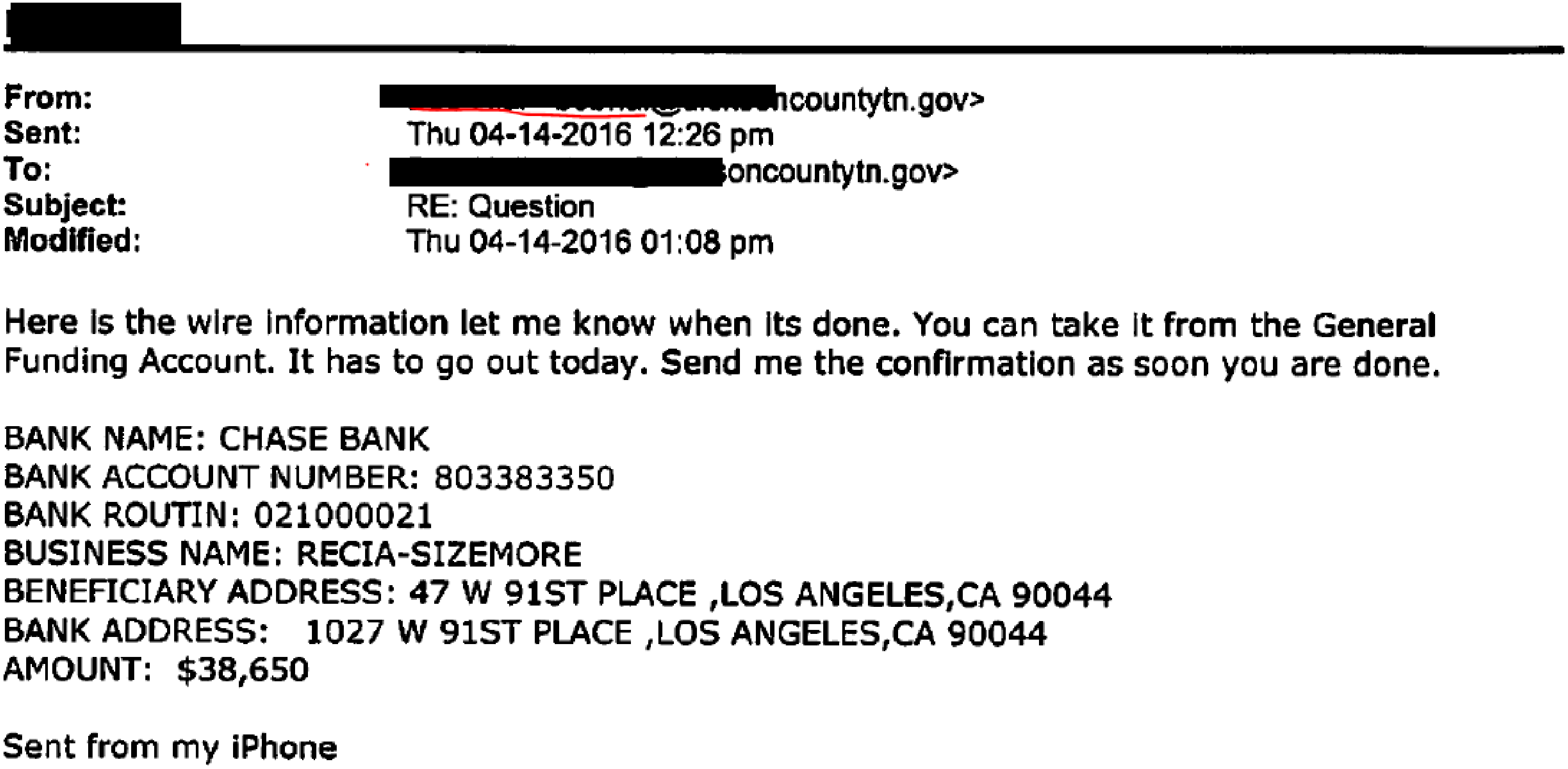
Tennessee Comptroller of the Treasury

Information Systems Audits

Penny Austin, Assistant Director - IS
Greg Brush, IS Auditor
Division of Local Government Audit

Phishing
@
Shift

Phishing Example



[redacted]

