Sen. Cristina Castro's Cybersecurity Forum

Protecting Your Data

Presented by: Shawn Davis
Adjunct Professor - Illinois Institute of Technology
Dir. of Digital Forensics – Edelson PC

Table of Contents:

1. Staying Safe Online

2. Protecting Your Online Privacy

3. Questions

Staying Safe Online

What are some typical online attacks against consumers???

- Phishing/social engineering
- Email hacked and friends spammed
- Hacked online accounts/cards
- Malicious software installed on your computer/mobile device
- Attackers gaining access to your computer or network

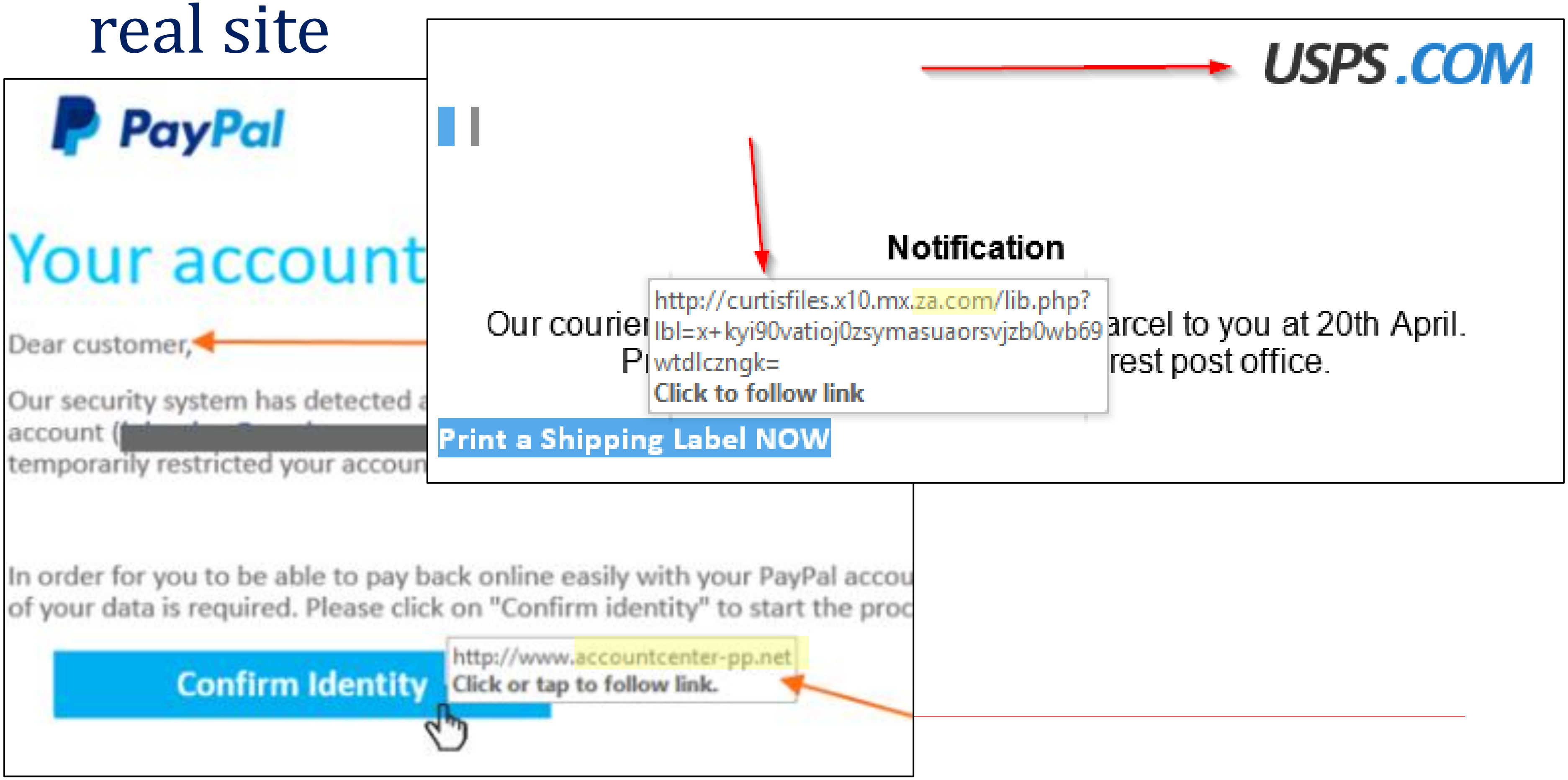
Social Engineering (Phishing Emails)

Make sure not to:

1. Click on a malicious link
   - Leads to infected or fake website that requests your username/password (fake Gmail, Facebook, etc.)
2. Open a malicious attachment
   - Infection with spyware, ransomware, etc.
3. Reply to attacker with PII or other sensitive information

Phishing Email Example 1

- Hover over link but don't click
- Make sure the domain (highlighted) is for the real site



USPS.COM

Notification

Our courier

P

http://curtisfiles.x10.mx.za.com/lib.php?lbl=x+kyi90vatioj0zsymasuaorsvjzb0wb69wtdlczngk=
Click to follow link

arcel to you at 20th April.
rest post office.

