



Public Works

LOS ANGELES COUNTY

HR Security

(Securing Sensitive Data)

"We have a duty to protect the information that has been entrusted to us."

Paul Lam
9/19/18

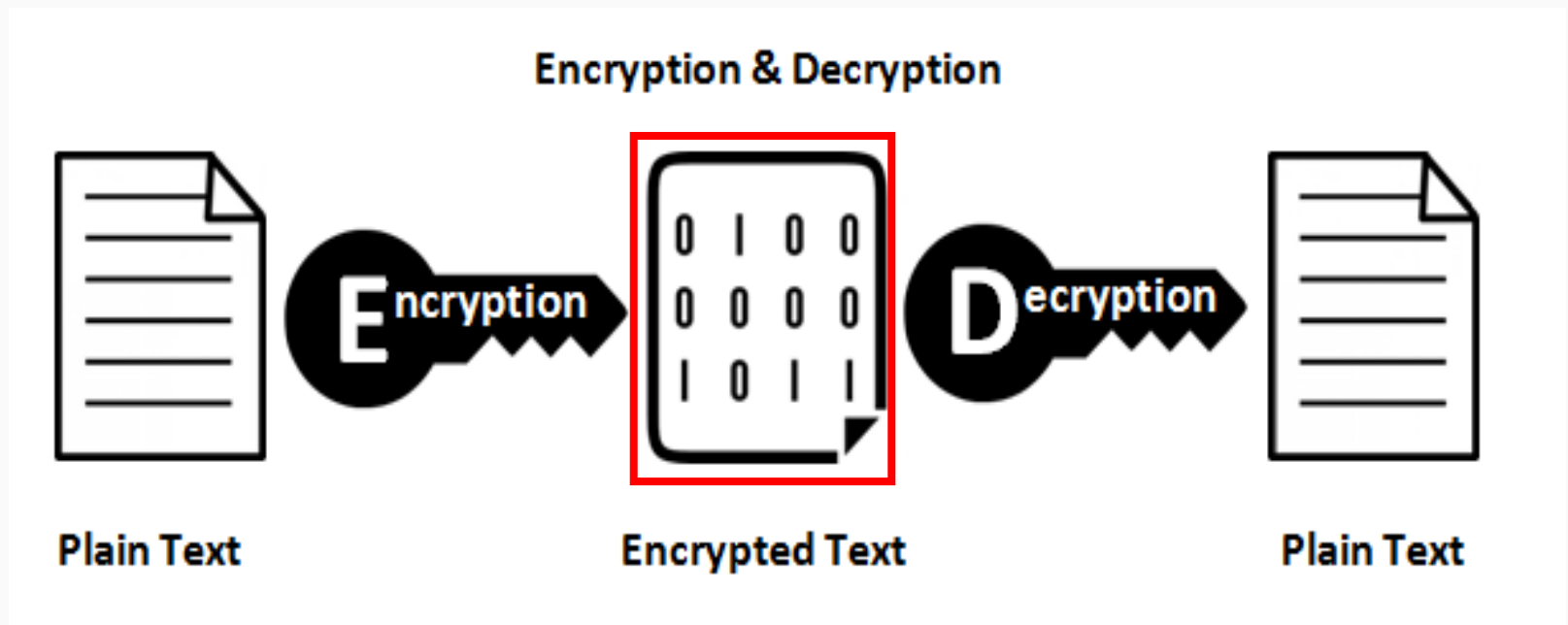
Agenda

- Personally Identifiable Information (PII)
- Securing Sensitive Data
- Sending Secure Email
- Phishing Examples
- Questions

Personally Identifiable Information (PII)

PII includes: Name, Email, Home Address, Phone Number, etc.	
Sensitive PII includes:	
If Stand Alone:	If Paired with Another Identifier:
Social Security Number (SSN)	Last four digits of SSN
Driver's License or State ID Number	Date of Birth
Passport Number	Account Passwords
Financial Account Number	Mother's Maiden Name
Credit Card Number (s)	Protected Health Information (PHI)
Biometric Identifiers	Criminal History
	Any Information that may adversely affect a person

Securing Sensitive Data (Encryption)