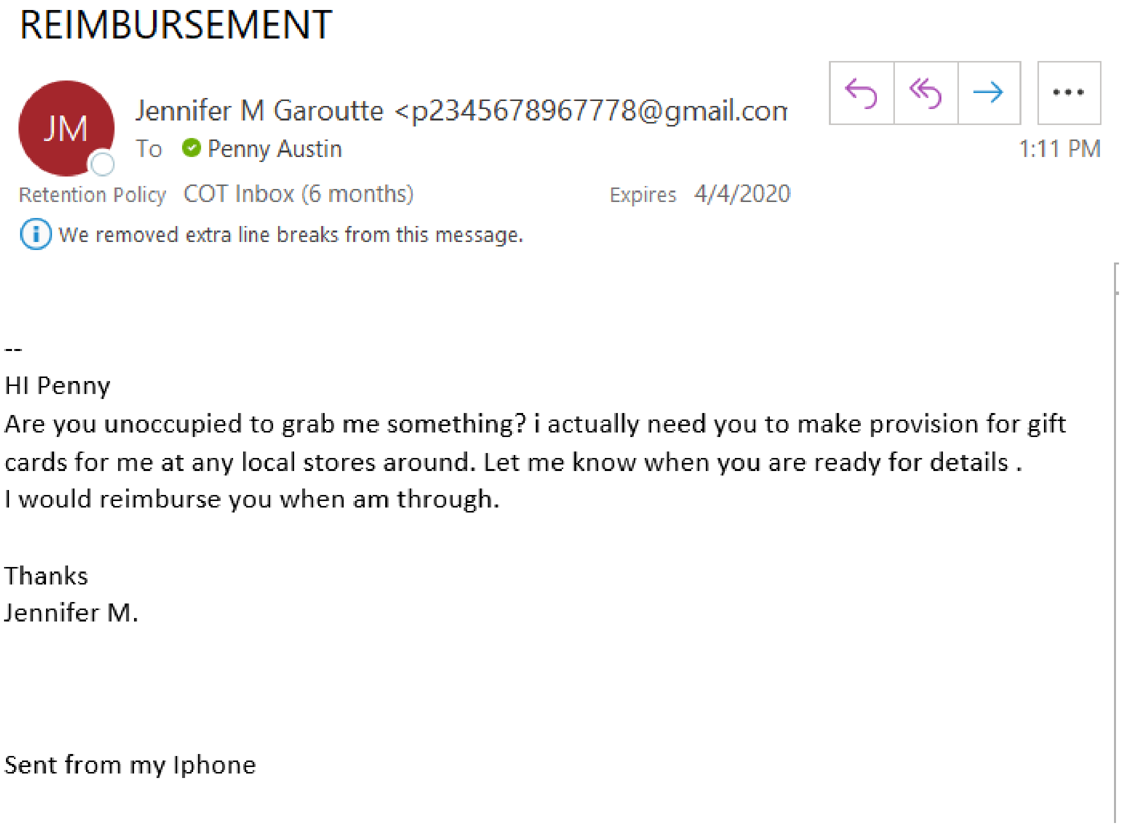
From: [redacted]ncountytn.gov>
Sent: Thu 04-14-2016 12:26 pm
To: [redacted]oncountytn.gov>
Subject: RE: Question
Modified: Thu 04-14-2016 01:08 pm

Here is the wire information let me know when its done. You can take it from the General Funding Account. It has to go out today. Send me the confirmation as soon you are done.

BANK NAME: CHASE BANK
BANK ACCOUNT NUMBER: 803383350
BANK ROUTIN: 021000021
BUSINESS NAME: RECIA-SIZEMORE
BENEFICIARY ADDRESS: 47 W 91ST PLACE ,LOS ANGELES,CA 90044
BANK ADDRESS: 1027 W 91ST PLACE ,LOS ANGELES,CA 90044
AMOUNT: $38,650

Sent from my iPhone

Phishing Example



REIMBURSEMENT

Jennifer M Garoutte <p2345678967778@gmail.con

To Penny Austin

1:11 PM

Retention Policy COT Inbox (6 months) Expires 4/4/2020

We removed extra line breaks from this message.

--

HI Penny

Are you unoccupied to grab me something? i actually need you to make provision for gift cards for me at any local stores around. Let me know when you are ready for details .

I would reimburse you when am through.

Thanks

Jennifer M.

