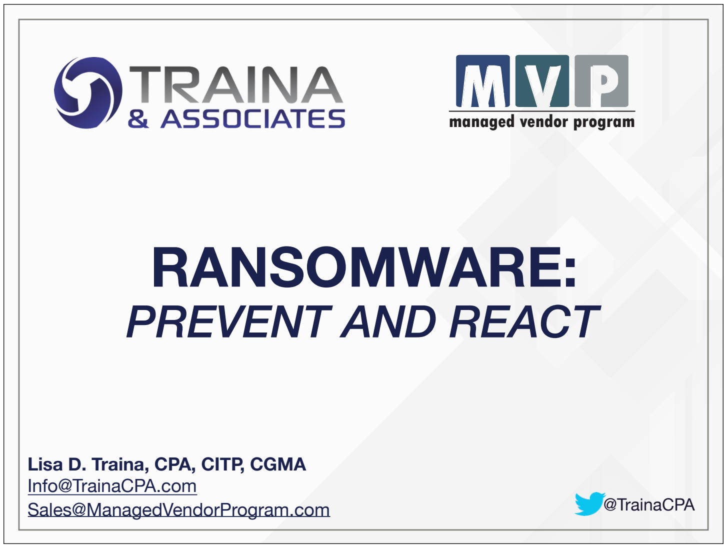


TRAINA & ASSOCIATES

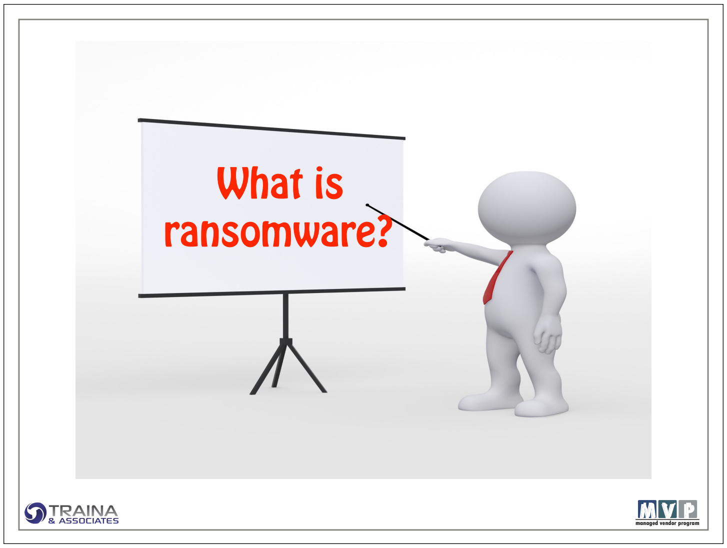
MVP managed vendor program

RANSOMWARE:

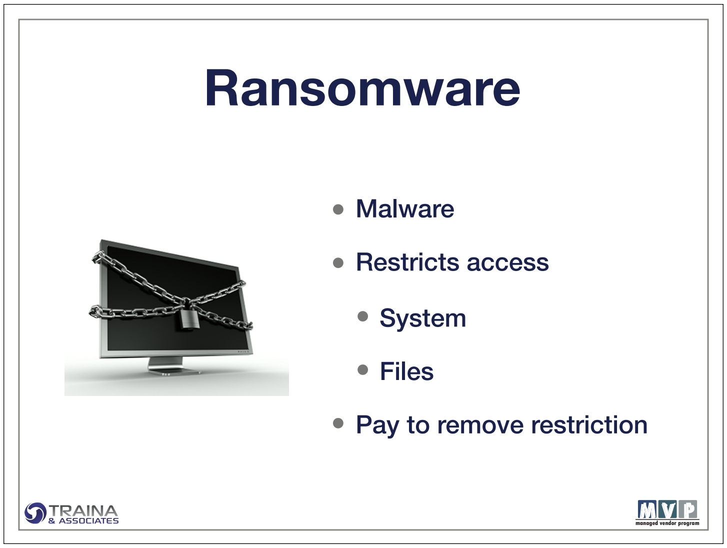
PREVENT AND REACT

Lisa D. Traina, CPA, CITP, CGMA
Info@TrainaCPA.com
Sales@ManagedVendorProgram.com

@TrainaCPA



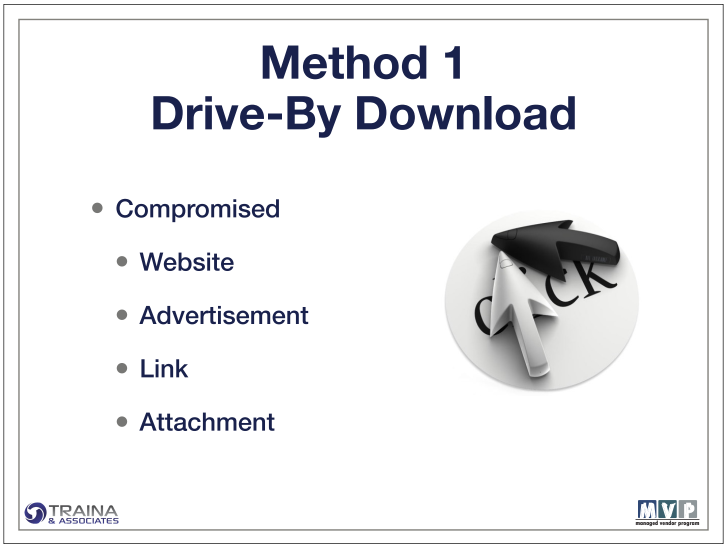
What is ransomware?