Securing Sensitive Data

1. APPLICATION

- ☐ Enable Two-Factor Authentication
- ☐ Use password with a minimum of 8 characters (uppercase, lowercase, numbers, and special characters)
- ☐ Use 'https' for accessing websites/applications

2. STORAGE OR FILE TRANSFERS

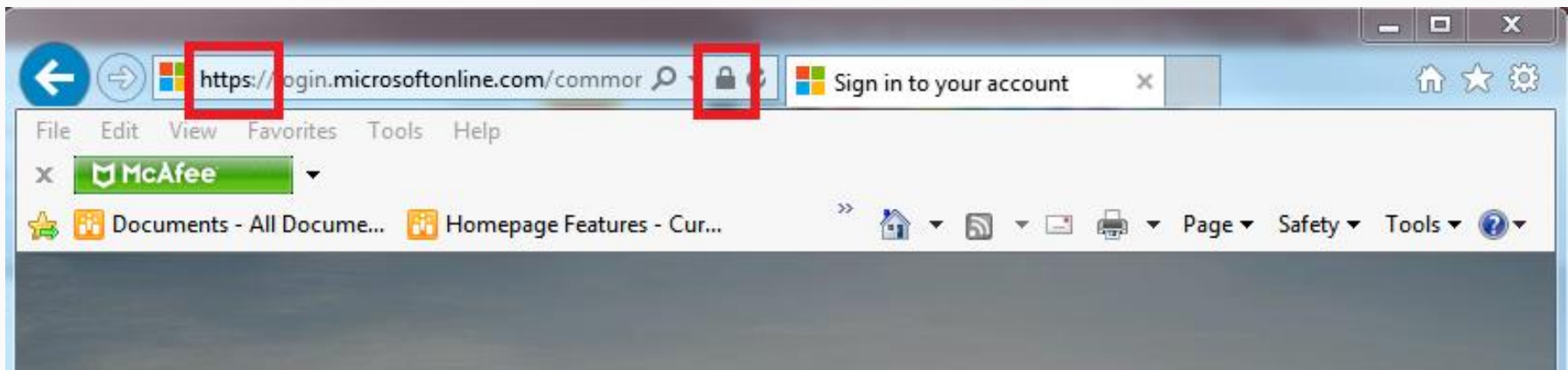
- ☐ Encrypt using zip (AES-256 with strong passphrase)
- ☐ Hard Drive is encrypted at source and destination
- ☐ USB Drive is encrypted when transferring/storing
- ☐ Use Managed File Transfer (Secure FTP)
- ☐ Use [Secure] email for sending to external recipients
- ☐ Password protect Email attachments and contact the recipient outside of email to share the password (e.g., text, phone call)

3. PAPER DOCUMENTS

- ☐ Use secure printing (File → Print → Printer Properties → Job Type: Secure print)
- ☐ Shred documents when not needed
- ☐ Lock Drawers and Cabinets

Applications/Websites

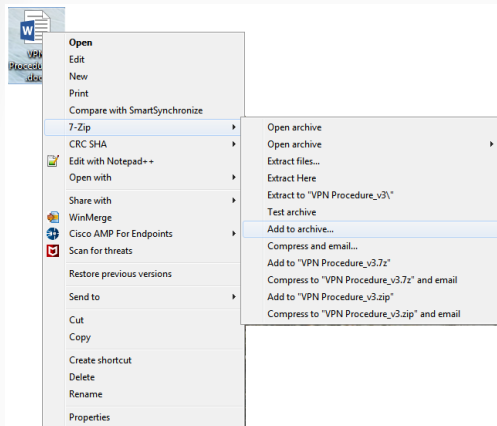
- Ensure URL has '**https**' and you see the '**lock**'  symbol.