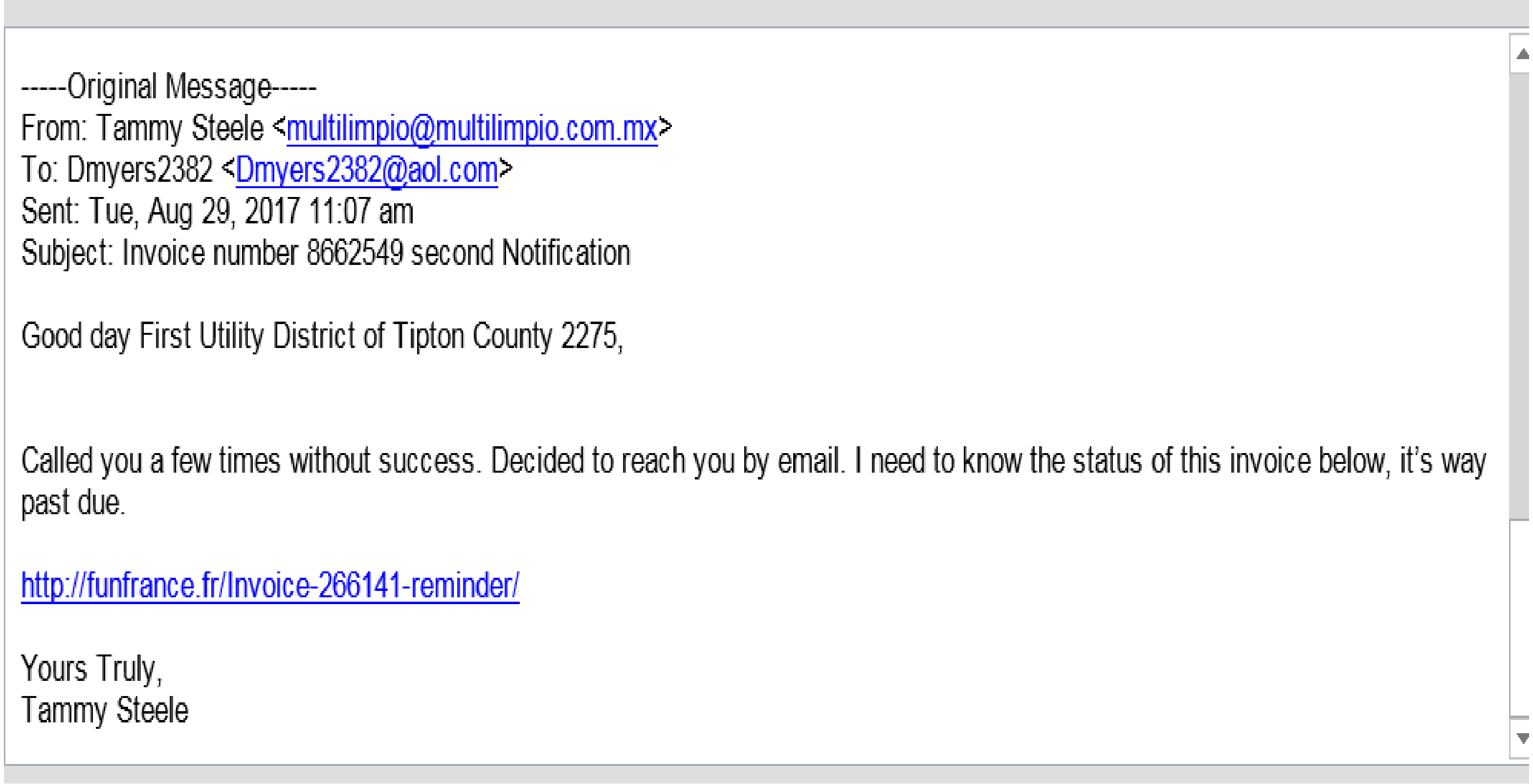
Sent from my Iphone

DIRECT DEPOSIT CONFIRMATION

Current	Year to Date
$659.16	$3,954.96

Description	
TAXABLE	$659.1
NET PAYMENT	$595.5

payment has been direct deposited to your account



-----Original Message-----
From: Tammy Steele <multilimpio@multilimpio.com.mx>
To: Dmyers2382 <Dmyers2382@aol.com>
Sent: Tue, Aug 29, 2017 11:07 am
Subject: Invoice number 8662549 second Notification