Print a Shipping Label NOW

PayPal

Your account

Dear customer,

Our security system has detected a
account ([redacted]
temporarily restricted your accoun

In order for you to be able to pay back online easily with your PayPal accou
of your data is required. Please click on "Confirm identity" to start the proc

Confirm Identity

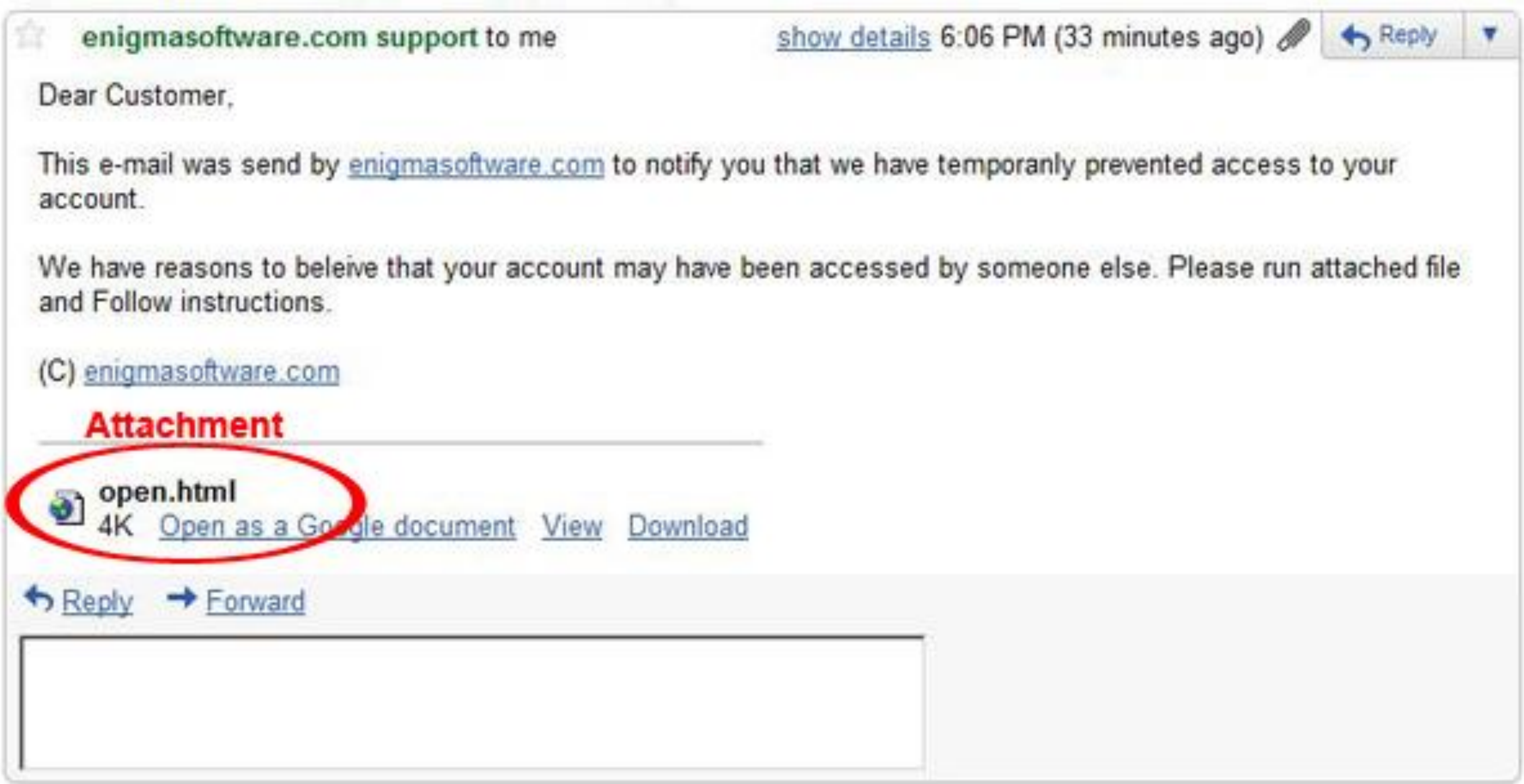
http://www.accountcenter-pp.net
Click or tap to follow link.

