

System and User Security for PMP Systems September 25, 2009

5th National Harold Rogers
PDMP Meeting



BruckEdwards, Inc.

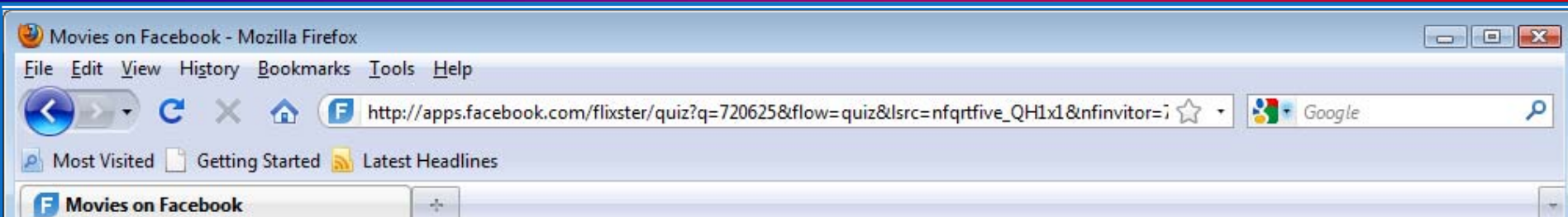
*Secure, Compliant,
Process Improvement*

Agenda

- Introduction
- Balancing Security Usability
- Data Breach Lessons Learned
- Remote Access Authentication Lifecycle
- Available Controls

- **Processes have resisted automation because...**
 - *reliance on paper*
 - *dependence on a human signature*
 - *involve sensitive information*
- **Leverage advanced technologies to enable E-Government processes**
 - Identity and Access Management
 - Information sharing and collaboration
- **Combine technology and policy expertise to:**
 - Improve operational efficiency
 - Reduce fixed and variable costs
 - Improved system security
 - Facilitate information sharing

Internet Security Pop Quiz



Question 1

Which is a data breach?



- Cool pants with a built in 32GB Cruiser
- Someone took your data & you know about it
- Someone took your data & you don't know about it

Sponsored Links

[Find Out Peoples Password](#)
Remote Monitoring Password Finder.
View Other Peoples Passwords, \$89
www.RemoteSpyware.com

Question 2

Why is this guy relevant?



- He spends too much on birthday parties?
- He stole 45 million card numbers from TJ Maxx
- He stole 130M card numbers from Heartland Payment systems

[Is Your Spouse Cheating?](#)

Find out what your spouse or children are doing online!
www.needapassword.com

[Find Email Passwords](#)

Record all passwords with PC Magazine Editors' Choice.
www.SpectorSoft.com

Question 3

Hacking an email password is a?



- Poor manners
- A misdemeanor
- A felony

Submit Answers

Note: you will need to add the application to save your results.

How do you provide...

- ✓ Remote access
- ✓ Ease of use

While ensuring that...

- ✓ Data at rest is secure
- ✓ Data in motion is secure
- ✓ Only authorized users are granted access

To maximize...

- ✓ Adoption
- ✓ Return on Investment (ROI)



High Profile Data Breaches...

and Lessons Learned

What is a Breach?

Section 13400, American Recovery and Reinvestment Act of 2009—

"the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

Proposed Section 318.2 FTC regulations—

"with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information."

The state of California was the first state to require that institutions notify individuals that their personal information had been compromised as a result of a data breach. Breach is defined in California Civil Code, §1789.82 (d)

Recent Data Breach Incidents



The Washington Post
June 4, 2006
Navy, Guard Personnel's Data Among Those Lost

cnet news
January 18, 2007
T.J. Maxx hack exposes consumer data.

The Washington Post
January 21, 2009
Firm Reports Massive Data Breach From Credit Transactions

The Washington Post
June 22, 2006
VA to Offer Credit Monitoring; 1 Year of Service Free To Data-Theft Victims

msnbc
March 30, 2007
T.J. Maxx theft believed largest hack ever.