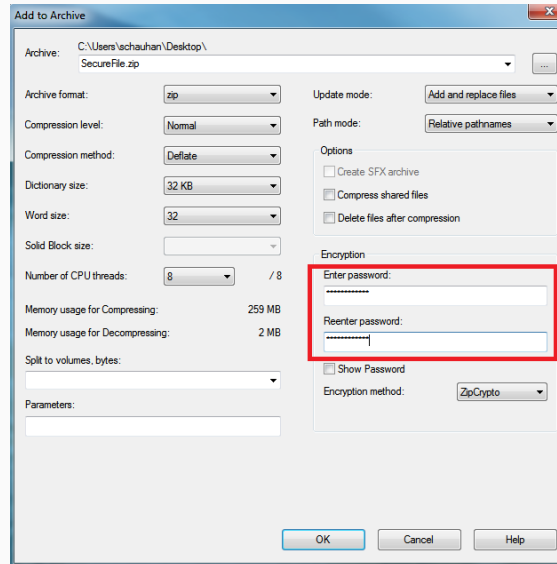
Files

■ Archive and set password (Recommend 7zip)

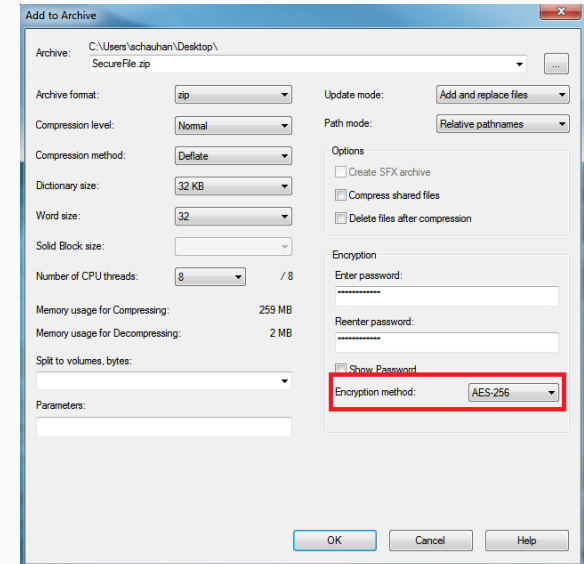
Step 1 - Archive



Step 2 – Set Password



Step 3 – Set Encryption



Sending Secure Email

■ External Emails

- Insert [Secure] in Subject line



The screenshot shows an email composition window. On the left is a 'Send' button. To its right are fields for 'To...', 'Cc...', and 'Bcc...'. The 'To...' field contains two email addresses: 'lacserviceteam@greatwest.com;' and 'strategicaccounts-teaminbox@kp.org'. Below these is the 'Subject' field, which is highlighted with a red rectangular box. The text in the 'Subject' field is '[Secure] Employee Benefits Update - John Smith #123456'.

■ Internal Emails

- Send password protected file as an attachment for all other 'lacounty.gov' departments
- Do not send password in Email