Identifying Malicious Links in Phishing Emails

- Good links:
  - https://www.google.com
  - https://mail.google.com
  - https://www.google.com/signup
- Bad Links:
  - https://www.google.com.me.com
  - https://www.corp-google.com
  - https://www.googgle.com

Phishing Email Example 2

- Don’t open unknown attachments



enigmasoftware.com support to me   show details 6:06 PM (33 minutes ago)

Dear Customer,

This e-mail was send by enigmasoftware.com to notify you that we have temporanly prevented access to your account.

We have reasons to beleive that your account may have been accessed by someone else. Please run attached file and Follow instructions.

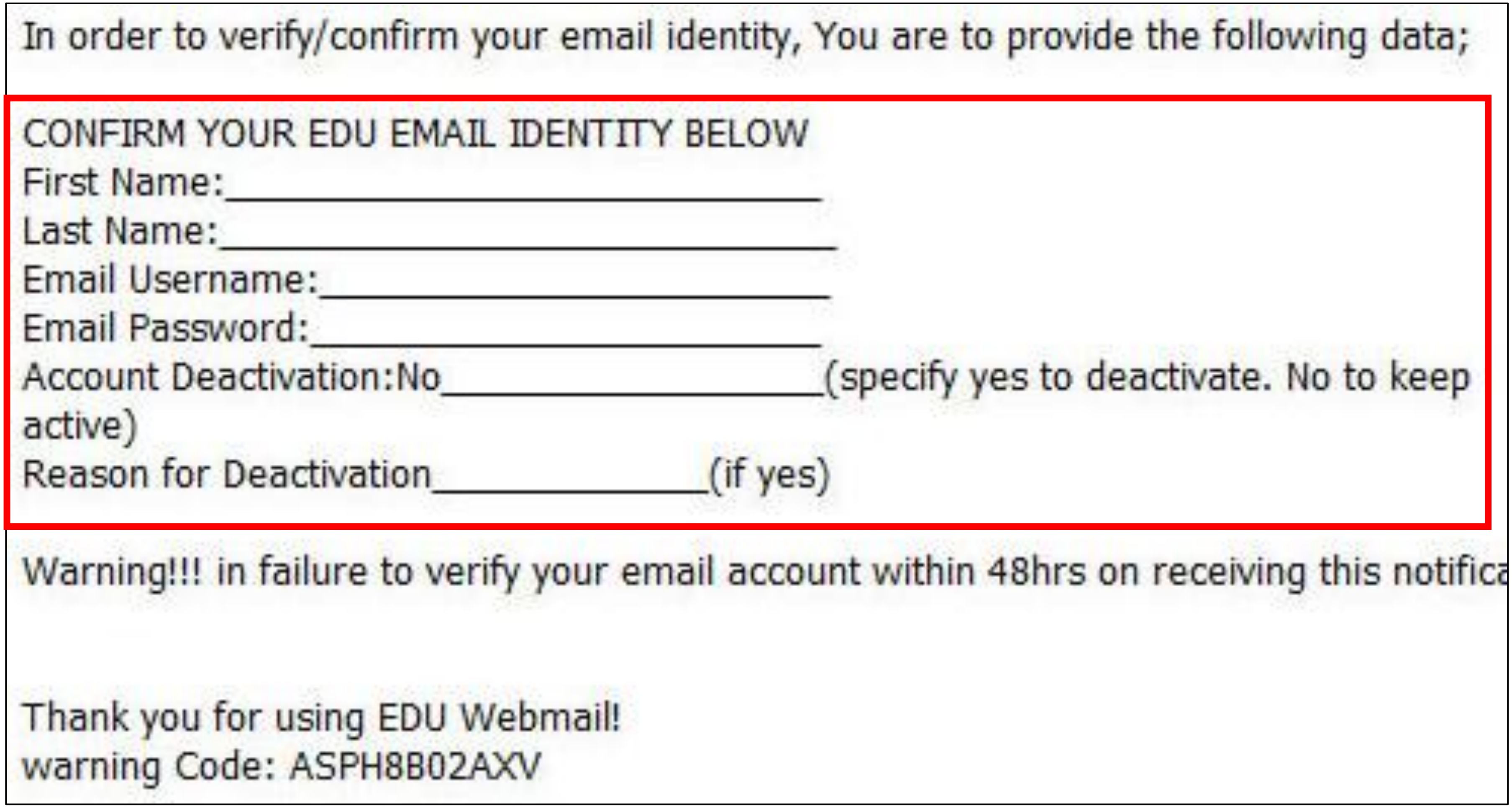
(C) enigmasoftware.com

Attachment

open.html
4K

Phishing Email Example 3

- Don’t ever provide password or PII



In order to verify/confirm your email identity, You are to provide the following data;