The Washington Post
February 3, 2009
Data Breaches Are More Costly Than Ever

The Washington Post
July 1, 2006
Thieves' Indifference May Mean VA Laptop's Data Is Secure

Los Angeles Times
August 06, 2008
11 charged in largest ID theft in U.S. history

eWEEK.COM
August 28, 2006
Hacker Agrees to Guilty Plea in Massive Data Breach Case



UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

2006



2007



2009

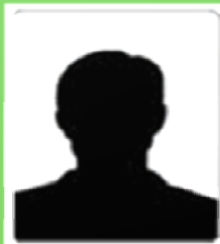
Impacts... Don't ignore them

Notice of suspected or confirmed breach



Data setup
Print merge
Postage

Account Lockout / Reset
Administration
Provisioning



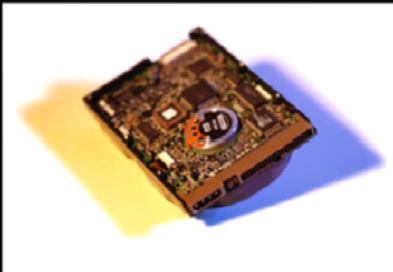
DOE
JOHN, W

Identity/Credit Monitoring



\$15 per month

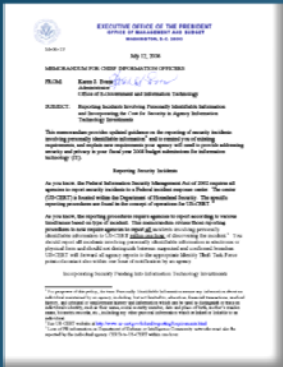
Data Analysis/Forensics



Card Reissuance

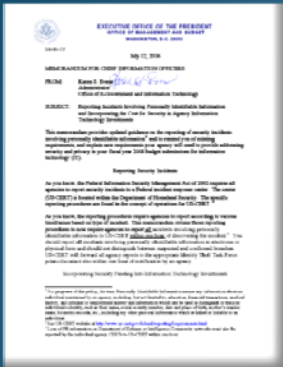


Printing
Postage



OMB Memorandum M-06-16 Protection of Sensitive Agency Information Released on June 23, 2006.

- ❑ Guidelines for the protection of sensitive information located on federal agency computers and networks.
- ❑ Recommends that all data on mobile computers be encrypted, remote access to agency networks require two-factor authentication, a time-out function be applied for remote access of networks, and that all data extracts holding sensitive information be deleted within 90 days of their receipt, unless there is a need to keep them longer.

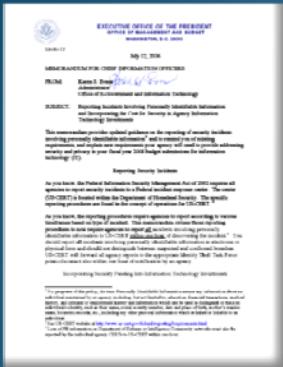


OMB Memorandum M-06-19 Released on July 12, 2006.

- Guidelines for reporting incidents where loss of PII is confirmed or suspected.

- All incidents involving PII must be reported to the DHS Incident Response Center (US-CERT) within one hour of their discovery. Within one hour, US-CERT passes the information on to the appropriate Identity Theft Response Team.

- The agency making the initial report is not to distinguish between confirmed or suspected PII breaches.



OMB Memorandum M-07-16 Released on May 22, 2007.

- Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Breach Notification Policy.
- Agencies must develop breach notification policy.
- External Breach notifications (Determining “Harm”)
 - Nature of the data elements
 - Number of individuals affected
 - Likelihood that information is accessible and usable
 - Will it lead to harm?

