



Cyber Security Update for Economic Forum

Mike Vahle
CIO - Sandia National Laboratories
February 24th, 2015



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



LICENSED APPLICATION END USER LICENSE AGREEMENT

The Products transacted through the Service are licensed, not sold, to You for use only under the terms of this license, unless a Product is accompanied by a separate license agreement, in which case the terms of that separate agreement will govern, subject to Your prior acceptance of that separate agreement. Application Provider ("Application Provider") reserves all rights not expressly granted to You. The Product is licensed to You by Application Provider under this license as the "Licensed Application."

a. Scope of License: This license granted to You for the Licensed Application is a non-transferable license to use the Licensed Application on any iPhone or iPod touch device that You own or control, as permitted by the Usage Rules set forth in Section 9.b. of the App Store Terms of Service. The App Store Terms of Service license does not allow You to use the Licensed Application on any iPod touch device that You do not own or control. You may not copy (except as expressly permitted by this license), reverse engineer, disassemble, attempt to derive the source code of, modify, or create derivative works of the Licensed Application, any updates, or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or to the extent as may be permitted by the licensing terms governing use of any open source components included with the Licensed Application). Any attempt to do so is a violation of the law and will subject to prosecution and damages. The terms of this license will govern any upgrades provided by Application Provider to the Licensed Application or to any other Product, unless such upgrade is accompanied by a separate license in which case the terms of that separate license will govern.

b. Consent to Use of Data: You agree that Application Provider may collect and use information, including but not limited to technical information about Your device, screen and application software and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to You (if any) related to the Licensed Application. Application Provider may use this information, as long as it is in a form that does not personally identify You, to improve its products and services and to better understand its users.

c. Termination. The license is effective until terminated by You or Application Provider. The license will terminate automatically without notice from the Application Provider if You fail to comply with any provisions of this license. Upon termination of the license, You shall cease all use of the Licensed Application.

d. Services; Third Party Materials. The Licensed Application may enable You to access and use third party services and web sites (collectively and individually, "Services"). Use of the Services is subject to the terms and conditions of the applicable service provider's terms of service.

To continue with this installation, you must accept the terms of the End-User License Agreement. If you do not accept the agreement, click the checkbox below.

