#BeCyberSafe

David Pollino

Senior Vice President

Deputy Chief Security Officer

BANK OF THE WEST

BNP PARIBAS GROUP

About the Speaker

David Pollino

SVP, Deputy Chief Security Officer, Bank of the West

David Pollino, SVP, Deputy Chief Security Officer for Bank of the West, is responsible for fraud prevention oversight and education at the bank. Pollino was recently named a top ten influencer by Bank Information Security.

Prior to joining Bank of the West, Pollino served in senior fraud prevention positions for Wells Fargo, Washington Mutual, and Charles Schwab. During his career, Pollino has also worked as an information security consultant at @stake and UUNET advising Fortune 100 companies on information security issues.

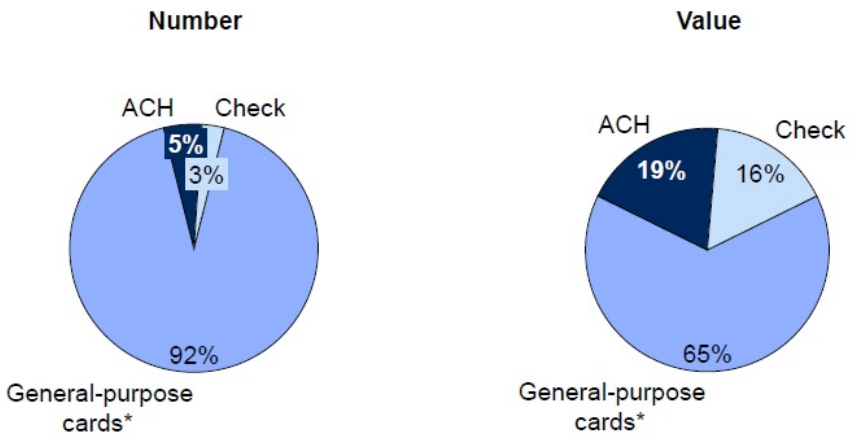
Pollino is the author of RSA Press: Wireless security, The Hacker's Challenge Books 1, 2 and 3, and Hacking Exposed: Wireless.

"You know, you can do this just as easily online."

Top 5 Fraud Threats

1. Card fraud
2. Online threats
3. Customer scams
4. New account
5. Internal Fraud

Exhibit 20: Distribution of unauthorized transactions (third-party fraud) in 2012



Figures may not add due to rounding.

*General-purpose cards include credit, debit, and prepaid purchases as well as ATM withdrawals.

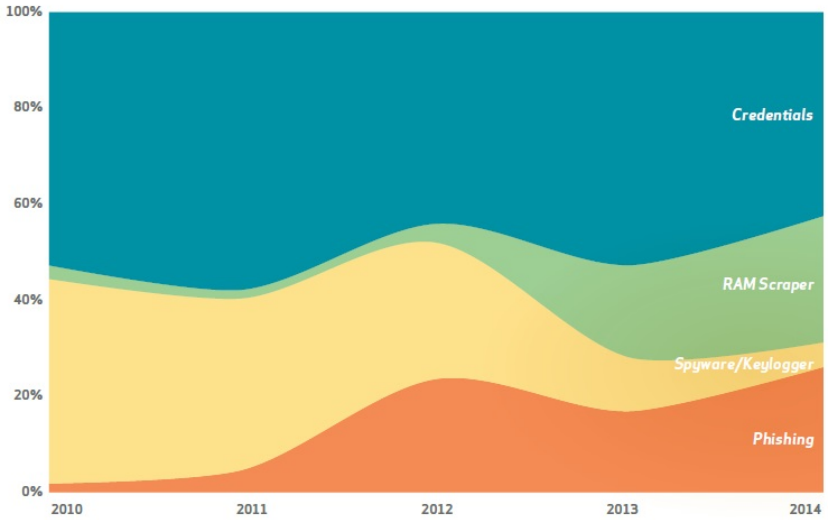
https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

Know Your Enemy

- Principle 6 - The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
  - **Nation-states and spies** — Hostile foreign nations who seek intellectual property and trade secrets for military and competitive advantage. Those that seek to steal national security secrets or intellectual property.
  - **Organized criminals** — Perpetrators that use sophisticated tools to steal money or private and sensitive information about an entity's consumers (e.g., identity theft).
  - **Terrorists** — Rogue groups or individuals who look to use the Internet to launch cyber attacks against critical infrastructure, including financial institutions.
  - **Hacktivists** — Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.
  - **Insiders** — Trusted individuals inside the organization who sell or share the organization's sensitive information
- Principle 13 - The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Source: COSO