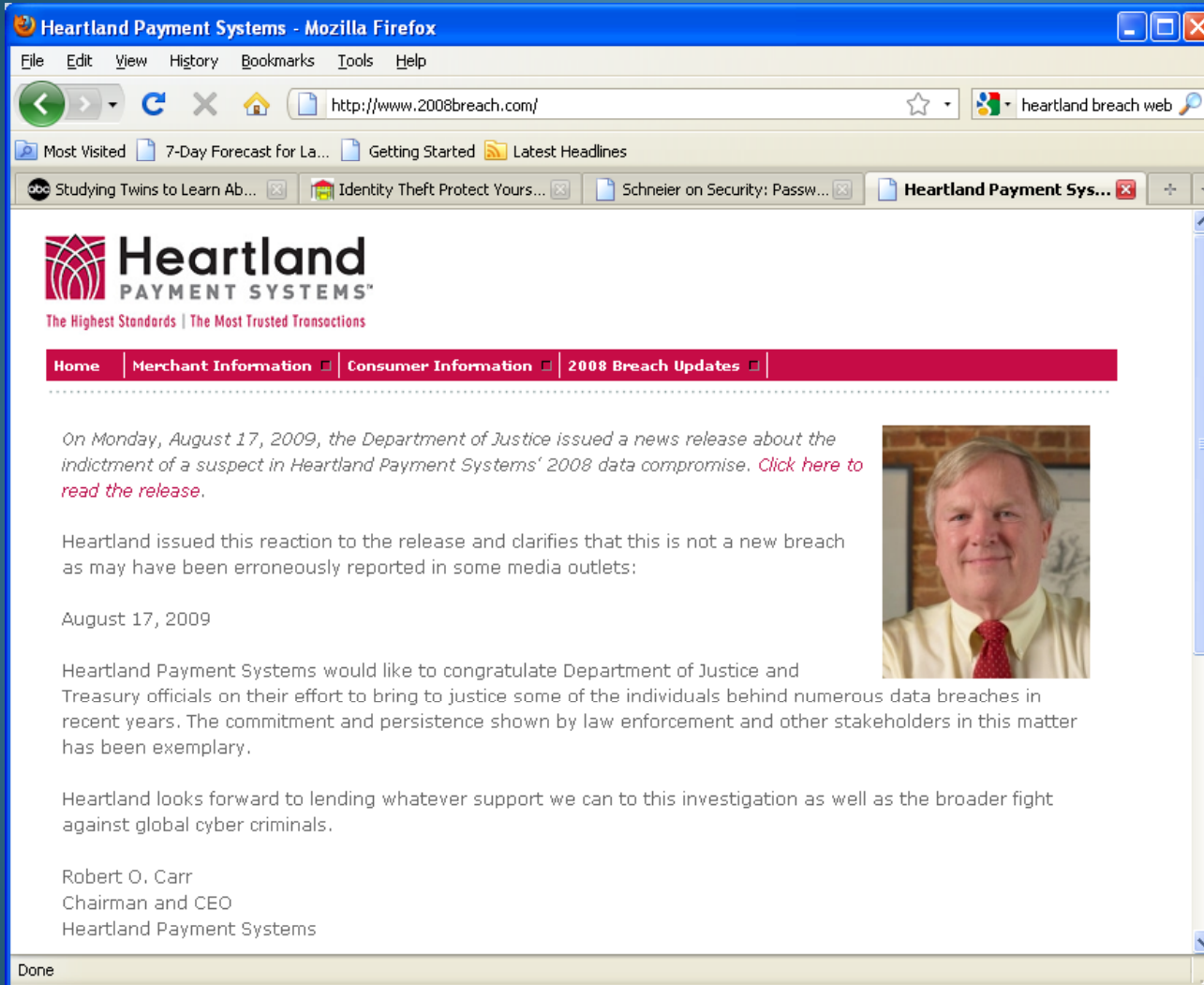
Communication Guidelines for merchants

1. Consider a Breach Likely — and Prepare Accordingly
2. Be Accurate And Be Fast
3. Be Open, Honest and Transparent
4. Be Accountable — Always
5. Get the Word Out – Be Thorough



"The key lesson of the [major retailer] security breach, may be that it is impossible to prevent data crimes against the card system. The ease of access to valuable consumer information, the considerable rewards for stealing it, the failure of law enforcement to prevent it, and the increasingly prohibitive cost of protecting it all militate against any easy solution."