Good day First Utility District of Tipton County 2275,

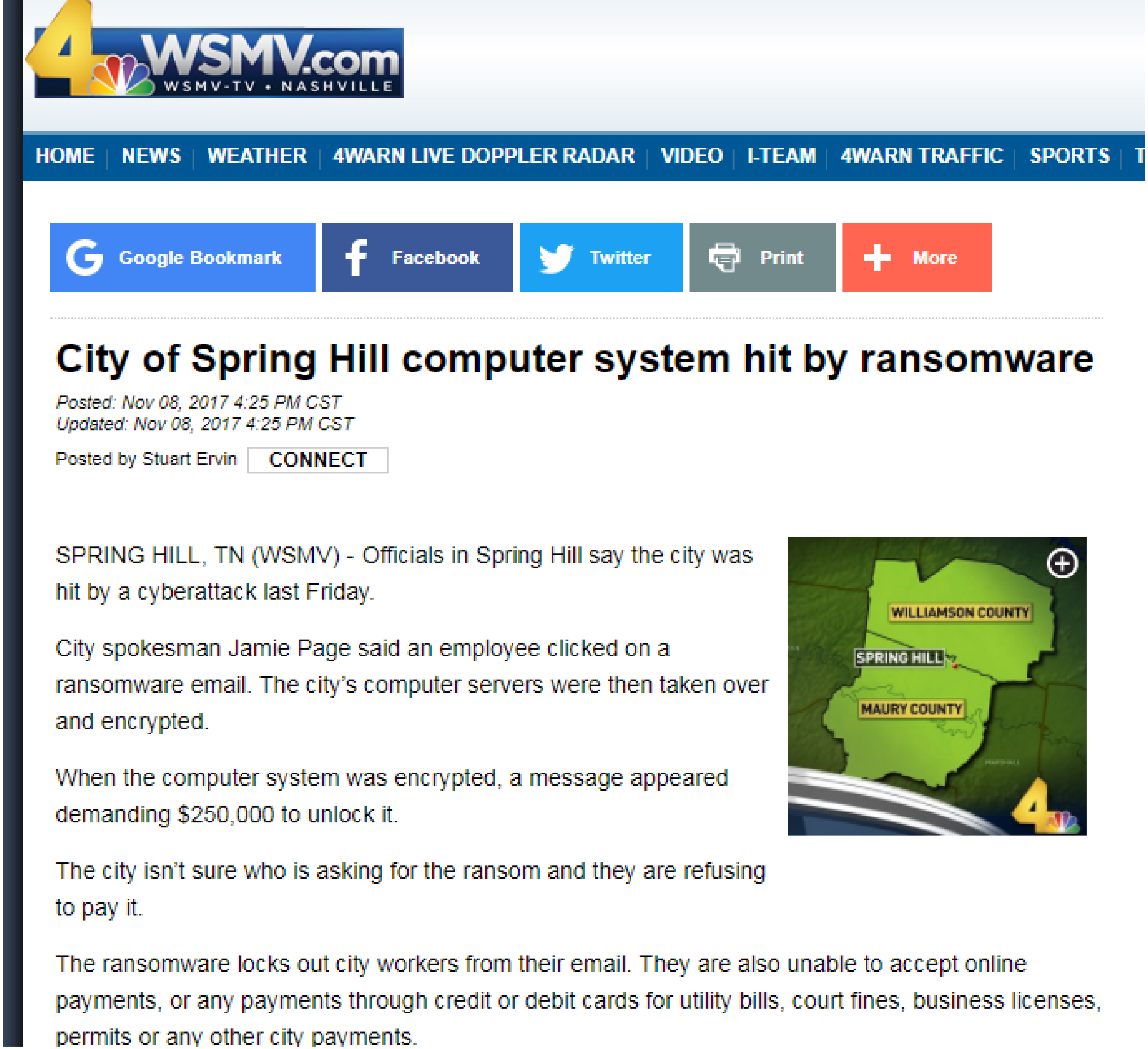
Called you a few times without success. Decided to reach you by email. I need to know the status of this invoice below, it's way past due.

http://funfrance.fr/Invoice-266141-reminder/

Yours Truly,
Tammy Steele

What does a phishing email look like?