Ransomware

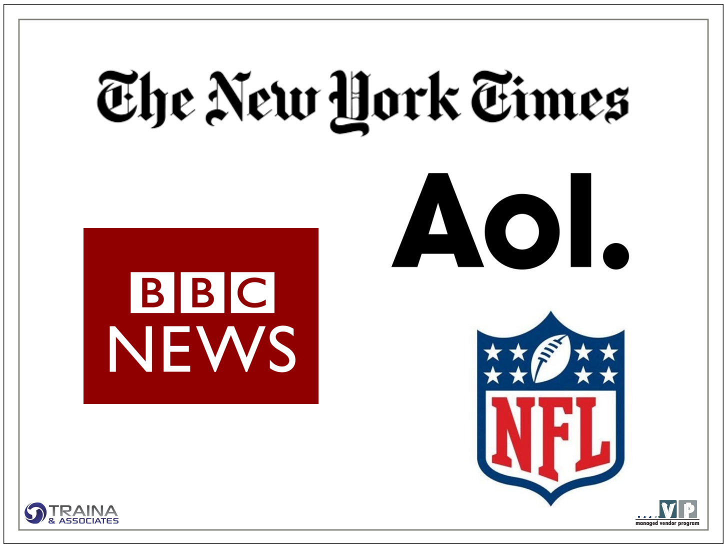
- Malware
- Restricts access
  - System
  - Files
- Pay to remove restriction

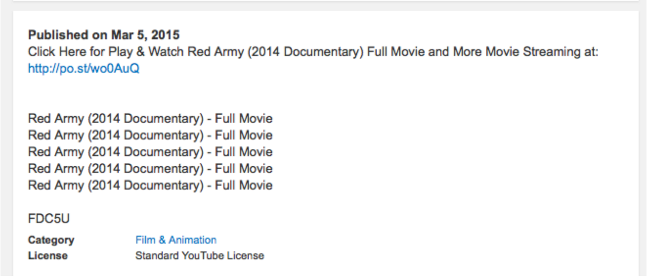
How?



Method 1
Drive-By Download

- Compromised
  - Website
  - Advertisement
  - Link
  - Attachment



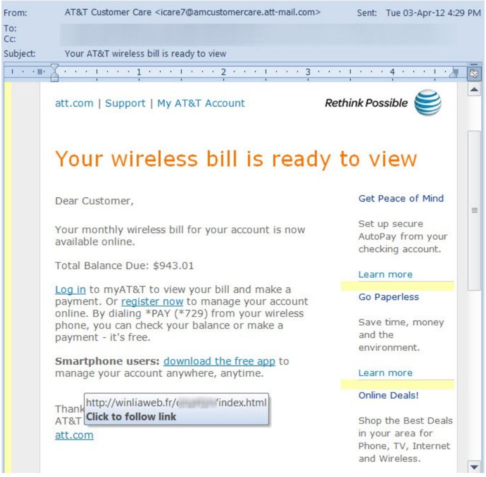


Published on Mar 5, 2015
Click Here for Play & Watch Red Army (2014 Documentary) Full Movie and More Movie Streaming at:
http://po.st/wo0AuQ

Red Army (2014 Documentary) - Full Movie
Red Army (2014 Documentary) - Full Movie
Red Army (2014 Documentary) - Full Movie
Red Army (2014 Documentary) - Full Movie
Red Army (2014 Documentary) - Full Movie

FDC5U

Category	Film & Animation
License	Standard YouTube License



From: AT&T Customer Care <icare7@amcustomercare.att-mail.com> Sent: Tue 03-Apr-12 4:29 PM
To: [redacted]
Cc:
Subject: Your AT&T wireless bill is ready to view

att.com | Support | My AT&T Account

Rethink Possible

Your wireless bill is ready to view

Dear Customer,

Your monthly wireless bill for your account is now available online.

Total Balance Due: $943.01

Log in to myAT&T to view your bill and make a payment. Or register now to manage your account online. By dialing *PAY (*729) from your wireless phone, you can check your balance or make a payment - it's free.

Smartphone users: download the free app to manage your account anywhere, anytime.

Thank
AT&T
att.com

http://winliaweb.fr/[redacted]/index.html
Click to follow link

Get Peace of Mind

Set up secure AutoPay from your checking account.

Learn more

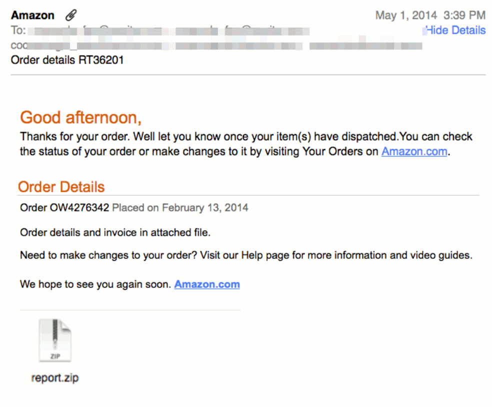
Go Paperless

Save time, money and the environment.

Learn more

Online Deals!

Shop the Best Deals in your area for Phone, TV, Internet and Wireless.



Amazon May 1, 2014 3:39 PM
To: [redacted] Hide Details
[redacted]
Order details RT36201

Good afternoon,
Thanks for your order. Well let you know once your item(s) have dispatched.You can check the status of your order or make changes to it by visiting Your Orders on Amazon.com.

Order Details

Order OW4276342 Placed on February 13, 2014

Order details and invoice in attached file.

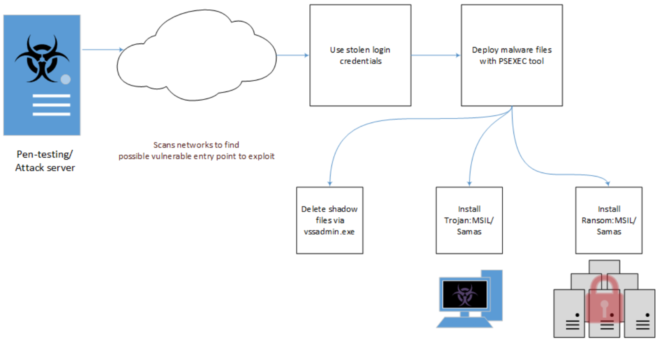
Need to make changes to your order? Visit our Help page for more information and video guides.