Heartland's approach



Heartland Payment Systems - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.2008breach.com/ heartland breach web

Most Visited 7-Day Forecast for La... Getting Started Latest Headlines

abc Studying Twins to Learn Ab... Identity Theft Protect Yours... Schneier on Security: Passw... Heartland Payment Sys...

Heartland
PAYMENT SYSTEMS™
The Highest Standards | The Most Trusted Transactions

Home Merchant Information Consumer Information 2008 Breach Updates

On Monday, August 17, 2009, the Department of Justice issued a news release about the indictment of a suspect in Heartland Payment Systems' 2008 data compromise. [Click here to read the release.](#)


Heartland issued this reaction to the release and clarifies that this is not a new breach as may have been erroneously reported in some media outlets:

August 17, 2009

Heartland Payment Systems would like to congratulate Department of Justice and Treasury officials on their effort to bring to justice some of the individuals behind numerous data breaches in recent years. The commitment and persistence shown by law enforcement and other stakeholders in this matter has been exemplary.

Heartland looks forward to lending whatever support we can to this investigation as well as the broader fight against global cyber criminals.

Robert O. Carr
Chairman and CEO
Heartland Payment Systems



Done

WWW.2008Breach.com

Key Lessons Learned

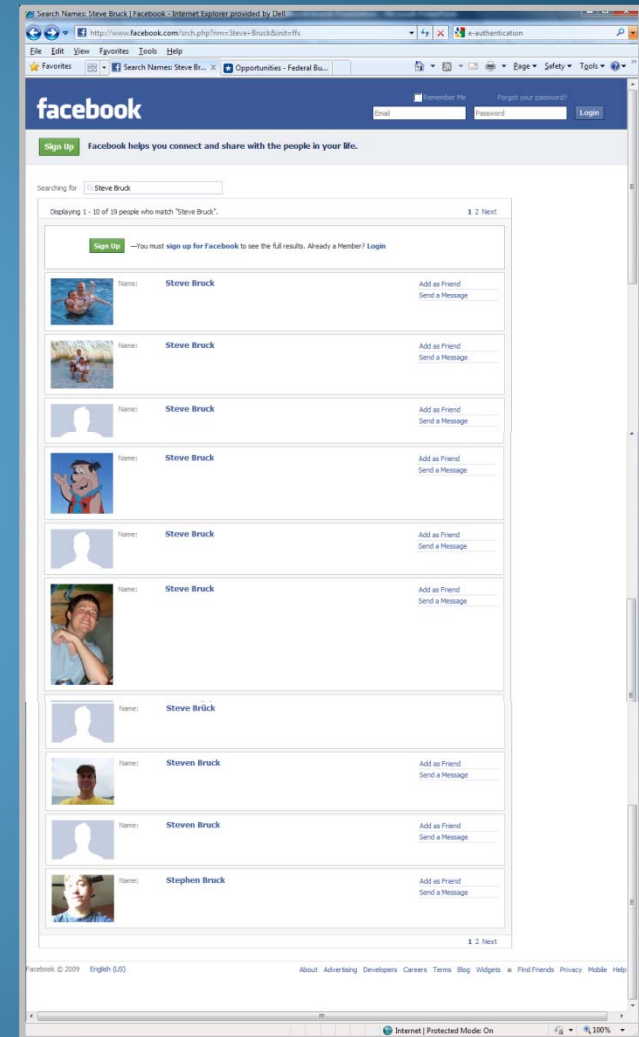
- Preparation for a breach and immediate response is essential
- A suspected event can be as damaging as a confirmed event
- The cost of a data breach can be quantified and used to justify budget/spending plans
- Secure data retention is key
 - Defense in depth
 - Leverage existing enterprise services (Perimeter, Patching, Backup)
 - De-identified data / encryption
 - Collection/pruning/grooming
 - Log files too!