- Sense of urgency
- Spelling or grammar mistakes
- Personal or unrecognized email addresses
- Requesting highly sensitive information
- Unfamiliar tone/language


4 WSMV.com
WSMV-TV • NASHVILLE
HOME | NEWS | WEATHER | 4WARN LIVE DOPPLER RADAR | VIDEO | I-TEAM | 4WARN TRAFFIC | SPORTS | T
Google Bookmark
Facebook
Twitter
Print
More

City of Spring Hill computer system hit by ransomware

Posted: Nov 08, 2017 4:25 PM CST
Updated: Nov 08, 2017 4:25 PM CST

Posted by Stuart Ervin

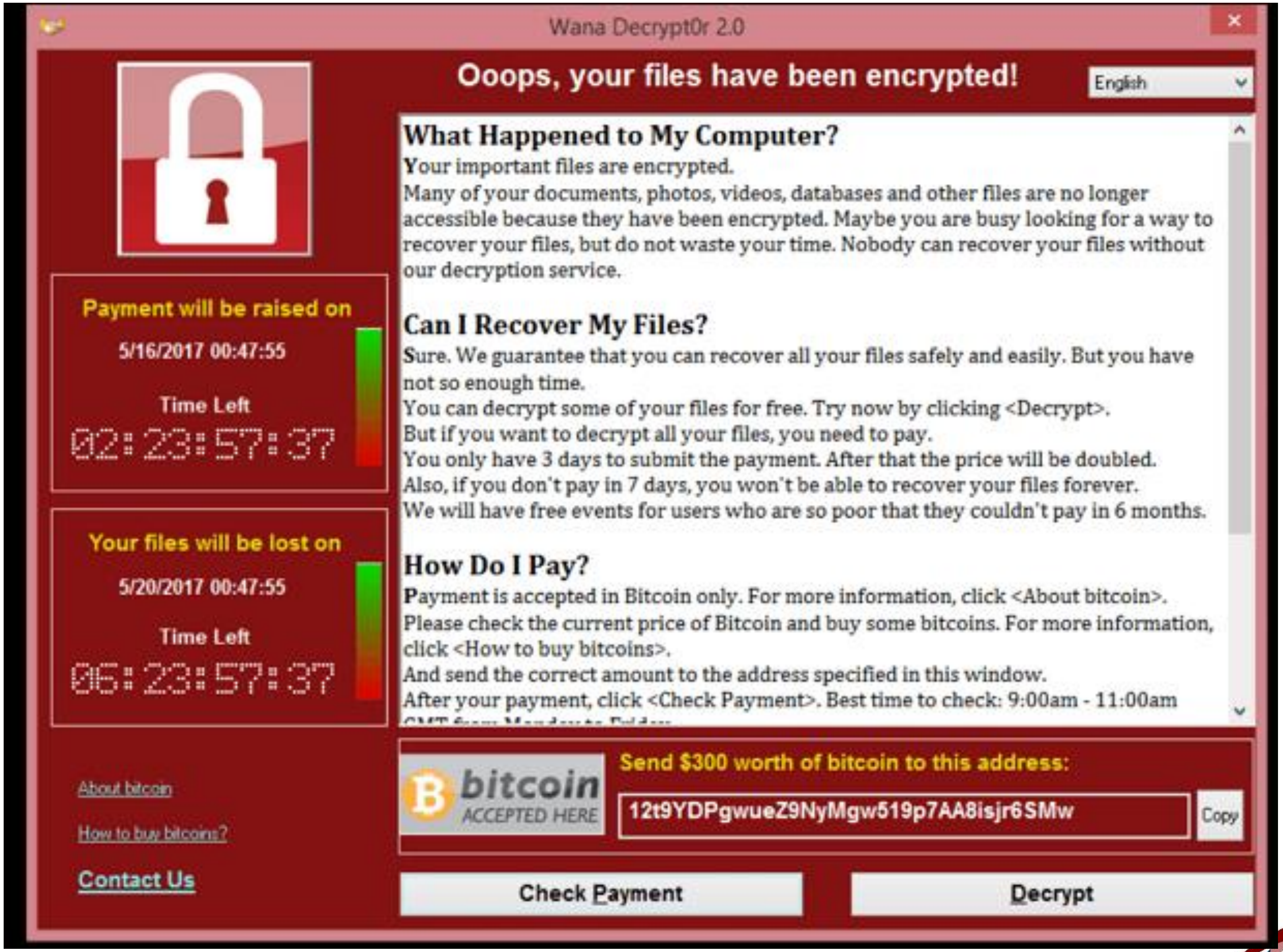
SPRING HILL, TN (WSMV) - Officials in Spring Hill say the city was hit by a cyberattack last Friday.

City spokesman Jamie Page said an employee clicked on a ransomware email. The city's computer servers were then taken over and encrypted.

When the computer system was encrypted, a message appeared demanding $250,000 to unlock it.

The city isn't sure who is asking for the ransom and they are refusing to pay it.

