



CML's 95th Annual Conference
June 20 - 23, 2017
Breckenridge

The contents of this presentation reflect the view of the presenter, not of CML.



Local Governments and Cybersecurity Threats

Mark Turnage, CEO OWL Cybersecurity
www.owlcyber.com

The contents of this presentation reflect the view of the presenter, not of CML.



Cybersecurity in the News

Anthem: Hacked Database Included 78.8 Million People


Target Says Credit Card Data Breach Cost It \$162M In 2013-14

JPMorgan fell victim to the largest theft of customer data from a financial institution in US history

Sony Pictures Hacked And Blackmailed

OPM Hack: Government Finally Starts Notifying 21.5 Million Victims

The contents of this presentation reflect the view of the presenter, not of CML.



What is happening in cybersecurity, and why is it accelerating now?

- Open access to computer systems + the internet
- Only recent growing awareness of risks (Windows XP and Windows 7!)
- Continually increasing number of targets as internet usage explodes
- Criminals are getting smarter + sharing information with each other
- Nation state participation in cybercrime

The contents of this presentation reflect the view of the presenter, not of CML.



The "Internet of Things" will only accelerate these trends

20.8 billion devices predicted to be connected by 2020 (Gartner, Inc.)



Image source: Pixabay

The contents of this presentation reflect the view of the presenter, not of CML.



What can local governments do about it?

A lot.

The contents of this presentation reflect the view of the presenter, not of CML.



Let's think about just a personal few attack vectors:

- Passwords
- Social media
- Social engineering
 - Phishing
 - Spear phishing
- Wifi

The contents of this presentation reflect the view of the presenter, not of CML.



Passwords



The contents of this presentation reflect the view of the presenter, not of CML.



Top 10 Passwords in the U.S.

- | | |
|-------------|--------------|
| 1. 123456 | 6. 123456789 |
| 2. password | 7. football |
| 3. 12345678 | 8. 1234 |
| 4. qwerty | 9. 1234567 |
| 5. 12345 | 10. baseball |

Lesson: Enforce the use of complex passwords!
What is a complex password?

- Time to crack password "broncos" = less than 1 minute
- Time to crack password "Broncos1SuperBoWL_!!" = 100 years

The contents of this presentation reflect the view of the presenter, not of CML.



Digital Footprint



The contents of this presentation reflect the view of the presenter, not of CML.



Social Media



Lesson? Be careful what you post on social media

LIFE- Living Independently Forever
3 hours ago

We wish to announce that the two employees recently involved in the Arlington Cemetery incident are no longer employees of LIFE. Again, we deeply regret any disrespect to members of the military and their families. The incident and publicity has been very upsetting to the learning disabled population we serve. To protect our residents, any comments, however well-intentioned, will be deleted. We appreciate your concern and understanding as we focus on the care of our community.

The contents of this presentation reflect the view of the presenter, not of CML.



What is Social Engineering?

- The act of obtaining information via misdirection or lies.

The contents of this presentation reflect the view of the presenter, not of CML.



How does it happen?

- We want to be helpful.
- We respect authority.
- We fear repercussions.

The contents of this presentation reflect the view of the presenter, not of CML.



Phishing

- Phishing - A widespread social engineering campaign, usually carried out through Email, with the intention of getting people to click on a malicious link or open a malicious attachment.

The contents of this presentation reflect the view of the presenter, not of CML.



From: apple@icloud.com [mailto:apple@icloud.com] <apple@icloud.com>
 To: [redacted]
 Sent: Thursday, June 22, 2014, 10M 12:35 P
 Subject: Update your Account information



Dear iTunes Customer

Your iTunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

[Get Started](#)

If you need help logging in, go to our Help left by clicking the Help link located in the upper right-hand corner of any Apple page.

Sincerely,
 Apple Inc.

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.
 Copyright 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.



Let's take it apart:



The contents of this presentation reflect the view of the presenter, not of CML.

From: Apple [mailto:apple@apple.com] Sent: Thursday, April 24, 2014, 12:35 PM
Subject: Update your Account Information



Dear iTunes Customer:

Your iTunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

If you need help, click on the Help link located in the upper right-hand corner of the page.

Sincerely,
Apple Inc.

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help site by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131



The contents of this presentation reflect the view of the presenter, not of CML.