E-Authentication and Identity Management

Authentication challenges include:

- ID proofing **Critical**
Registering/enrollment
- Provisioning / issuance
- Initial activation
- Administration / lost passwords
- Hacked accounts
- Identity Theft

“A Race to be second”



Multiple Service Delivery Channels
“Call, Click, or Visit”

Opt-in for authentication security

User experience is critical factor, corporations wants to be viewed as “mainstream”

And...

Security is used as a marketing tool

Bank of America 

WELLS FARGO



BB&T



AMERICAN EXPRESS

facebook

General Growth

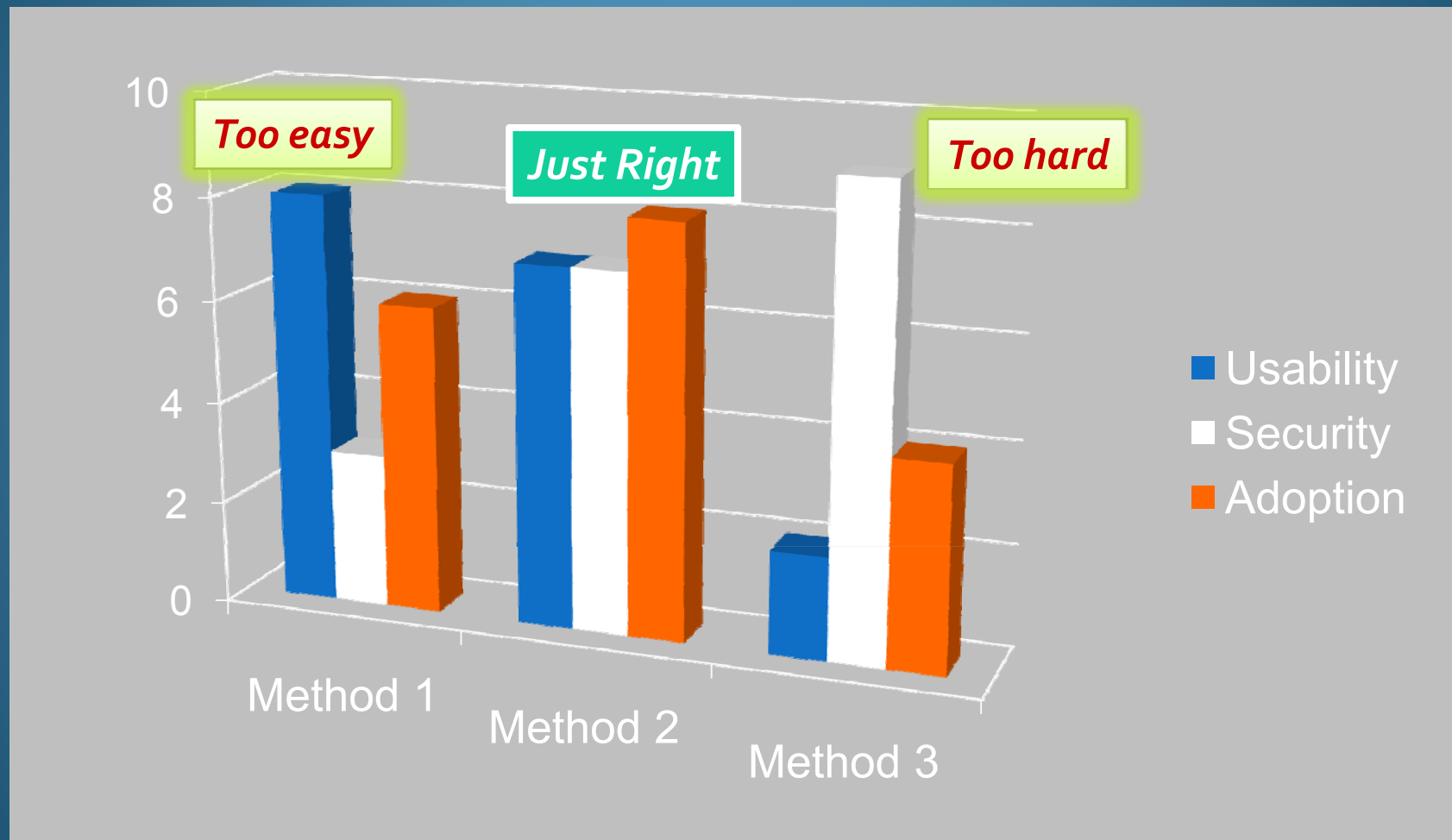
- More than 250 million active users
- More than 120 million users log on to Facebook at least once each day
- More than two-thirds of Facebook users are outside of college
- The fastest growing demographic is those 35 years old and older