CONFIRM YOUR EDU EMAIL IDENTITY BELOW
First Name:____________________________
Last Name:____________________________
Email Username:________________________
Email Password:________________________
Account Deactivation:No__________________(specify yes to deactivate. No to keep active)
Reason for Deactivation_____________(if yes)

Warning!!! in failure to verify your email account within 48hrs on receiving this notifica

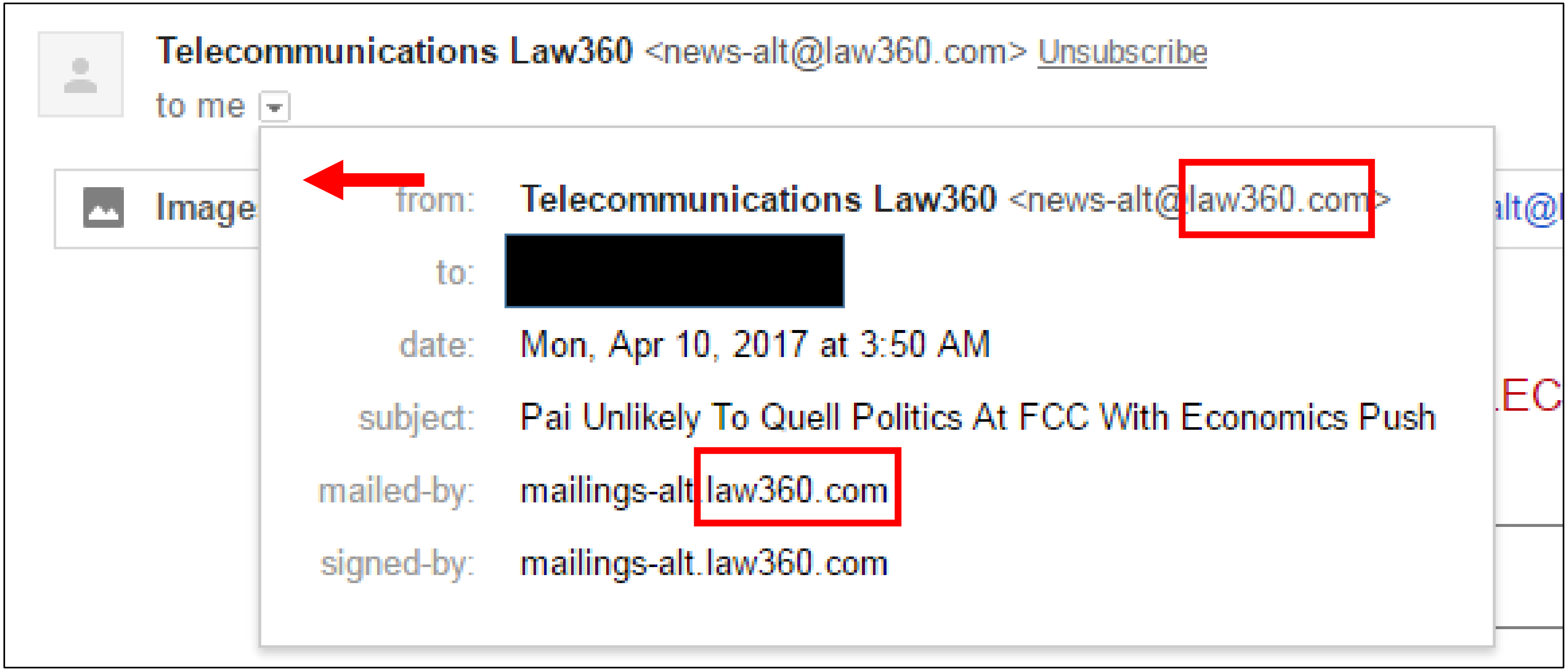
Thank you for using EDU Webmail!
warning Code: ASPH8B02AXV

Identifying Phishing Emails

- Let’s take a quiz!
- https://phishingquiz.withgoogle.com/

Legitimate Email (shown below)

- Make sure “from” and “mailed-by” domains match and are the real domain of the site (not something similar or spelled incorrectly)