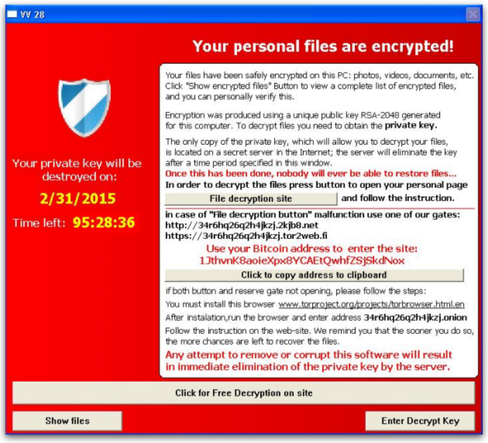
We hope to see you again soon. **Amazon.com**

report.zip

Method 2
Vulnerability Exploitation

- Exploits system vulnerability
- Uses other vectors (stolen credentials)
- Targeted attack


Pen-testing/
Attack server
Scans networks to find
possible vulnerable entry point to exploit
Use stolen login credentials
Deploy malware files with PSEXEC tool
Delete shadow files via vssadmin.exe
Install Trojan:MSIL/ Samas
Install Ransom:MSIL/ Samas



Your personal files are encrypted!

Your private key will be destroyed on:

2/31/2015

Time left: 95:28:36

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site **and follow the instruction.**

in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.2kjb8.net
https://34r6hq26q2h4jkzj.tor2web.fi

Use your Bitcoin address to enter the site:
1JthvnK8aoieXpx8YCAEtQwhfZSjSkdNox

Click to copy address to clipboard

If both button and reserve gate not opening, please follow the steps:

You must install this browser www.torproject.org/projects/torbrowser.html.en

After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**

Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Method 3
???

- Ransomware is evolving
- Trojans are most popular form
- Future of ransomware
  - Self-propagating ransomware (cryptoworms)

Damage

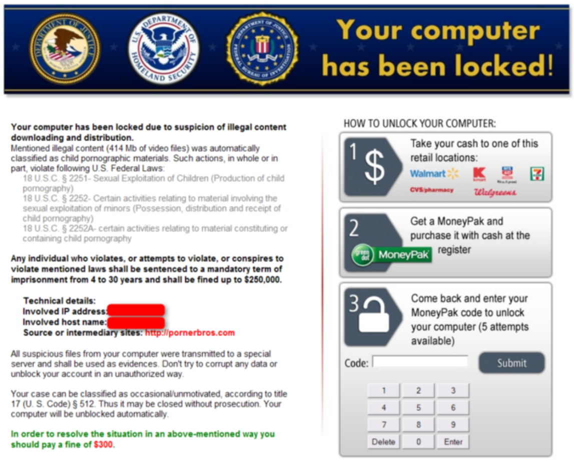
Ransomware Damage

- Prevent system acces
- Encrypt files
  - Local hard drive
  - Mapped drive
  - Unmapped drive
- Deletes files
- Detects AND deletes backup files
- Threatens data dump

Assets at Risk

- Workstations
- Servers
- Laptops
- Mobile devices
- External hard drives
- USB removable media
- SAN/NAS
- Cloud storage

Prevents System Access



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

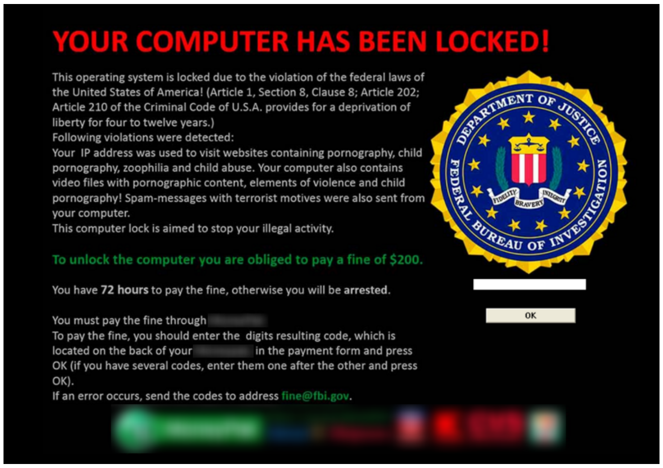
In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)



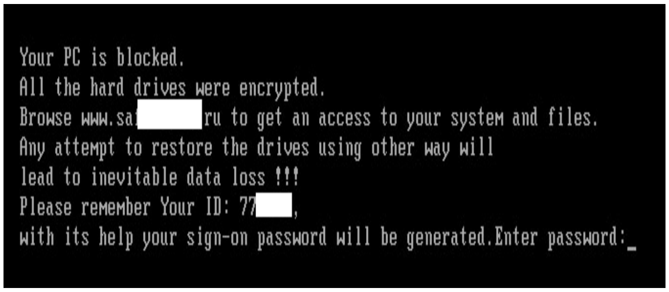
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

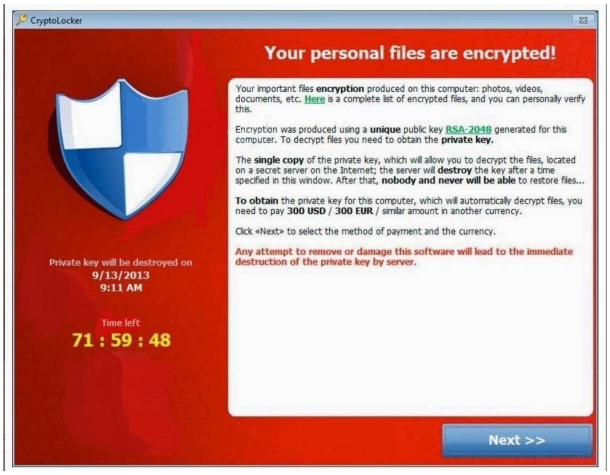


```
Your PC is blocked.
All the hard drives were encrypted.
Browse www.sa[redacted]ru to get an access to your system and files.
Any attempt to restore the drives using other way will
lead to inevitable data loss !!!
Please remember Your ID: 77[redacted],
with its help your sign-on password will be generated.Enter password:_
```

Encrypts Files

File Examples

- Searches for predetermined file extensions
  - Microsoft office files
  - Database files
  - PDF
  - Text documents
  - Backup files (volume snapshot service)
  - Bitcoin wallet (wallet.dat)