User Engagement

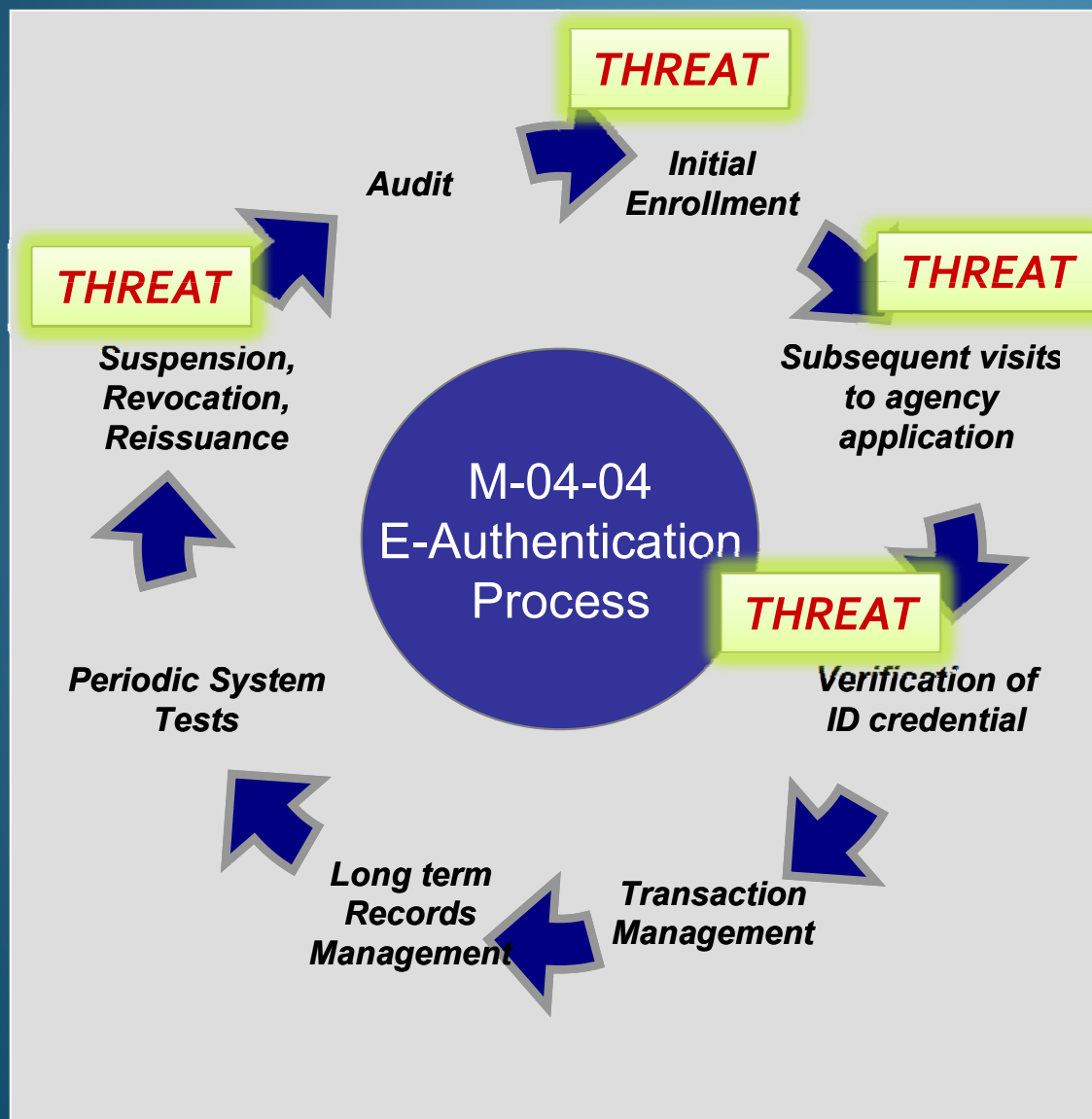
- Average user has 120 friends on the site
- More than 5 billion minutes are spent on Facebook each day (worldwide)
- More than 30 million users update their statuses at least once each day
- More than 8 million users become fans of Pages each day