From: Apple [mailto:apple@apple.com] Sent: Thursday, April 24, 2014, 12:35 PM
Subject: Update your Account Information



Dear iTunes Customer:

Your iTunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

If you need help, click on the <http://go.apple.com/itunes/verify> link located in the upper right-hand corner of the page.

Sincerely,
Apple Inc.

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help site by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131



The contents of this presentation reflect the view of the presenter, not of CML.

Spear Phishing

- Spear Phishing - A sophisticated phishing attack targeting specific individuals. Spear phishing attacks are initiated only after extensive research on the target. The goal of spear phishing is often theft.

The contents of this presentation reflect the view of the presenter, not of CML.



How they do it.

- Research the Company
- LinkedIn, Twitter, Facebook
- Searching Company Website
- Build the Email

The contents of this presentation reflect the view of the presenter, not of CML.



Email

The screenshot shows an email interface with the following elements:

- Sender: [Red box]@org (labeled "CEO proper Email account")
- Recipient: [Red box] (labeled "Head of HR")
- Subject: 2015 WAGES
- Body: I want you to send me the list of W-2 copy of our employees wage and tax statement for 2015 for a very quick review and budget purposes. I need them in PDF file type and please respond ASAP.
- Signature: Thanks


The contents of this presentation reflect the view of the presenter, not of CML.



Email

- Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.
- I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.
- Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).

The contents of this presentation reflect the view of the presenter, not of CML.



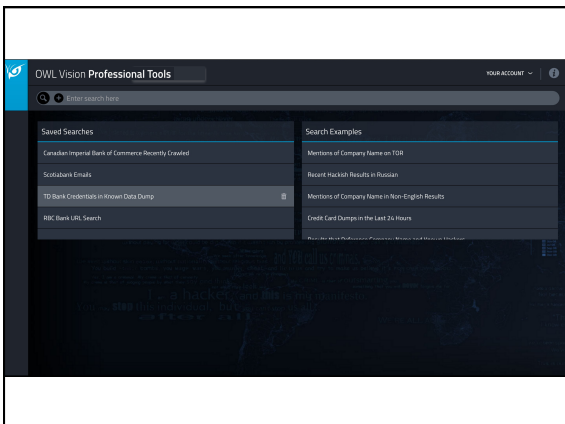
Be careful using public Wifi!

- NEVER use public wifi for banking or retail transactions. NEVER!
- Use VPNs if you are comfortable doing so
- Do not use autoconnect to unknown networks
- Make sure firewalls are up to date!



The contents of this presentation reflect the view of the presenter, not of CML.






The screenshot shows the OWL-Vision Professional Tools interface. It features a search bar at the top with the text "Enter search here". Below the search bar, there are two columns of search results. The left column is titled "Saved Searches" and lists several search queries, including "Canadian-Imperial Bank of Commerce Security Created", "Skatobare Emails", "TD Bank Credentials in Intranet Data Dump", and "RBC Bank USA Search". The right column is titled "Search Examples" and lists search results such as "Members of Company Name on TOR", "Recent Russian Results in Russian", "Members of Company Name in Non-English Results", and "Credit Card Dumps in the Last 24 Hours".

Implications for Local Governments

- **Be prepared!**
- Incident Response Plan
 - What is your incident response plan?
 - Who is responsible for what elements of that plan? What if they are on vacation?
 - When was the last time you conducted a full tabletop exercise to test your plan?
 - What is your PR strategy if you are breached? What if you are breached during an election?


The contents of this presentation reflect the view of the presenter, not of CML.



Implications for Local Governments

- Have you conducted a full security assessment recently?
 - If so, did you remediate the deficiencies identified?
 - What is your ongoing cybersecurity plan with respect to technology, software upgrades, endpoint protection and devices?
- Pentest
 - When was the last time you had someone external to your IT/security team pentest your network?

The contents of this presentation reflect the view of the presenter, not of CML.



Implications for Local Governments

- Policies and procedures
 - External devices/BYOD
 - Best email practices
 - Mandatory password reset policies
 - Data at rest—is it encrypted?
 - Data in transit—is it encrypted?
 - New technology introduction and overall planning
- Education
 - Your weakest link is your people.....you cannot educate enough. **If you do nothing else, do this.**

The contents of this presentation reflect the view of the presenter, not of CML.

