When in Doubt Throw it Out!

PHISHING: DON'T GET HOOKED BY A SCAM!

Outline

- Phishing Defined
- Phishing Terminology
- How to identify a Phishing attempt
- How to protect yourself from being Phished
- Examples
- Resources available to you if you have been Phished
- Summary
- Questions ?

Phishing Defined

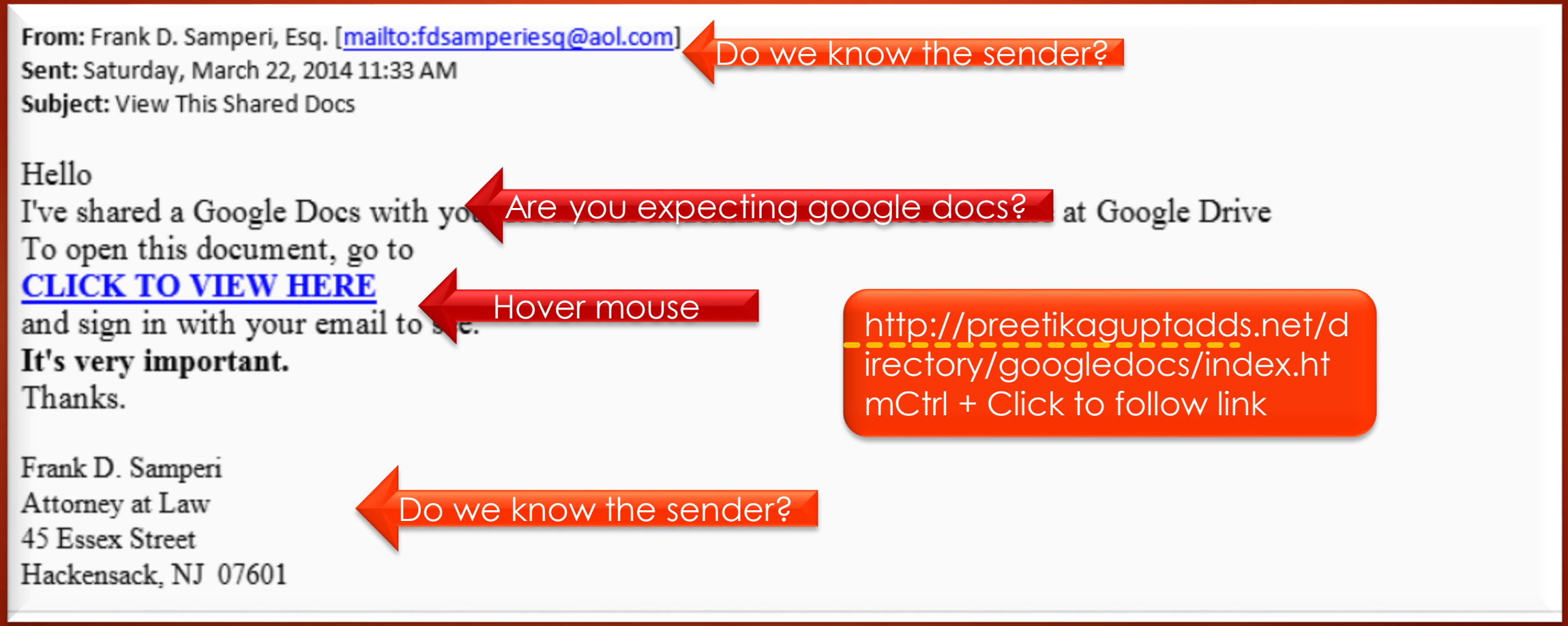
- Phishing : is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by impersonating a trustworthy source, normally by email.
- Phishing Methods
  - Spoofed – A fraudulent e-mail sent to mask as a legitimist company
    - Confirmation Emails – Are one of the most common spoofed emails.
      - Such as UPS,USPS, FEDEX, or any Retail store.
    - Helpdesk or Support emails – Are sent to have a user click a link within the email to "fix" an issue with their account.
      - This is commonly used for accounts that may contain financial or medical information.
  - Malicious URL –
    - Malicious URL - http://www.american.expres.com
    - Legitimate URL - http://www.americanexpress.com
      - Use caution when clicking on embedded links as your eyes can play tricks on you as it is easy to miss the subtle differences
      - Fraudsters are counting on users to miss these minor differences

Phishing Terminology

- Phishing
- Spoofed
- Ransomware
- Malware
- Keylogger
- URL
- Redirect
- Marcros & Ad Ons