Telecommunications Law360 <news-alt@law360.com> Unsubscribe

to me

from: Telecommunications Law360 <news-alt@law360.com>

to: [redacted]

date: Mon, Apr 10, 2017 at 3:50 AM

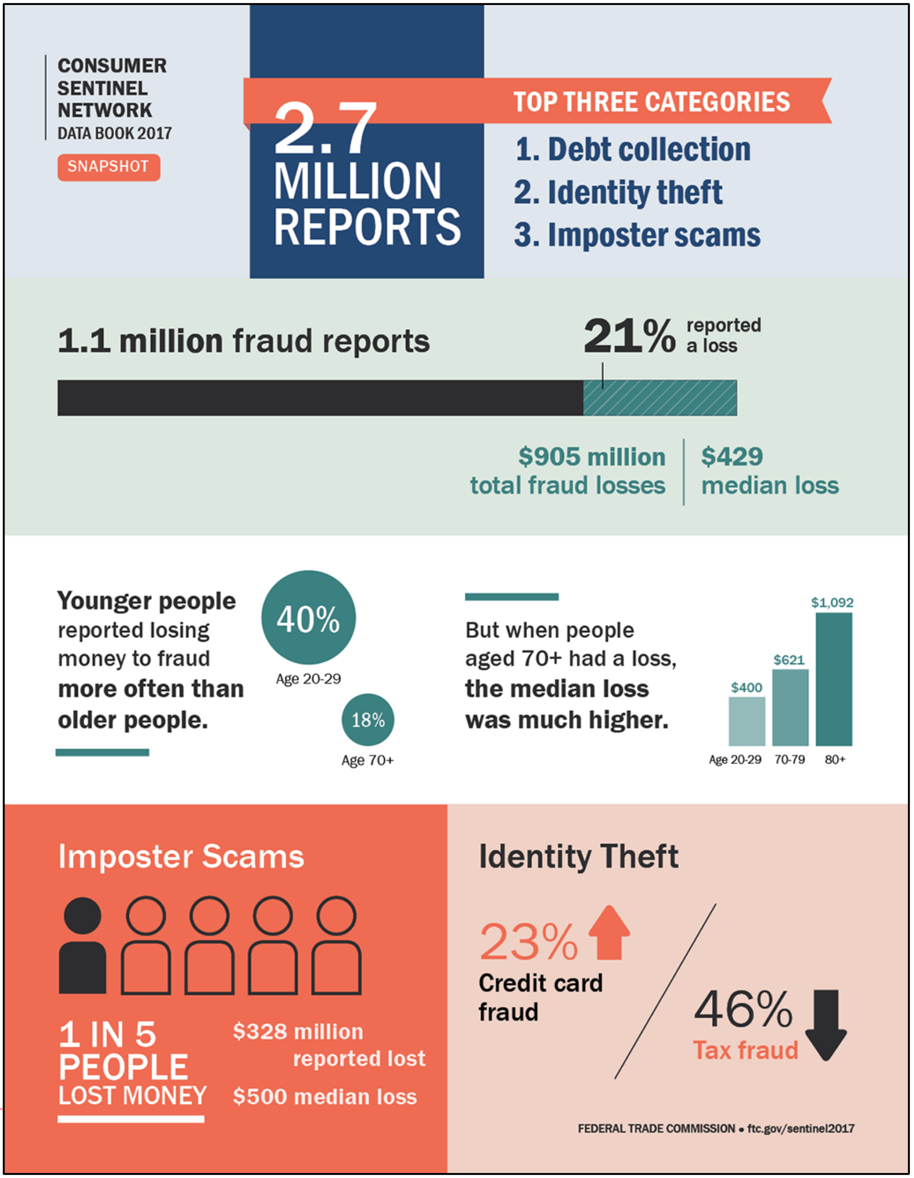
subject: Pai Unlikely To Quell Politics At FCC With Economics Push

mailed-by: mailings-alt.law360.com

signed-by: mailings-alt.law360.com

Social Engineering (Phone)

- Fake Tech Support
- Fake IRS
- Fake Loved One
- Fake Sweepstakes
- Fake Utility/Bank