External Entities



DA



BOS

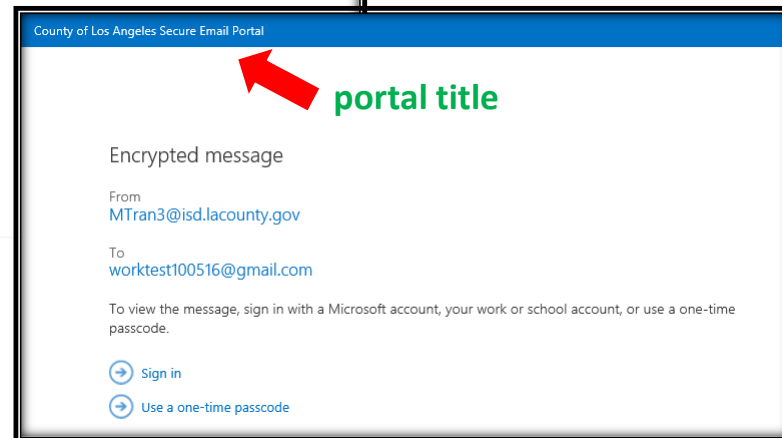
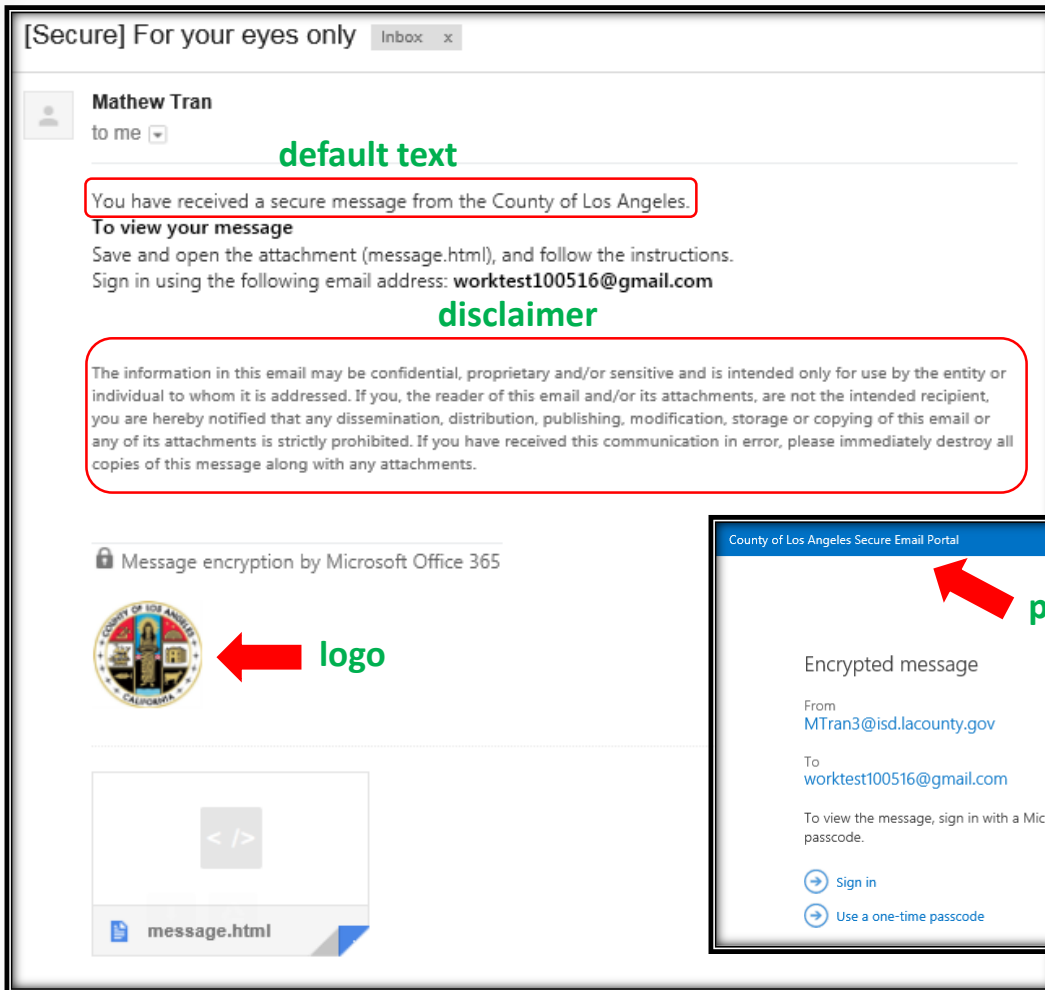


External
Agencies



Sheriff

External Email



External Email (One time passcode)

Step 1 – Select 'Use a one-time passcode'

County of Los Angeles Secure Email Portal

We sent a one-time passcode to
johndoe@dpw.lacounty.gov

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

☐ This is a private computer. Keep me signed in for 12 hours.

 Continue

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).