The ransomware locks out city workers from their email. They are also unable to accept online payments, or any payments through credit or debit cards for utility bills, court fines, business licenses, permits or any other city payments.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

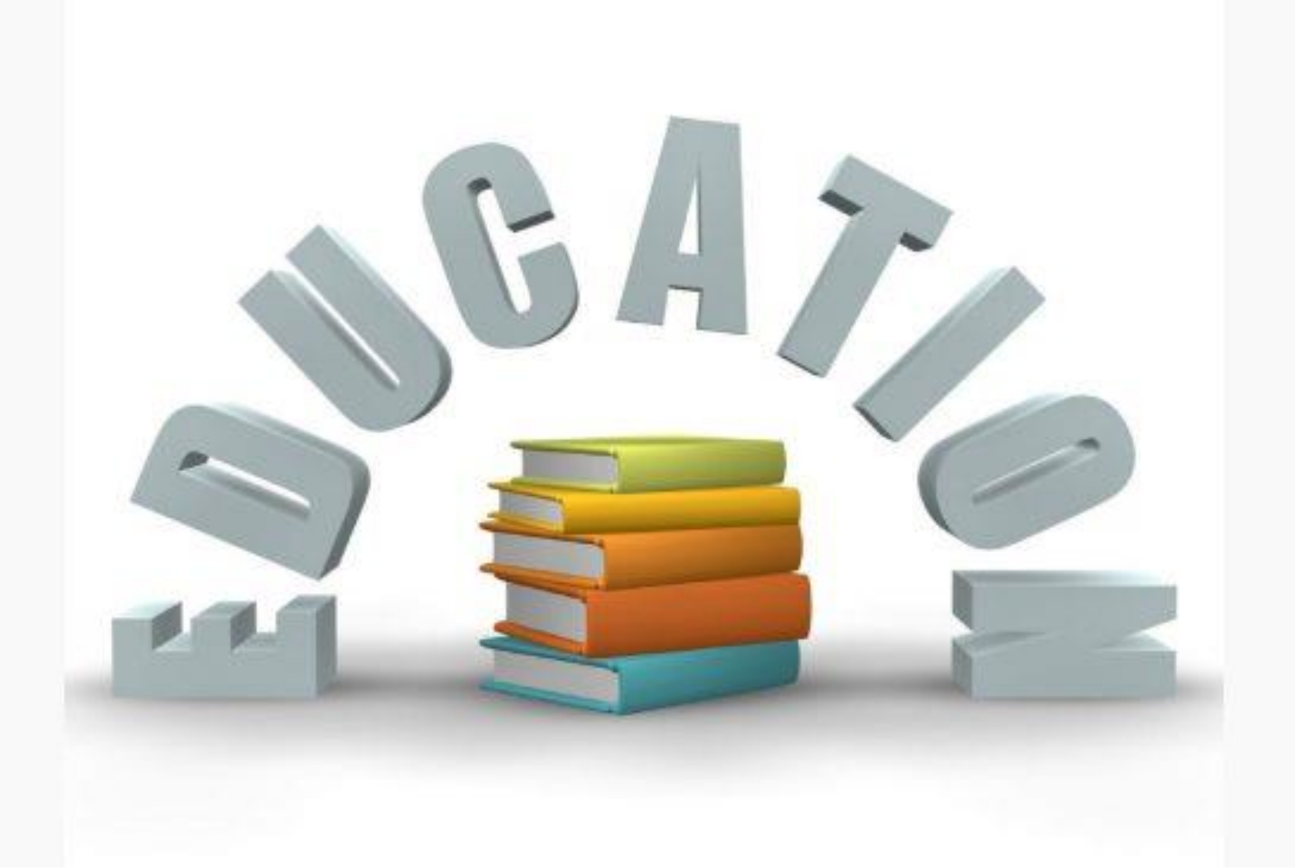
06:23:57:37

Send $300 worth of bitcoin to this address:

