SAILING INTO RETIREMENT

2018

TMRS Annual Seminar

Presentations available at www.tmrs.com/ats.php

SAILING INTO RETIREMENT

Batten Down the Hatches

Fraud and Security Panel

Presentations available at www.tmrs.com/ats.php

Batten Down the Hatches — Panel

- Sandra Vice, Director of Internal Audit
- Oscar Guzman, Information Systems Security Analyst
- Peter Jeske, Member Services Business Analyst
- Moderator: Colin Davidson, Regional Manager

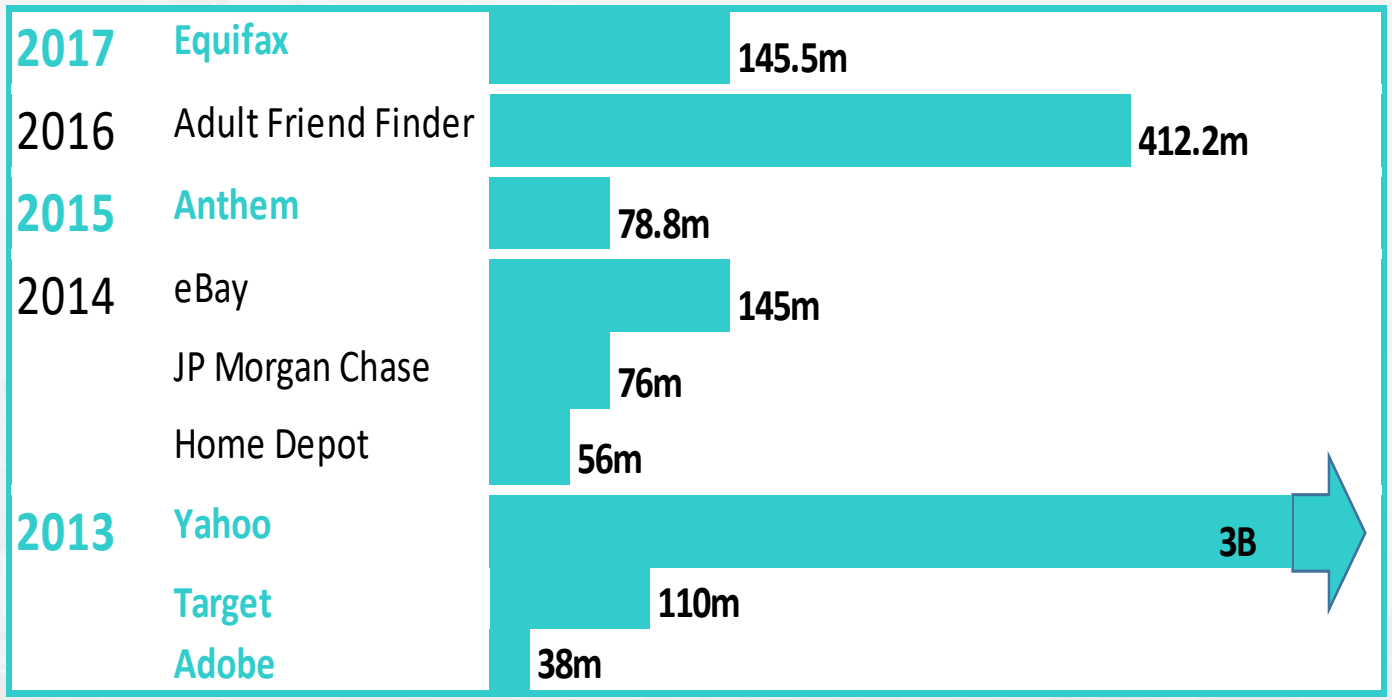
Areas of Concern

- Hacking
  - Malware
- Phishing
  - Social Engineering
  - Ransomware
- Cyber Threats
  - Public Wi-Fi
  - Account Takeover
  - Password Safety

Hacking — Definition

- Subverting computer or network security for malicious purposes
- Loss of personal information to hackers = data breach
- Includes Malware
  - "Malicious Software" -- Software that is intended to damage or disable computers and computer system
  - Introduced to target computer via executable code, scripts, other software. Types of code:
    - Viruses, worms, Trojan horses
    - Spyware, adware, scareware

Impact of Equifax and Other Breaches



The 17 Biggest Data Breaches of the 21st Century, by Taylor Armerding, Jan. 26, 2018, CSO Online.

What do hackers want?

- Your Identity
  - Name, Birthdate
  - Social Security Number
  - Email/Mailing Address
  - Phone Number
- Financial Information
  - Employment Data
  - Credit Card Data

Phishing — Definition

- Fraudulent attempt to obtain sensitive information such as usernames, passwords, credit card details
  - Social engineering is deceiving individuals into divulging PII
- Like fishing in that “bait” is used on victim (fake websites, social sites)
- Fraudster pretends to represent an official organization (IRS)
- Emails with “invoices” asking for a response

Phishing – How to spot a fake email

- Fake (“spoofed”) email address in header
- Urgent request
- “Click to learn more”
- Request to confirm account information
- Unexpected refund or prize
- Makes threats
- Poor grammar and spelling

Phishing — Ransomware Example

- Ransomware
- How TMRS protects against this type of attack

Cyber Threats

- Public Wi-Fi
- Account Takeover
- Password Safety

Public Wi-Fi


PUBLIC WIFI
We live in a world where public WiFi is nearly everywhere. But here's the thing about public WiFi: it's public.
When using public WiFi, everything you do can be intercepted.
This means passwords, user IDs, banking creds, emails and more.