I accept the terms in the License Agreement

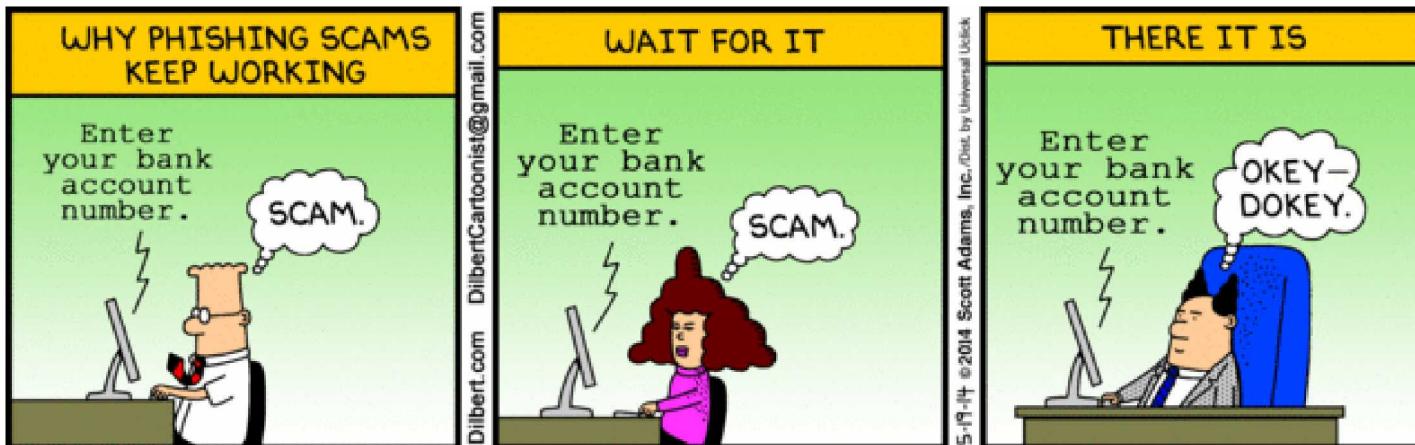
<< Back

Next >>

Cancel

About Phishing

- “Phishing” is the practice of using electronic communication to manipulate a target into doing something counter to the target’s interests.



Maintenance Issues



Things are not always as they appear



Example Email -Phishing



Greetings from [Amazom.com](#),

We wanted to notify you that an [Amazom.com](#) Gift Card was sent to you on 9 Dec 2013 16:04:40 GMT.

Details:

Order # 314-2520202-8371419 from 9 Dec 2013 10:49:24 GMT

Sent to:

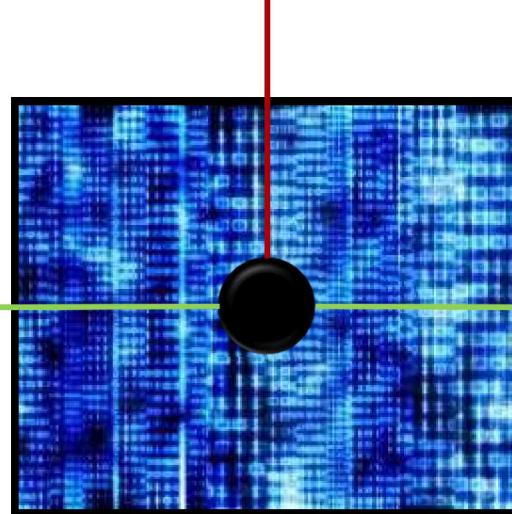
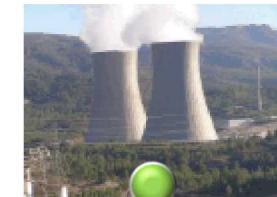
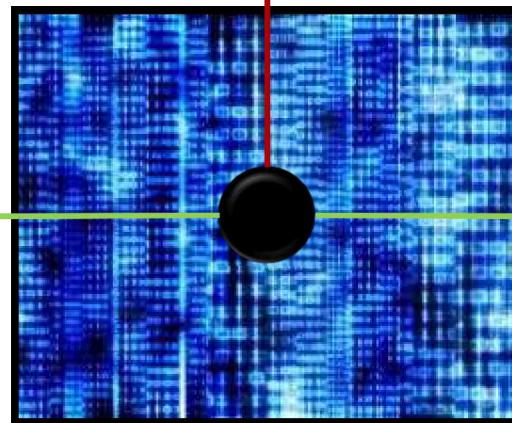
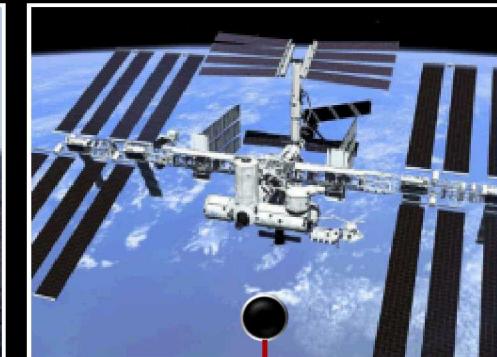
Message: **Happy Early Holidays!**

[Click here](#) to redeem your gift card.

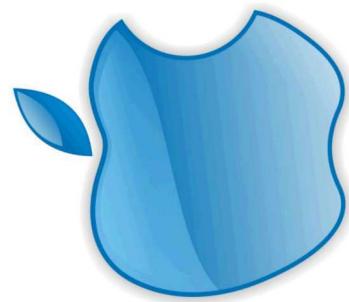
Please note: This e-mail was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.