Step 2 – Receive a one time passcode via email



Here is your one-time passcode

54918131

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

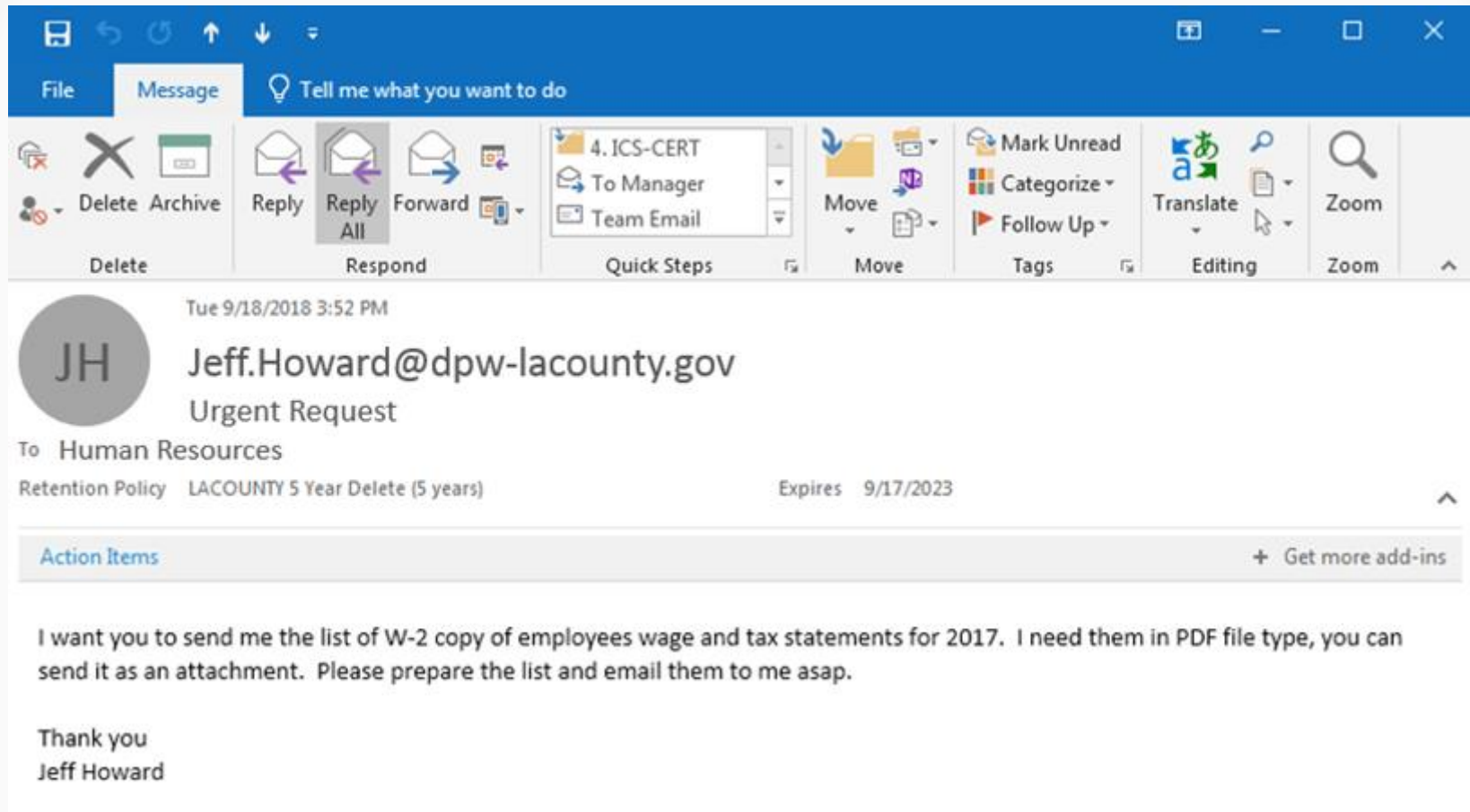
Don't want to use one-time passcode every time you get a protected message? Use your email address to [create a Microsoft account](#)

This message is automatically generated. Please don't reply to it.

Email Security Tips

- ❑ Redact Sensitive information (if not needed)
- ❑ NO Sensitive Data in email body
- ❑ Password PROTECT FILE with sensitive data (Do not include the password)
- ❑ Contact the recipient outside of email to share the password (e.g., text, phone call)


How to identify a Phishing scam?



Phishing Tips

- Do not reply, click on links, or call unknown numbers.
- Contact sender or businesses directly to confirm message.
- Do not provide any personal information in response to a text message.

Secrity is not complete without **U**!

- Always lock computers (Win  + L) and other valuables when walking away from your desk.
- Report
 - Incident to Help Desk @ (626) 458-**4118**
 - Theft to HQ Security @ (626) 458-**4040**
- IT Security Information
 - <https://go/security>