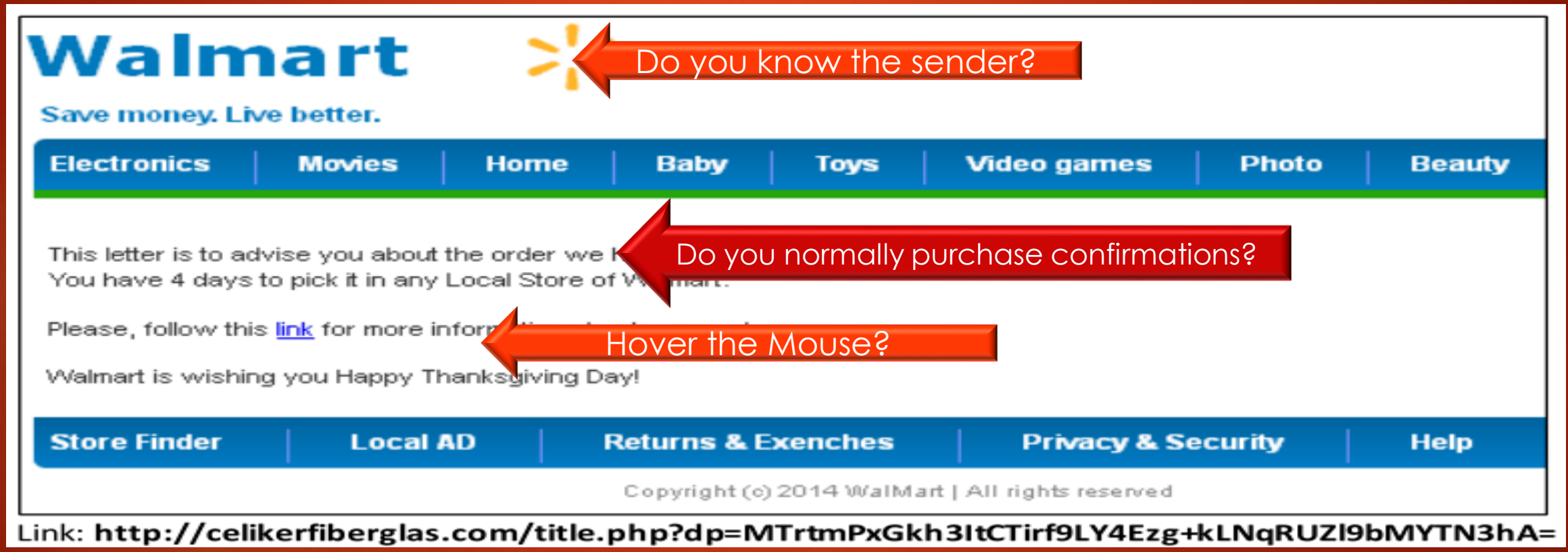
Identify Phishing Attempt

- Are you expecting files to large to email?



Identify Phishing Attempt

- A closer look
  - At first glance what do we see…



A user who received this email…

…. Opened the Attachment ☹

Top Ten 10 Phishing Attempts 2014

- Phishing Scams of 2014
  - 10. Fax Notice
  - 09. Bank Alert, installs Keylogger
  - 08. Message from Attorney
  - 07. Email delivery failure installs Ransomware Phishing
  - 06. Payroll, ADP, with PDF (malware) attachment.
  - 05. IRS, tax collection.
  - 04. Fax notice, with banking malware.
  - 03. .EDU domain that offers remote access.
  - 02. Dropbox, offers malware or crypto-malware instead.
  - 01. Unknown sender or 3rd party file share, offers malware & remote access.

Summary

- Phishing. It's old school but it still works.
- Think before you click!
- Privacy is everyone's responsibility
- Just like your personal data, your employer needs to ensure its privacy too.
- A targeted phishing mail was sent to a number of celebrities, enticing them to enter their iCloud credentials onto a fake login page would do the job just as well as any more complex hack.
- Do not open attachments or click links in unusual email, text, or instant messages (IM), on social networks, or in random pop-up windows.

- Questions to ask yourself:
  - Do you know the sender?
  - Does the attachments make sense (do you normally receive invoices as
  - Be extremely cautious if you receive an email, text messages, or messages from social networks like Facebook, LinkedIn, and Twitter.
  - You should you be suspicious of links and attachments from someone on your team?