 **amazon**
web services™

Getting Remote Access Right



Remote Access Lifecycle



- Adoption depends on usability
- E-Authentication analysis must include a strong focus on initial registration and identity proofing
- Convenience depends on flexibility and reusability

Threats: Phishing, Vishing, and Smishing



Internal Revenue Service

- Inheritance/Lotto winnings
- Tax Refunds



Dept. of Veterans Affairs

National Highway Transportation Safety Agency

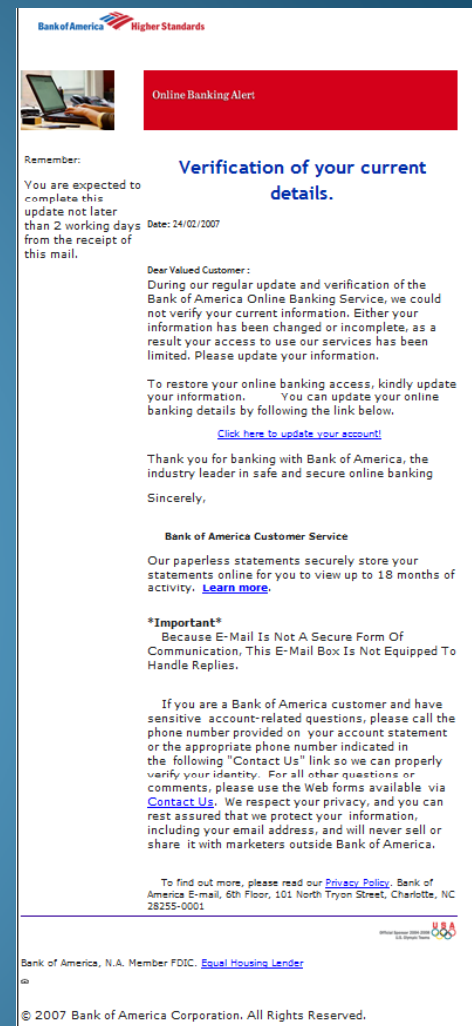


- Cash for clunkers websites



Facebook

- Collecting logon credentials



Threats "Password Hacking" and Malware



The image illustrates a phishing attack. It shows two overlapping web browser windows. The top window, titled "HACK EMAIL PASSWORDS SOFTWARE", displays the URL "http://www.passwordportal.net" and a yellow warning icon. The bottom window, titled "Need A Password", displays the URL "http://www.needapassword.com/" and a large, stylized "Need A Password" text. Below this text, it says "Click HERE to get it!" and "PLEASE READ". A large cyan sign with red text "CLICK HERE !!!!" is overlaid on the bottom window, pointing to the "Click HERE to get it!" text. The bottom window also contains the text: "If you enter this website with the above link and cannot view it, come back to this page and [click here](#)."