The “Internet of Things” is the 5th domain of conflict



Recent Cyber Events Impacting Business



Cyber Theft of Intellectual Property

- The Center for Strategic and International Studies (CSIS) produced a study in June 2014 which estimates that cybercrime costs business approximately \$445 billion annually worldwide. The cost is about 200,000 U.S. jobs annually.
- Cybercrime is a tax on innovation. In 2013, CSIS researchers found that the United States notified 3,000 companies that they had been hacked. CSIS estimated that the United States lost about \$100 billion.



Zero-Day Threat

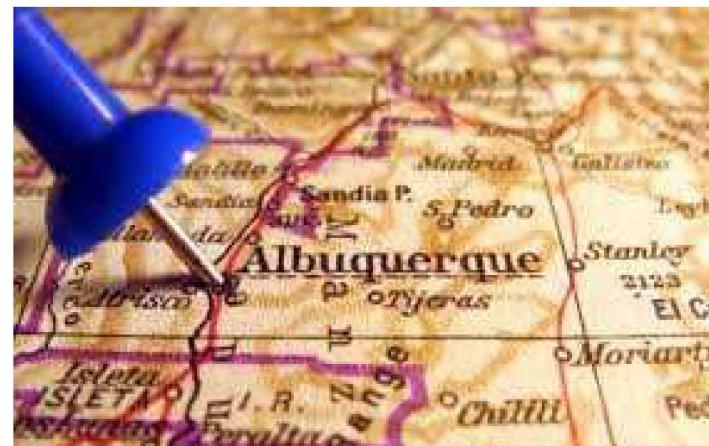


Advanced Persistent Threat (APT)



Today's Threat Environment

- Threats are real; even in Albuquerque.
Example: Attack on Journal Web Site – January 2015



Today's Threat Environment

Ideological Movements



Organized Crime



Nation States



Sony PlayStation Network Shut Down
'Indefinitely' Following Attack 5/11

Home Depot is hacked -
initial estimates exceed
Target loss 8/14

Mandiant releases APT1 –
calls out China for cyber
espionage 2/13

A win for the good guys...
FBI/Microsoft team to shut
down \$500M botnet 6/14

Ebay Hacked – 1000s of
Accounts Deleted, Auctions
Vanished, Millions Lost 9/14

Russian PM's
twitter account is
hacked 8/14

Target's point of sale system
yields financial data of 40M
12/13

Hacked ATMs net cyber
criminals \$45M 5/13

PII of 100,000+ is stolen
from DOE 7/13

RSA security firm hit by
'sophisticated' hackers 3/11

HeartBleed – secure web browsing
compromised, impacts 75% of internet 4/14

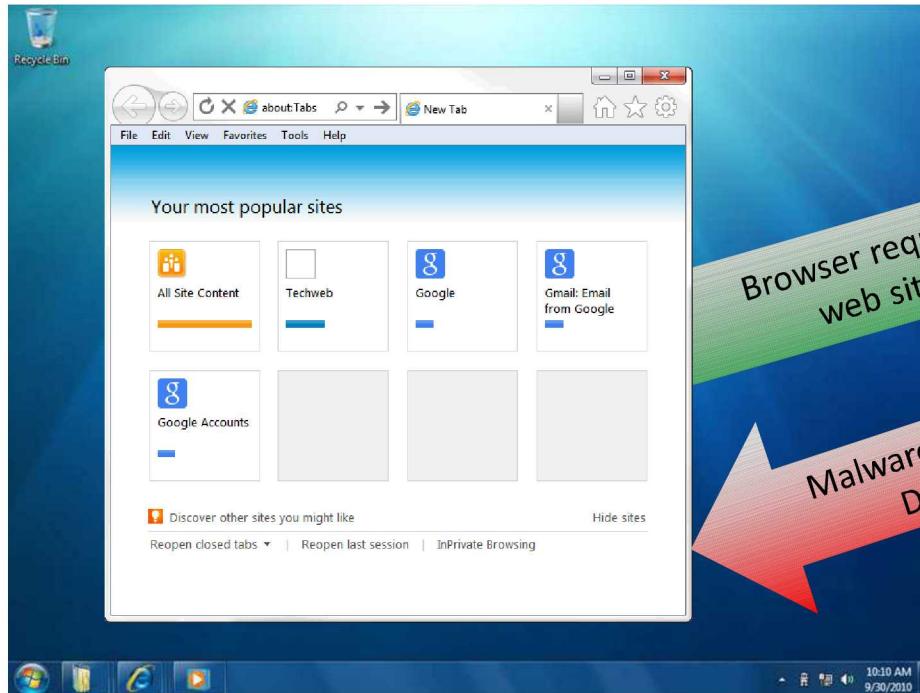
OPM is hacked – security
clearance info taken 7/14