CONSUMER SENTINEL NETWORK
DATA BOOK 2017
SNAPSHOT

2.7 MILLION REPORTS

TOP THREE CATEGORIES

1. Debt collection
2. Identity theft
3. Imposter scams

1.1 million fraud reports

21% reported a loss

$905 million total fraud losses

$429 median loss

Younger people reported losing money to fraud **more often than older people.**

But when people aged 70+ had a loss, **the median loss was much higher.**

Imposter Scams

1 IN 5 PEOPLE LOST MONEY

$328 million reported lost

$500 median loss

Identity Theft

23% Credit card fraud

46% Tax fraud

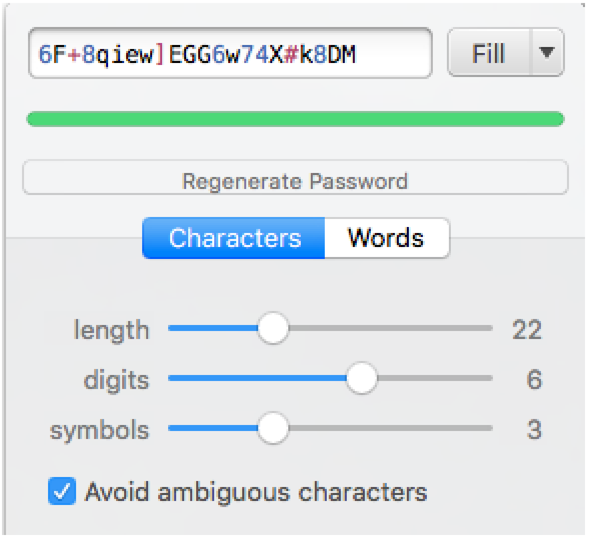
FEDERAL TRADE COMMISSION • ftc.gov/sentinel2017

Prevent Hacked Online Accounts by…

- Not falling for Phishing
- Not using the same password on multiple sites
- Not using an insecure password
  - Bad: Short, dictionary word, all lowercase, etc.
  - Good: 10 char or more, no dictionary words, use uppercase, lowercase, numbers, symbols
  - Best: Use a password manager!
- Using 2-Factor Verification!
- Not entering information on illegitimate sites

Password Managers

- Generates good random passwords for each site
- Only need to remember one master password!



6F+8qiew]EGG6w74X#k8DM

length 22

digits 6

symbols 3

☑ Avoid ambiguous characters

LastPass ****

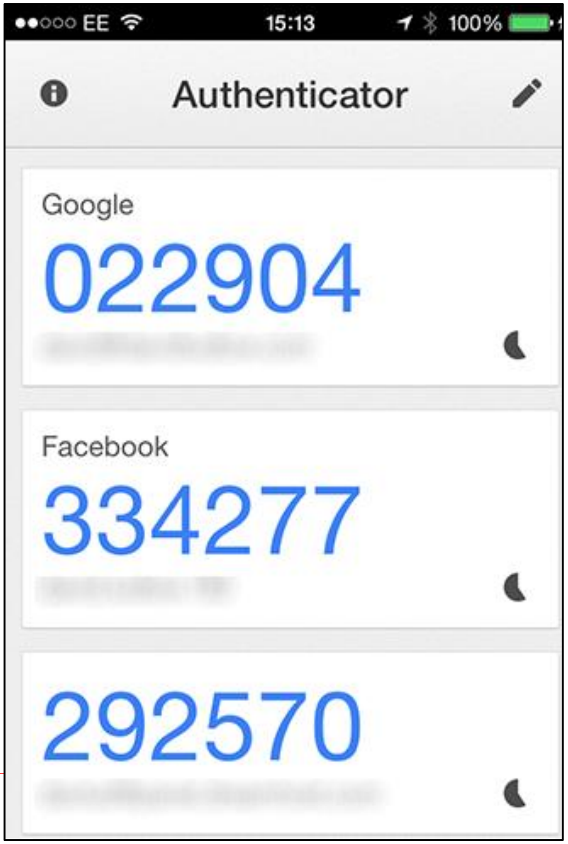
KeePass X

dashlane

1Password

Simple, Convenient Security

- Use 2-Factor Authentication for email, banks, etc.!!!
  - https://www.google.com/landing/2step/
  - Use mobile app with codes as opposed to email when you can