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

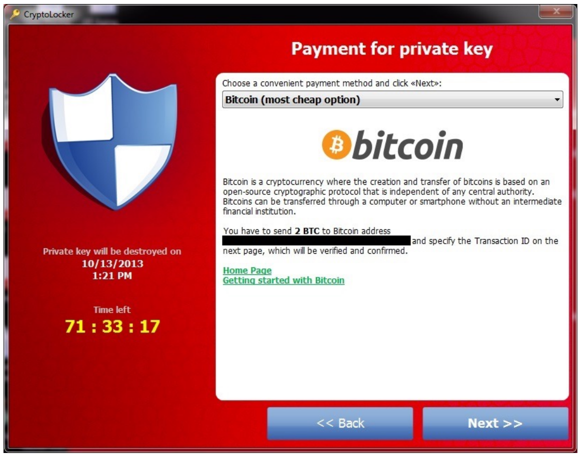
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
9:11 AM

Time left
71 : 59 : 48



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option) ▾

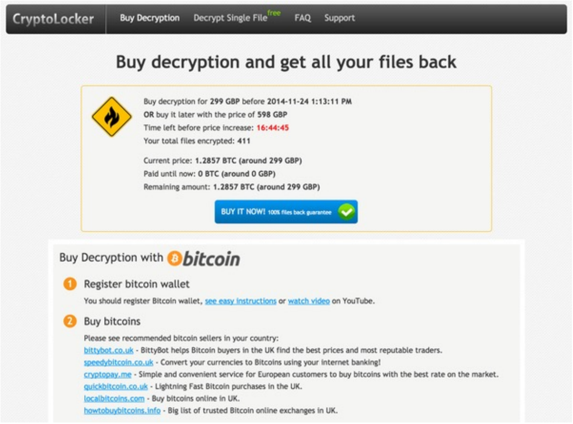
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17



CryptoLocker | Buy Decryption | Decrypt Single File free | FAQ | Support

Buy decryption and get all your files back

Buy decryption for **299 GBP** before **2014-11-24 1:13:11 PM**
OR buy it later with the price of **598 GBP**
Time left before price increase: **16:44:45**
Your total files encrypted: **411**

Current price: **1.2857 BTC (around 299 GBP)**
Paid until now: **0 BTC (around 0 GBP)**
Remaining amount: **1.2857 BTC (around 299 GBP)**

BUY IT NOW! 100% files back guarantee

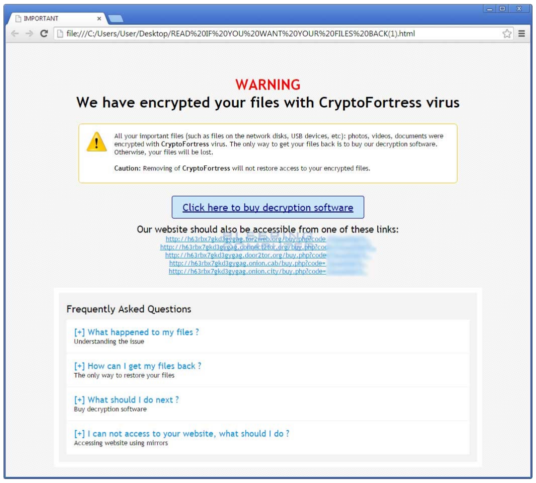
Buy Decryption with bitcoin

1. Register bitcoin wallet

   You should register Bitcoin wallet, see easy instructions or watch video on YouTube.

2. Buy bitcoins

   Please see recommended bitcoin sellers in your country:
   bittybot.co.uk - BittyBot helps Bitcoin buyers in the UK find the best prices and most reputable traders.
   speedybitcoin.co.uk - Convert your currencies to Bitcoins using your internet banking!
   cryptopay.me - Simple and convenient service for European customers to buy bitcoins with the best rate on the market.
   quickbitcoin.co.uk - Lightning Fast Bitcoin purchases in the UK.
   localbitcoins.com - Buy bitcoins online in UK.
   howtobuybitcoins.info - Big list of trusted Bitcoin online exchanges in UK.



IMPORTANT

file:///C:/Users/User/Desktop/READ%20IF%20YOU%20WANT%20YOUR%20FILES%20BACK(1).html

WARNING
We have encrypted your files with CryptoFortress virus

All your important files (such as files on the network disks, USB devices, etc): photos, videos, documents were encrypted with **CryptoFortress** virus. The only way to get your files back is to buy our decryption software. Otherwise, your files will be lost.

Caution: Removing of **CryptoFortress** will not restore access to your encrypted files.

Click here to buy decryption software

Our website should also be accessible from one of these links:
http://h63rbx7gkd3gygag.tor2web.org/buy.php?code
http://h63rbx7gkd3gygag.connect2tor.org/buy.php?coc
http://h63rbx7gkd3gygag.door2tor.org/buy.php?code
http://h63rbx7gkd3gygag.onion.cab/buy.php?code=
http://h63rbx7gkd3gygag.onion.city/buy.php?code=
[redacted]

Frequently Asked Questions

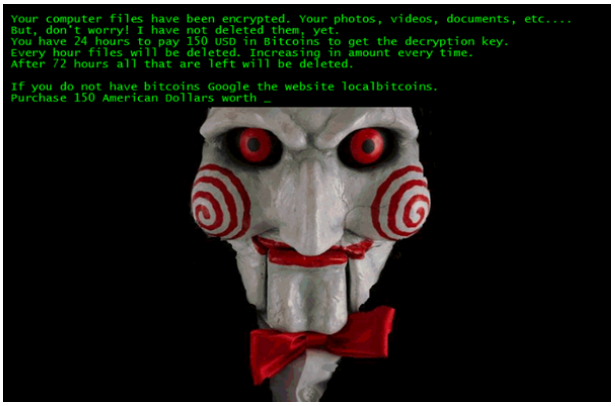
[+] What happened to my files ?
Understanding the issue