Connect with care
Switch off your Wi-Fi and Bluetooth connections when not in use to help prevent malicious parties from connecting to your device without your knowledge. If you're banking or shopping, remember, a 3G or 4G connection is safer than an unsecured Wi-Fi connection.

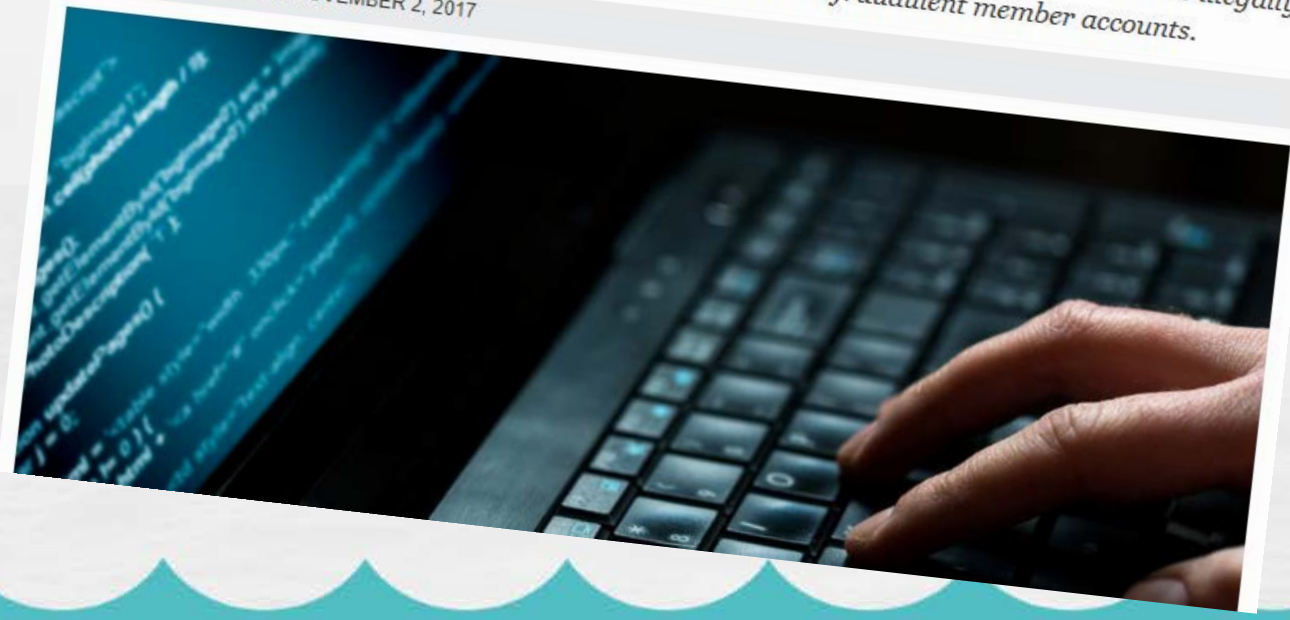
Account Takeover

No paycheck: Retirees' accounts compromised after data breach

[redacted] Employee Pension Accounts Compromised, Security Practices Scrutinized

Officials at a public employees pension fund are investigating how thieves were able to use illegally acquired Social Security numbers and dates of birth to create fraudulent member accounts.

BY THEO DOUGLAS / NOVEMBER 2, 2017



Password Safety

Security Features of MyTMRS® and the City Portal

- Multifactor authentication
- Complex passwords and challenge questions
- I am not a robot
- City Portal User Agreement

What Can Cities Do?

- Educate yourselves, and schedule training for employees
- Don’t share passwords and keep them safe
- Encourage members to create MyTMRS accounts
- Update your TMRS authorized contacts
- Don’t assume; ask questions

The biggest part of the struggle against fraud and cybercrime is increasing awareness by educating users.

Free Training Resources

- Training RE phishing for small organizations (PhishMe was acquired by Cofense, but still has a free tier) https://cofense.com/free/
- Free SANS resources (also recommend subscribing to their free OUCH! newsletter): https://www.sans.org/security-awareness-training/resources
- Basic tips and advice: https://www.stopthinkconnect.org/
- RSA Conference external resources (links to general security awareness information) https://www.rsaconference.com/about/rsac-cyber-safety/external-resources
- Some basic personal awareness/phishing tests:
  http://www.pewinternet.org/quiz/cybersecurity-knowledge/

  https://www.opendns.com/phishing-quiz/

  https://www.sonicwall.com/en-us/phishing-iq-test-landing

Where to Report

- City IT Department
- TMRS Help Desk
- IRS Scam phishing@irs.gov
- Identity Theft https://www.treasury.gov/services/report-fwa/Pages/id_theft.aspx
- Consumer Fraud https://www.consumer.gov/section/scams-and-identity-theft
- Scams and Frauds https://www.usa.gov/stop-scams-frauds

Questions ?

Presentations available at www.tmrs.com/ats.php