Authenticator

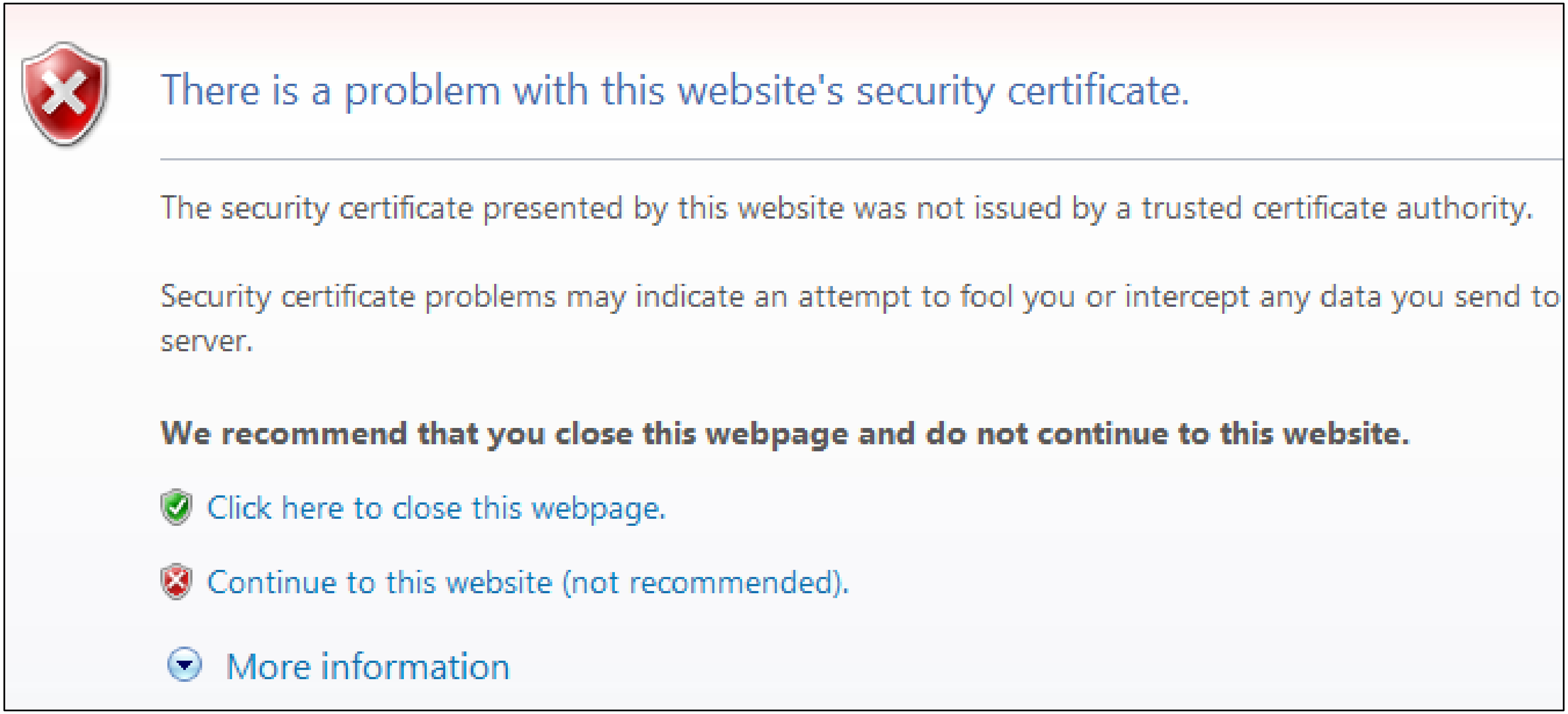
Google
022904

Facebook
334277

292570

Illegitimate Web Sites

- Don’t proceed/continue to websites that have issues with their certificate (which determines if site is legitimate)



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to
server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Other Avenues for Device Infection

- Don’t use out of date software
  - Patch OS, Browser, Browser Extensions (Java, Flash, etc.) regularly.
- Don’t use malicious mobile apps
  - More prominent on Android due to ability to install 3rd party apps and less stringent Google Play store when inspecting new apps (Apple is better at vetting apps)
- Don’t download computer applications from less than reputable sources (also no toolbars)

Other Avenues for Device Infection (Cont.)

- Don’t view shady websites (may contain malware)

- Don’t Use public Wi-Fi or insecure home Wi-Fi
  - Use VPN for computers and phones
  - Only setup home Wi-Fi with WPA2 with AES (not WEP or Open)

Other Avenues for Device Infection (Cont.)

- Make sure to change default passwords on IoT or network devices
  - Attackers can search online through Shodan.io for a nanny cam or other device and connect with default passwords

- Use updated Antivirus (AVG, Avira, McAfee, etc.) & Antimalware products (MalwareBytes, SpySweeper, etc.)

- You can take the steps I provided to help prevent the prior attacks
- However, you may still be at risk from a company not taking steps to protect your data
  - Resulting in a data breach
- The following are four examples of major data breaches and their causes

Target

- Attack:
  - Network credentials stolen from third party HVAC vendor
  - Malware pushed to POS devices to capture credit/debit cards
  - Didn’t act on alerts from own 1.6 mil FireEye system
- Result:
  - 41 million payment accounts stolen
  - Target paid ~200 million in lawsuits / CEO fired

Premera Blue Cross/Blue Shield

- Attack:
  - Attackers impersonated Premera website by using fake websites with “prennera.com” domain
  - Lured employees to fake sites with phishing emails
- Result:
  - Name, DOB, SSN, Contact Info, Bank Account Info, Clinical Info of 11 mil people may have been accessed