[+] How can I get my files back ?
The only way to restore your files

[+] What should I do next ?
Buy decryption software

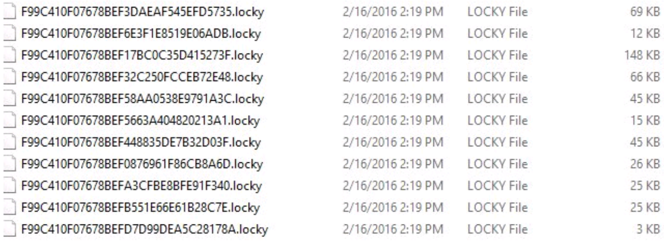
[+] I can not access to your website, what should I do ?
Accessing website using mirrors

Deletes Files



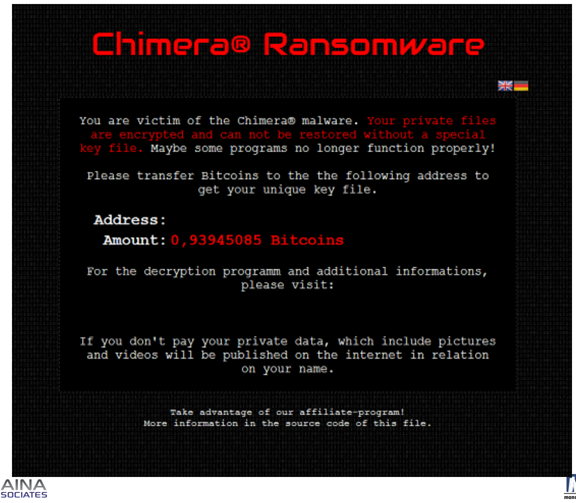
```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth _
```

Detects and deletes backup files



F99C410F07678BEF3DAEAF545EFD5735.locky	2/16/2016 2:19 PM	LOCKY File	69 KB
F99C410F07678BEF6E3F1E8519E06ADB.locky	2/16/2016 2:19 PM	LOCKY File	12 KB
F99C410F07678BEF17BC0C35D415273F.locky	2/16/2016 2:19 PM	LOCKY File	148 KB
F99C410F07678BEF32C250FCCEB72E48.locky	2/16/2016 2:19 PM	LOCKY File	66 KB
F99C410F07678BEF58AA0538E9791A3C.locky	2/16/2016 2:19 PM	LOCKY File	45 KB
F99C410F07678BEF5663A404820213A1.locky	2/16/2016 2:19 PM	LOCKY File	15 KB
F99C410F07678BEF448835DE7B32D03F.locky	2/16/2016 2:19 PM	LOCKY File	45 KB
F99C410F07678BEF0876961F86CB8A6D.locky	2/16/2016 2:19 PM	LOCKY File	26 KB
F99C410F07678BEFA3CFBE8BFE91F340.locky	2/16/2016 2:19 PM	LOCKY File	25 KB
F99C410F07678BEFB551E66E61B28C7E.locky	2/16/2016 2:19 PM	LOCKY File	25 KB
F99C410F07678BEFD7D99DEA5C28178A.locky	2/16/2016 2:19 PM	LOCKY File	3 KB

Threatens Data Dump



Chimera® Ransomware

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

Address:

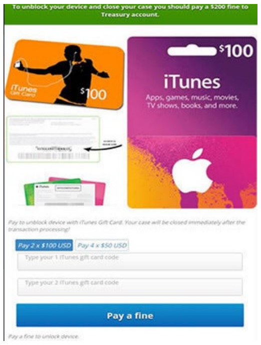
Amount: 0,93945085 Bitcoins

For the decryption programm and additional informations, please visit:

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!
More information in the source code of this file.

Pay Up!


To unblock your device and close your case you should pay a $200 fine to Treasury account.

Pay to unblock device with iTunes Gift Card. Your case will be closed immediately after the transaction processing!

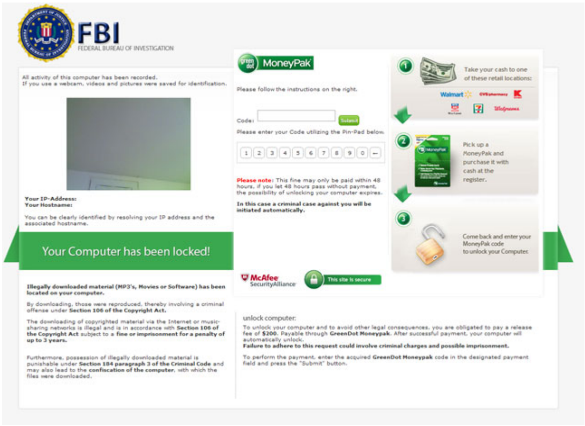
Pay 2 x $100 USD | Pay 4 x $50 USD

Type your 1 iTunes gift card code

Type your 2 iTunes gift card code

Pay a fine

Pay a fine to unlock device.



All activity of this computer has been recorded.
If you use a webcam, videos and pictures were saved for identification.

Your IP-Address:
Your Hostname:

You can be clearly identified by resolving your IP address and the associated hostname.

Your Computer has been locked!

Illegally downloaded material (MP3's, Movies or Software) has been located on your computer.

By downloading, those were reproduced, thereby involving a criminal offense under **Section 106 of the Copyright Act.**

The downloading of copyrighted material via the Internet or music-sharing networks is illegal and is in accordance with **Section 106 of the Copyright Act** subject to a **fine or imprisonment for a penalty of up to 3 years.**

Furthermore, possession of illegally downloaded material is punishable under **Section 184 paragraph 3 of the Criminal Code** and may also lead to the **confiscation of the computer**, with which the files were downloaded.

Please follow the instructions on the right.

Code: Submit

Please enter your Code utilizing the Pin-Pad below.

1 2 3 4 5 6 7 8 9 0 ←

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

1 Take your cash to one of these retail locations:

2 Pick up a MoneyPak and purchase it with cash at the register.

3 Come back and enter your MoneyPak code to unlock your Computer.

unlock computer:

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **$200**. Payable through **GreenDot Moneypak**. After successful payment, your computer will automatically unlock.
Failure to adhere to this request could involve criminal charges and possible imprisonment.

To perform the payment, enter the acquired **GreenDot Moneypak** code in the designated payment field and press the "Submit" button.

