of Securing Personal Information

## 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
- Review important files – Decide which files should be encrypted at rest
- Automate Your Backup – - multi-location, locally encrypted, redundant

## Email Security

- 5 principles: Solicited/Unsolicited; Careful with emails that are unusual, contain breaking news, or prompt for passwords or data
- Turn on Multifactor Authentication
- Encrypt files with important personal information (PII or PHI) during transmission

## 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 are safe

- 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 Handouts

“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

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 (800) 626-2306 [itservices@pbsinet.com](mailto:itservices@pbsinet.com)
- Speaker contact Ray Cool, CEO (513) 924-3915 [rayc@pbsinet.com](mailto:rayc@pbsinet.com)

## Upcoming Webinars

- Securing Personal Information available on Foster & Motley website
- **Email Security Practices** **today's topic**
- Password Management – Practical Strategies Tuesday, Feb 16, 1:00
- File Encryption, Cloud Security & Public Wi-Fi Thursday, Feb 18, 1:00