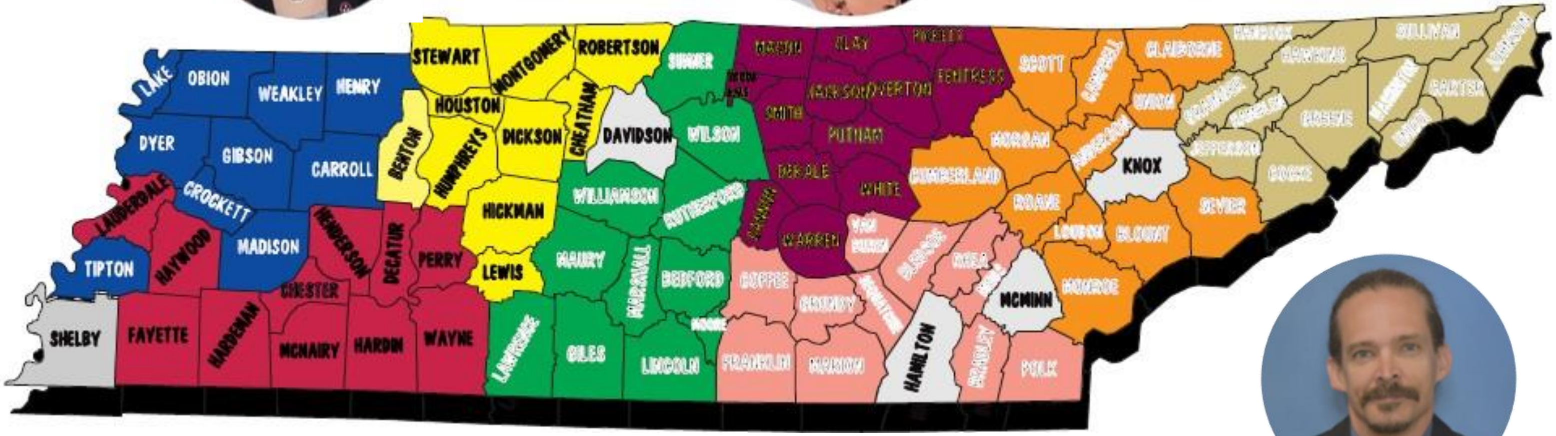
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How Is Ransomware Launched?

- Opening an email or email attachment from someone you may or may not know and were not expecting
- Visiting an unsafe, suspicious, or fake website
- Clicking on a malicious or bad link in an email, on Facebook, Twitter, and other social media posts (like articles, videos, ads), and even instant messenger chats


EDUCATION

COT
CYBER
AWARE



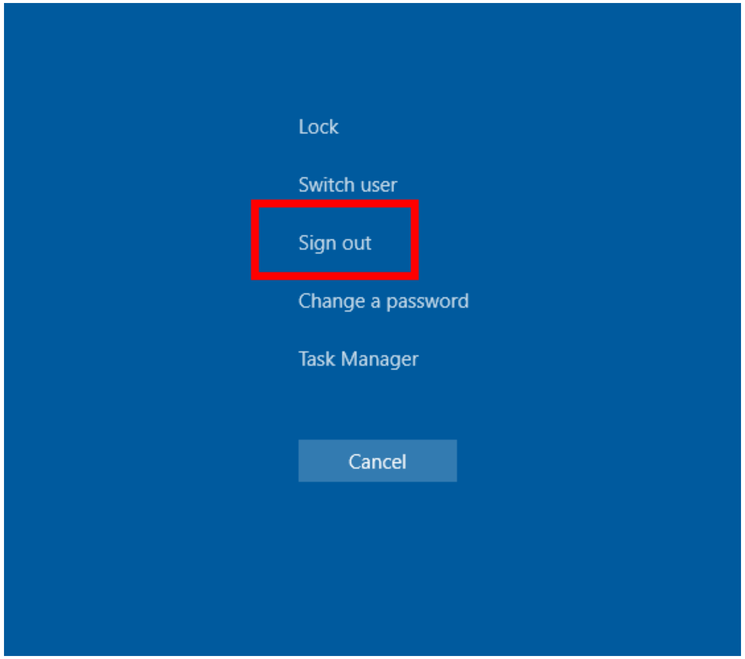
TENNESSEE
COMPTROLLER
OF THE TREASURY

Policies and Procedures

- System startup/shutdown
- Operating system and application security
- System backup procedures
- Hardware disposal policy
- Virus prevention policy
- Planning and budgeting of equipment
- Routine processing of applications
- Output distribution