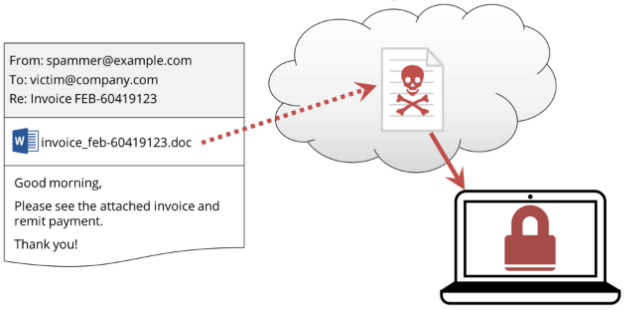
Common Strains

- Petya
- DMA Locker
- PowerWare
- Locky
- MSIL/Samas
- CryptoWall
- TorrentLocker
- Maktub
- TeslaCrypt
- Jigsaw
- Surprise
- Keranger

Common Strains

- New strains continuing to be released
- Ransom-as-a-service (Raas)
  - Download ransomware app builder
  - Customize accordingly
  - Examples: Sarento and Enrume

Fake Invoice Email Installs Locky Ransomware



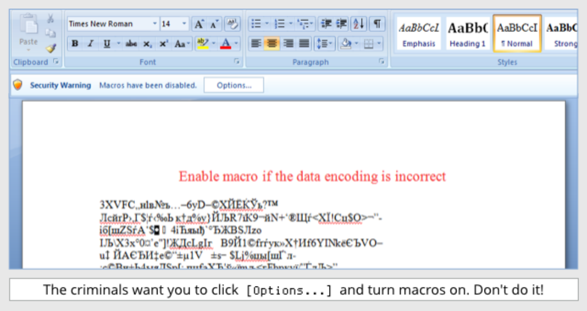
From: spammer@example.com
To: victim@company.com
Re: Invoice FEB-60419123

invoice_feb-60419123.doc

Good morning,

Please see the attached invoice and remit payment.

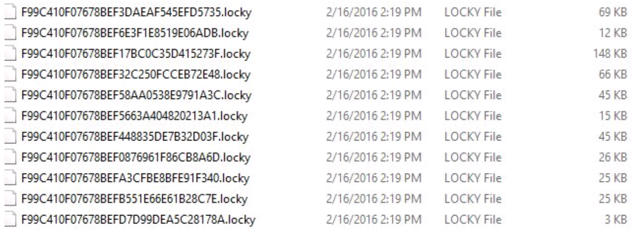
Thank you!



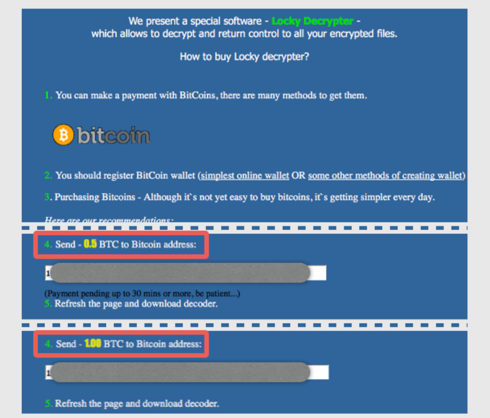
Enable macro if the data encoding is incorrect

3XVFC„нlвNъ…–6yD–©ХЙЁКЎъ?™
ЛсйrР›Г$¦ѓ‹%oЬ к†д%у}ЙЉR7іК9¬йN+'®Щѓ<XЇ!Cu$O>–"-
іб[шZSѓA`$ 4iЋяыђ`°ЪЖBSЛzo
IЉ\X3x°0¤'e"]!ЖДcLgIr B9Й1©frѓyк»X†Иf6YINkёЄЪVO–
u‡ ЙАЄЪИ‡e©"±µ1V ±s– $Lj%шы[шГ`л-

The criminals want you to click `[Options...]` and turn macros on. Don't do it!



```
F99C410F07678BEF3DAEAF545EFD5735.locky    2/16/2016 2:19 PM    LOCKY File     69 KB
F99C410F07678BEF6E3F1E8519E06ADB.locky    2/16/2016 2:19 PM    LOCKY File     12 KB
F99C410F07678BEF17BC0C35D415273F.locky    2/16/2016 2:19 PM    LOCKY File    148 KB
F99C410F07678BEF32C250FCCEB72E48.locky    2/16/2016 2:19 PM    LOCKY File     66 KB
F99C410F07678BEF58AA0538E9791A3C.locky    2/16/2016 2:19 PM    LOCKY File     45 KB
F99C410F07678BEF5663A404820213A1.locky    2/16/2016 2:19 PM    LOCKY File     15 KB
F99C410F07678BEF448835DE7B32D03F.locky    2/16/2016 2:19 PM    LOCKY File     45 KB
F99C410F07678BEF0876961F86CB8A6D.locky    2/16/2016 2:19 PM    LOCKY File     26 KB
F99C410F07678BEFA3CFBE8BFE91F340.locky    2/16/2016 2:19 PM    LOCKY File     25 KB
F99C410F07678BEFB551E66E61B28C7E.locky    2/16/2016 2:19 PM    LOCKY File     25 KB
F99C410F07678BEFD7D99DEA5C28178A.locky    2/16/2016 2:19 PM    LOCKY File      3 KB
```



We present a special software - Locky Decrypter -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)

3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

4. Send - 0.5 BTC to Bitcoin address:

[redacted]

(Payment pending up to 30 mins or more, be patient...)
5. Refresh the page and download decoder.