Apple iCloud gives up personal
Information and photos 8/14

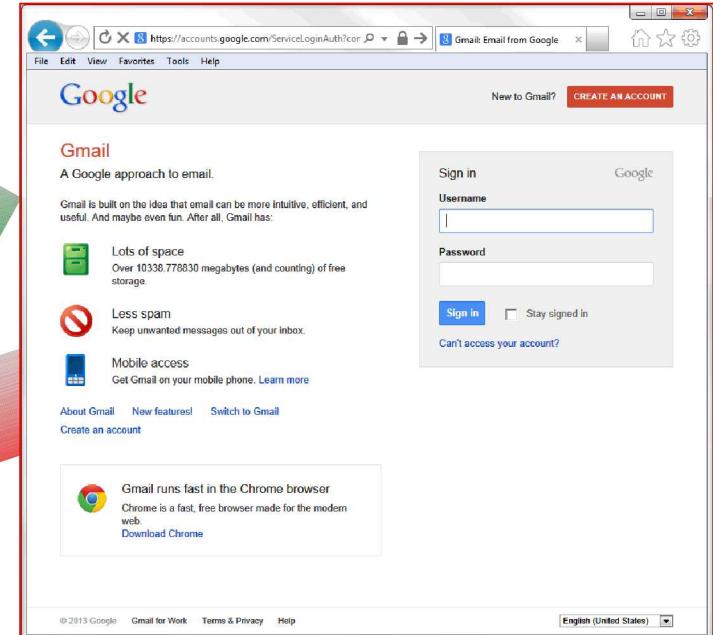
Typical Desktop Configuration

How it works

Desktop Computer - Trusted



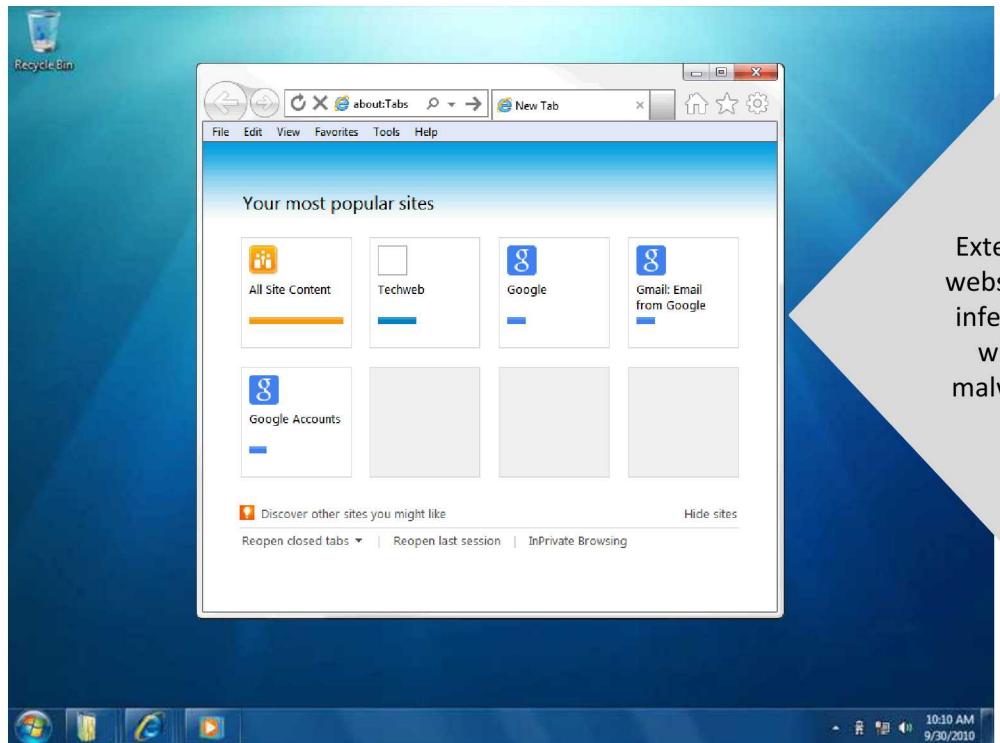
Outside Web Browser - Unsecure



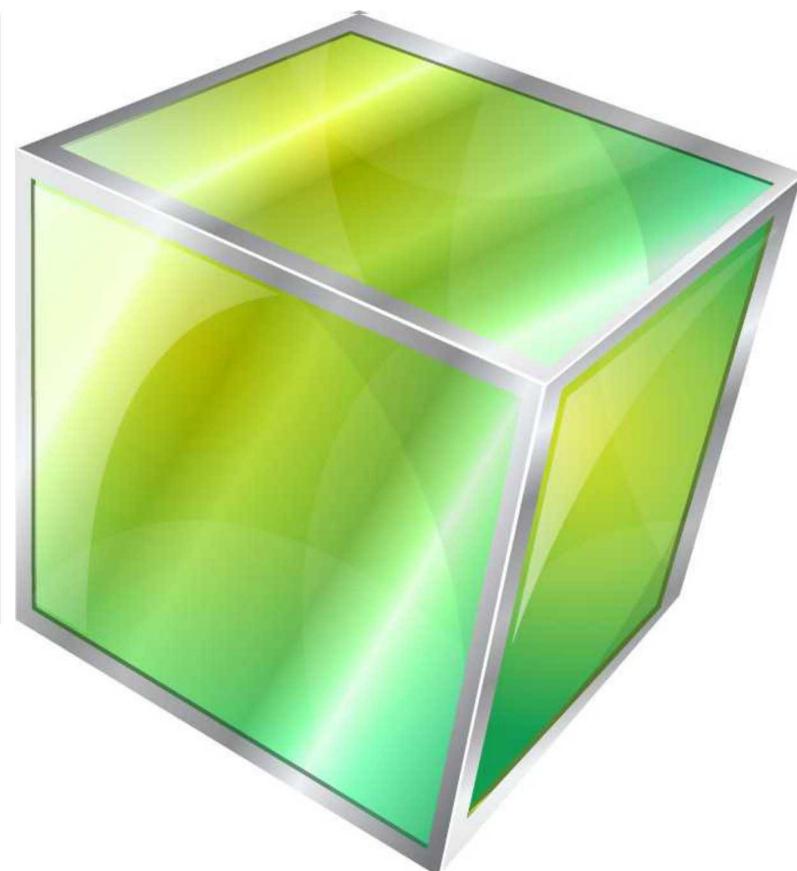
- Huge attack surface
- We can only protect against known attack vectors
- Virus is downloaded onto the trusted computer

Micro-Virtualization as a Security Solution

Desktop Computer - Trusted



Outside Web Browser - Untrusted



External website is infected with malware

Future: Vehicle To Vehicle (V2V)



Backup Slides