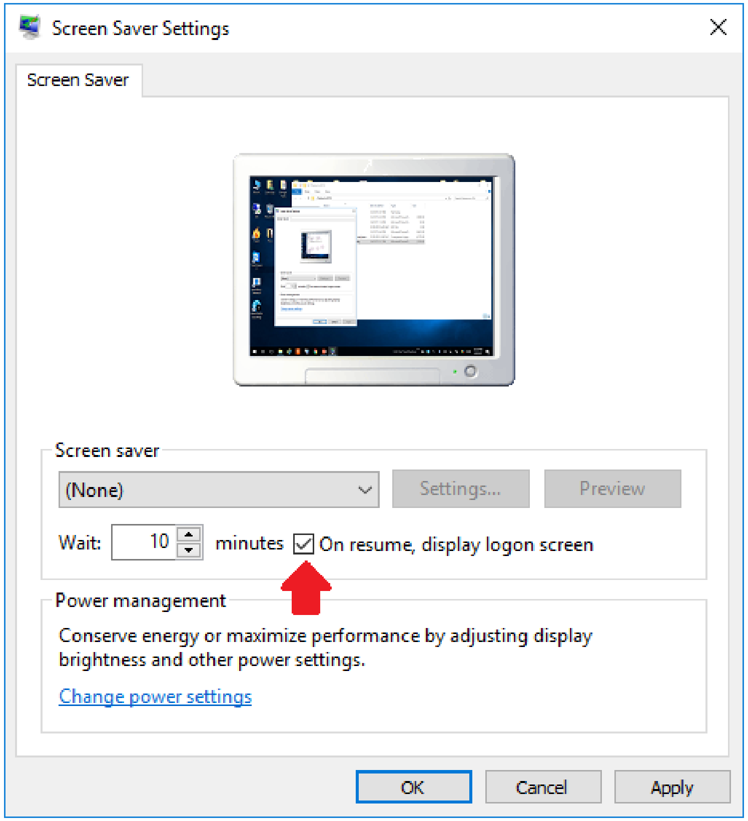
Operating System Security

- Passwords
- Protecting the operating system
  - Shut down
  - Log off Windows
  - Manually lock
    - Ctrl + Alt + Delete
    - “Windows” key + L



Operating System Security

- Screensaver
  - Password protected
  - Activates after a maximum of 30 minutes



Screen Saver Settings

Screen Saver

Screen saver

(None)

Wait: 10 minutes ☑ On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Change power settings

Operating System Security

- Windows Updates
  - Operating system updates should be installed when made available

- Guest Account
  - Local user account without a password
  - Disable or Rename

Antivirus

Wireless Networks

- Use encryption
- Require a strong password
- Hide your network name (SSID)
- Change the default password on your router
- Reboot / reset periodically

Acceptable Use Agreement

- The agreement should state that all hardware and software are the property of the local government.
- The agreement should state that the employee has no expectation of privacy in regards to any information created, stored, or distributed using the local government’s computer system.
- The agreement should state that passwords shall remain confidential and not be disclosed to others.

Disaster Recovery Planning

- Specific steps to needed to restore the system
- Emergency phone numbers of personnel and vendors
- Backup storage location
- Specific contingency site
- Manual processing procedures
- Hardware inventory listing

Tennessee Comptroller of the Treasury

Proper Back-up Procedures

- §10-7-121(c), TCA:
  - Daily backups
  - Off-site rotation once a week
- Daily backups should be stored in a secure location within the office.
- Off-site backups should be stored in a secure but appropriate storage location.
- A backup should remain at off-site location for the duration of the week.
- Don’t rely solely on cloud backups.
- Test backups once a year.

Application Security

- All users should have a unique username and password. Shared logins should not be used.
- Avoid generic usernames like MAIN or COUNTER.
- Passwords should remain confidential.
- Passwords should be changed every 90 days.
- Logins of former employees should be immediately disabled.
- Exit the applications when away from your desk for an extended period of time.

Tennessee
Comptroller
of the Treasury

Password Complexity

- Avoid using widely known information
- The longer, the better
- Create a passphrase which consists of multiple words and is at least 14 characters long

TENNESSEE
COMPTROLLER
OF THE TREASURY

Required Filings

- TCA 47-10-119
  - *Uniform Electronic Transaction Act (UETA)*
  - Requires all local governments who implement an electronic business system to file statements with the Comptroller’s office
- TCA 4-30-103
  - *Local Government Technology Act*
  - Requires all local governments who implement a new technology platform to file a statement with the Comptroller’s office

Required Filings

- TCA 10-7-123
  - *Remote Access Statement/Guidelines*
  - Requires all local governments who provide remote access to county records to file statement with the Comptroller's office
  - Access must be inquiry-only
  - Counties can charge a fee sufficient to recover the cost of providing the service.
  - Access must be offered to everyone equally.

?

Contact Information:

Penny Austin – Penny.Austin@cot.tn.gov

Greg Brush – Greg.Brush@cot.tn.gov

TENNESSEE COMPTROLLER OF THE TREASURY