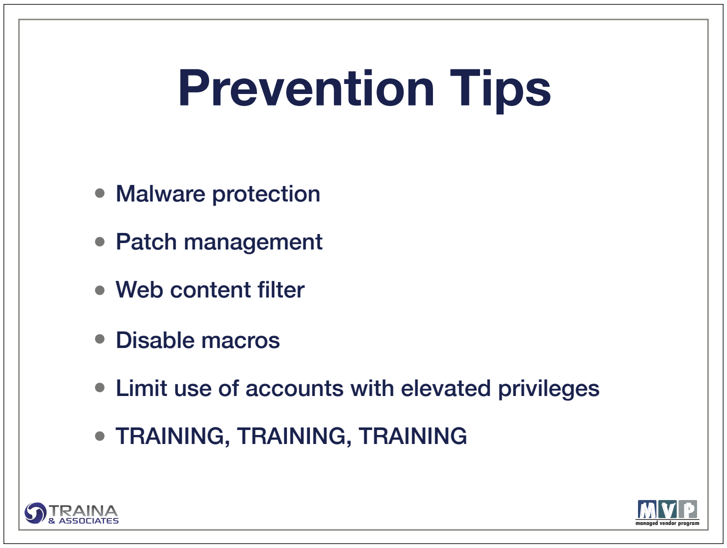
4. Send - 1.00 BTC to Bitcoin address:

[redacted]

5. Refresh the page and download decoder.

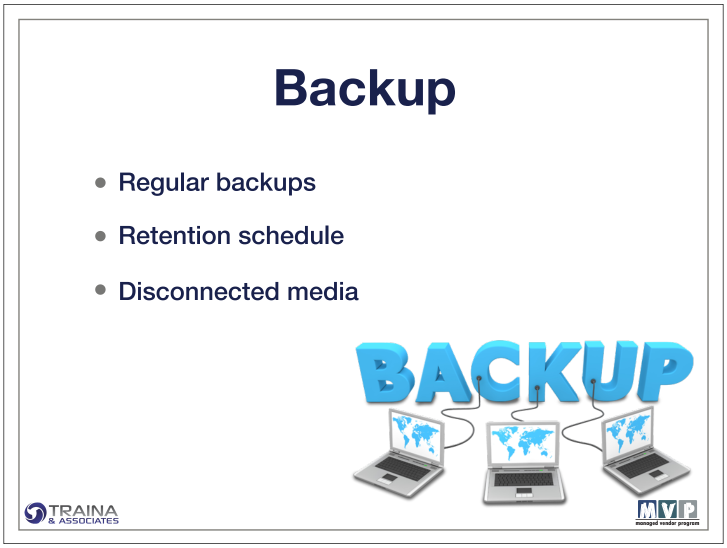
Different ransom demands by "Locky" at different times

Prevention
Reaction



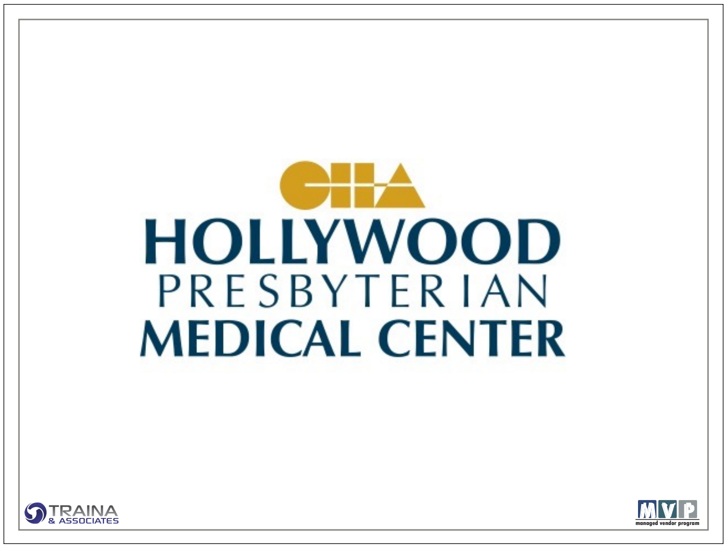
Prevention Tips

- Malware protection
- Patch management
- Web content filter
- Disable macros
- Limit use of accounts with elevated privileges
- TRAINING, TRAINING, TRAINING



Backup

- Regular backups
- Retention schedule
- Disconnected media



HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER

MedStar Health

Ransomware Victims

STEP 1

Unplug infected system/ contain the problem

STEP 2

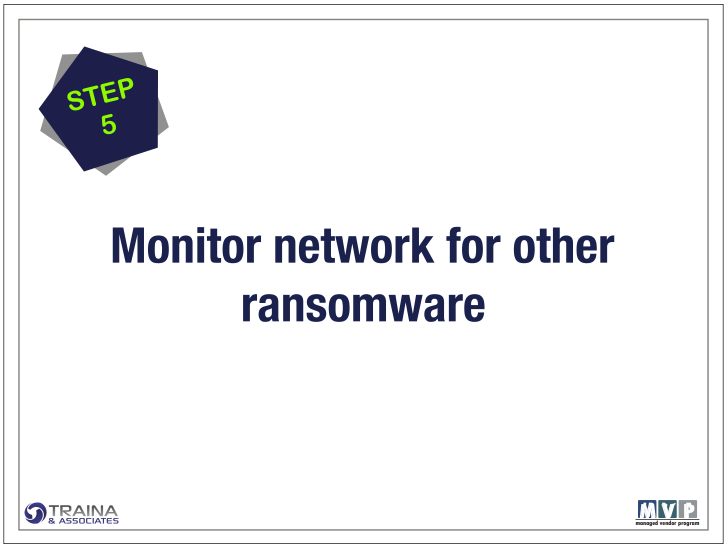
Report to law enforcement

STEP 3

Restore data from backup

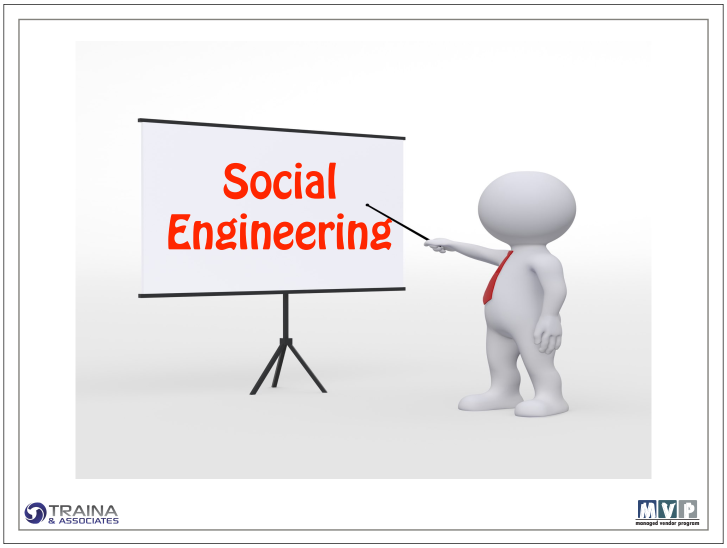
STEP 4

Pay ransom?