Advocate Health

- Attack:
  - Four unencrypted desktop computers were stolen from Park Ridge, IL
- Result:
  - Computers contained medical and financial records of ~4 mil patients
  - Paid 5.5 mil for HIPAA violation

Equifax

- Attack:
  - Equifax didn’t patch vulnerable Apache Struts server software even though patch was available for 4 months
- Result:
  - Sensitive personal and financial information of ~143 million consumers exposed

Protecting Your Online Privacy

Defenses Against Active Collection:

Consumer Surveys, Social Media Postings, Web Registration Forms

- Don’t overshare!
- Don’t add DOB, employer, hometown, current address or city, family member names, email, etc. to social media
- Keep in mind pictures taken on your cell phone may have GPS coordinates embedded (AKA Geotagging)

Disabling Geotagging in Photos

- iPhone
  - Settings / Privacy / Location Services / Camera
  - Select “Never”
- Android
  - Camera App / Settings
  - Turn off “Save location”

Defenses Against Passive Collection

3rd Party Computer Cookies

- Turn off 3rd party cookies in your browser

  or

- Install the EFF's Privacy Badger extension in Chrome, Opera, or Firefox to block 3rd party trackers

Defenses Against Passive Collection

3rd Party Cell Phone Cookies

- iPhone
  - Settings / Safari
  - Make sure “Prevent Cross-Site Tracking” is on
- Android
  - Chrome / Three Dots / Settings / Site Settings / Cookies
  - Uncheck “Allow third-party cookies”

Defenses Against Passive Collection

Cell Phone Advertising Identifier & Analytics

- iPhone Advertising ID
  - Settings / Privacy / Advertising
  - Turn on "Limit Ad Tracking"
  - Can also "Reset Advertising Identifier"
- iPhone Analytics
  - Settings / Privacy / Analytics
  - Turn off "Share iPhone Analytics"

Defenses Against Passive Collection

Cell Phone Advertising Identifier & Analytics

- Android Advertising ID
  - Google Settings / Ads
  - Select “Reset advertising ID”
  - Turn on “Opt out of Ads Personalization”
- Android Usage and Diagnostics
  - Google Settings / Three Dots / Usage & Diagnostics
  - Turn to Off

Defenses Against Passive Collection

Do Not Track

- iPhone
  - Settings / Safari
  - Turn on “Ask Websites Not to Track Me”
- Android
  - Chrome / Three Dots / Settings / Privacy
  - Turn “Do Not Track” to On

Defenses Against Passive Collection

Social Media

- Log out of social media accounts when browsing the web

Defenses Against Passive Collection

IP Address/MAC Address

- iPhone & Android
  - Turn off phone
  - Place phone in signal blocking pouch
  - Note: Turning off WiFi/Bluetooth or using Airplane mode might not prevent tracking depending on phone

Defenses Against Passive Collection

Geolocation

- iPhone
  - Settings / Privacy / Location Services
  - A few options:
    - Could turn off Location Services for all apps

      or
    - Choose one of the following for each app:
      - Never
      - While Using the App

Defenses Against Passive Collection

Geolocation

- Android
  - Settings / Location
  - A few options
    - Could turn off Location Services for all apps if prior to Android 6
    - If Android 6, could turn off location for each app
      - Settings / General / Apps / Configure apps / App permissions / Your location
      - Select specific apps to disable location-tracking

Defenses Against Passive Collection

Geolocation

- Google (Android & iPhone)
  - https://myaccount.google.com/activitycontrols
    - Pause “Web & App Activity”
      - This setting tracks your location when using Google apps and Google search when enabled.
      - On by default
    - Pause “Location History”
      - This setting tracks your location all of time in the background.
      - Off by default.

Defenses Against Active & Passive Collection

Credit Card Transactions

- Consider paying cash for sensitive purchases

Shopper Loyalty Programs

- Consider not using these programs if concerned about targeted advertising
  - Ex: Purchase new baby car seat, formula, etc.
    - Added to new parent profile

Defenses Against IoT Collection

- Not everyone has a testing lab to capture the traffic between IoT devices and the Internet
- If you do:
  - Wireshark
  - Burp Suite
  - Etc.
- If you don’t: Google for your product name and privacy, hacking, vulnerabilities, etc.

- Lastly, keep in mind that browser incognito mode doesn’t keep websites or your ISP from knowing the sites you visit.
    - Use a VPN on computer and mobile devices for greater ability to be anonymous!!

The last two sections of this presentation will be uploaded to:

- http://senatorcristinacastro.com

- You can then take time to review the privacy settings for your devices