A few solutions...Today

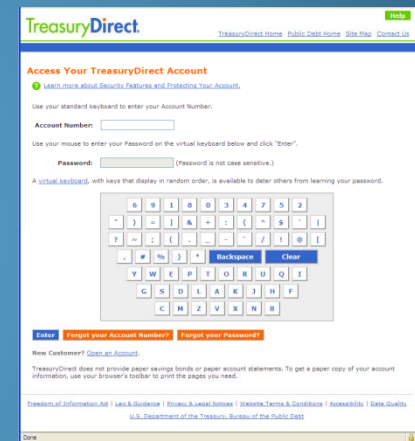
- Leverage in-person presentation as trust anchor
- Establish/maintain trusted communication channels with users— email, SMS, phone
- Keep the user informed...and allow “self policing”
 - Recent logons, Transactions
 - Change in communication channel address(es)
- Make your policies well known (We will Never...!)
 - To your users
 - To your trading partners
- Periodic independent assessment
- Stay vigilant

A few more solutions

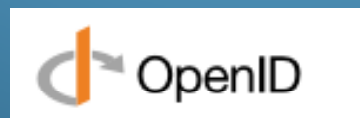
- Allow 2nd factor authentication mechanisms OTP



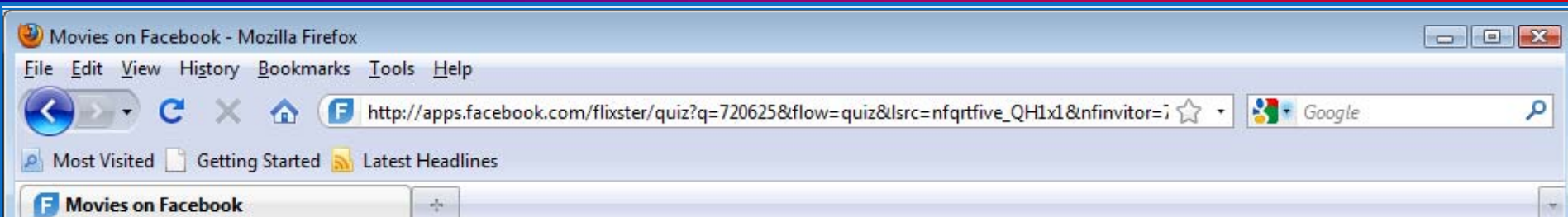
- Enable alternate input methods
- SSL
- Site Validation
- Extended Validation Certificates
- Challenge questions



- Or possibly ...



Internet Security Pop Quiz



Question 1

Which is a data breach?



- Cool pants with a built in 32GB Cruiser
- Someone took your data & you know about it
- Someone took your data & you don't know about it

Sponsored Links

[Find Out Peoples Password](#)
Remote Monitoring Password Finder.
View Other Peoples Passwords, \$89
www.RemoteSpyware.com

[Is Your Spouse Cheating?](#)
Find out what your spouse or
children are doing online!
www.needapassword.com

[Find Email Passwords](#)
Record all passwords with PC
Magazine Editors' Choice.
www.SpectorSoft.com

Question 2

Why is this guy relevant?



- He spends too much on birthday parties?
- He stole 45 million card numbers from TJ Maxx
- He stole 130M card numbers from Heartland Payment systems

Question 3

Hacking an email password is a?



- Poor manners
- A misdemeanor
- A felony

Submit Answers

Note: you will need to add the application to save your results.

Contact Information

Internet

Steve.Bruck@BruckEdwards.com

www.BruckEdwards.com

Offices

530B Huntmar Park Drive Suite G
Herndon, Virginia 20170

Tel: 703-286-5311 x101
Fax: 703-286-5312