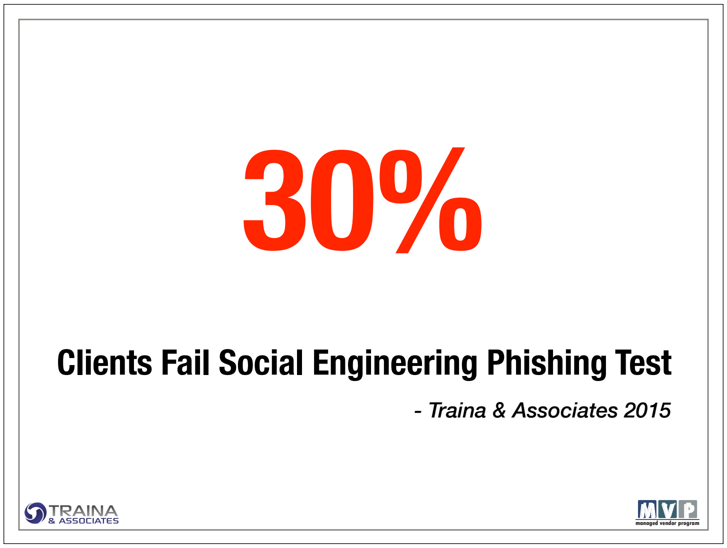
STEP 5

Monitor network for other ransomware



Social Engineering

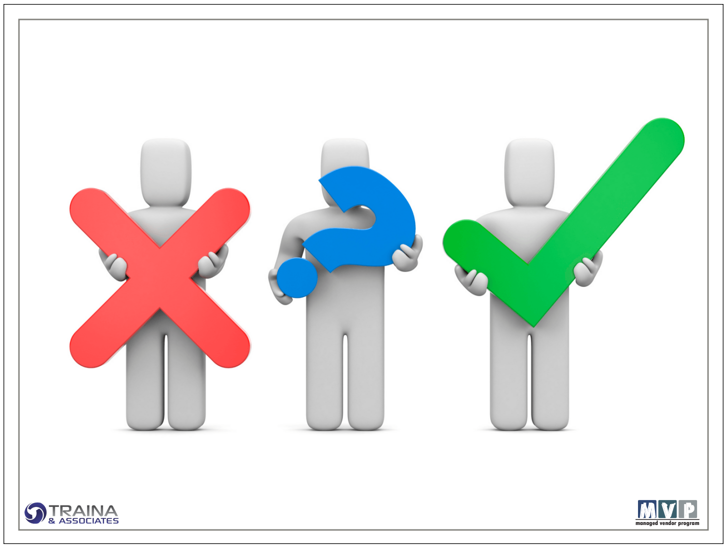
test

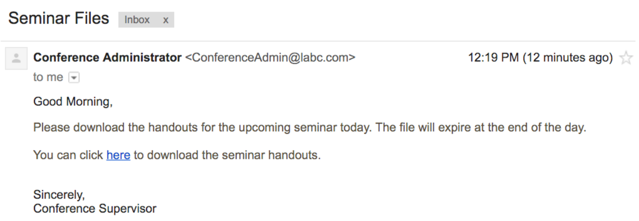


30%

Clients Fail Social Engineering Phishing Test

- Traina & Associates 2015





Seminar Files

Conference Administrator <ConferenceAdmin@labc.com>   12:19 PM (12 minutes ago)

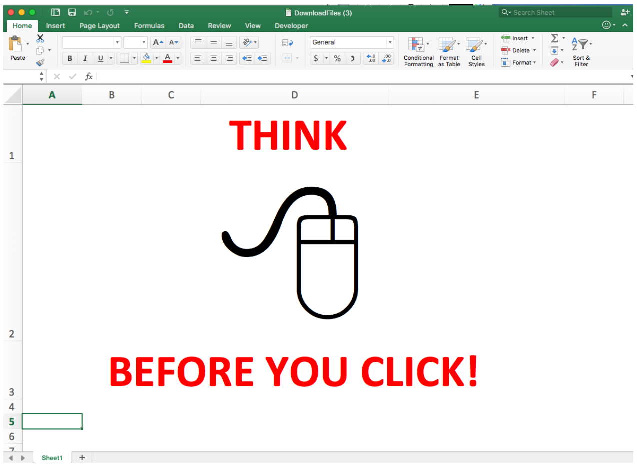
to me

Good Morning,

Please download the handouts for the upcoming seminar today. The file will expire at the end of the day.

You can click here to download the seminar handouts.

Sincerely,
Conference Supervisor



THINK

BEFORE YOU CLICK!

Audit

- IT Security Review
- Vulnerability/Penetration Testing
- HIPAA/Meaningful Use
- TR-39 Audit
- ACH Audit

Consulting

- IT Policy Creation
- IS Risk Assessment
- Disaster Recovery Planning
- Product Implementation Review
- IS Staffing Assessment

Training

- Cybersecurity
- Strategic Technology Planning
- Corporate Account Takeover
- Cloud Computing
- Mobile Device Security

Managed Vendor Program

- New Vendor/Annual Due Diligence
- Document Collection
- Assessment of Information
- Thorough Vendor Reports
- Concise Executive Summary

Ensuring data security since 1999

www.TrainaCPA.com   (225) 308-1712   Info@TrainaCPA.com

TRAINA
& ASSOCIATES

MVP
managed vendor program

Lisa D. Traina, CPA, CITP, CGMA
Info@TrainaCPA.com
Sales@ManagedVendorProgram.com

@TrainaCPA

Images courtesy of FreeDigitalPhotos.net