Card Fraud – 2015 Verizon Breach Report

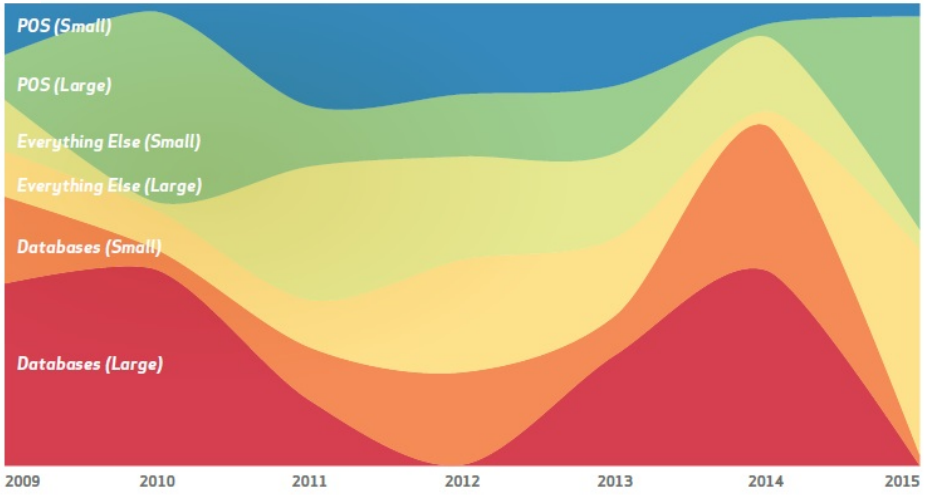


Ram scrapers

– "Your cash register has a virus"

Large Companies

– Big push before EMV



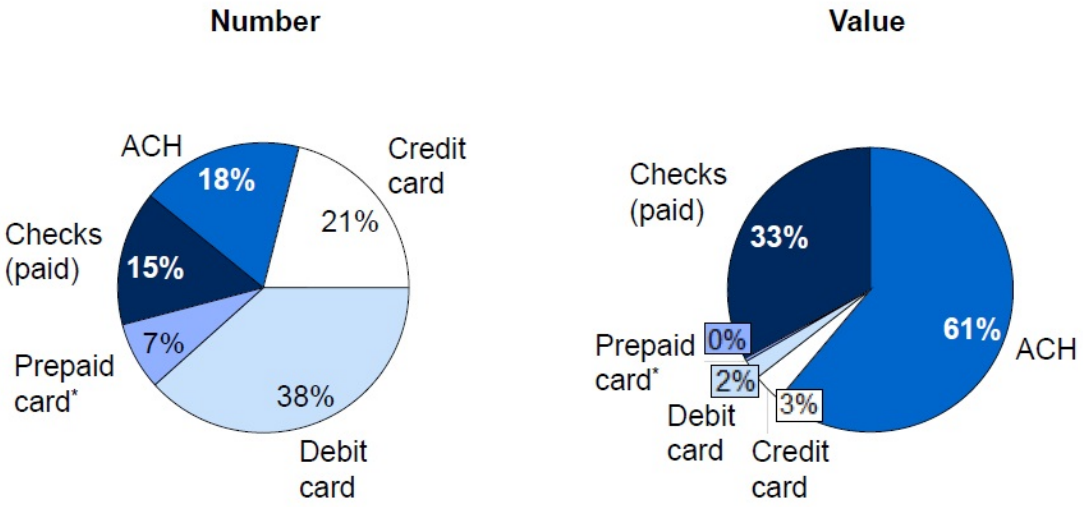
40 Yep, we did. That's how we roll. But, we're *really* fun at parties. Honest.

Current State – ACH Fraud

- "Cards are typically used for point-of-sale (POS) transactions largely because of their convenience, while ACH payments tend to be used primarily for bill payment, payroll, and other larger-value transactions."

- Current Schemes
  - Online Account Takeover
  - Bill payment fraud
  - Peer to peer payments
  - Masquerading

Exhibit 3: Distribution of noncash payments in 2012



https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

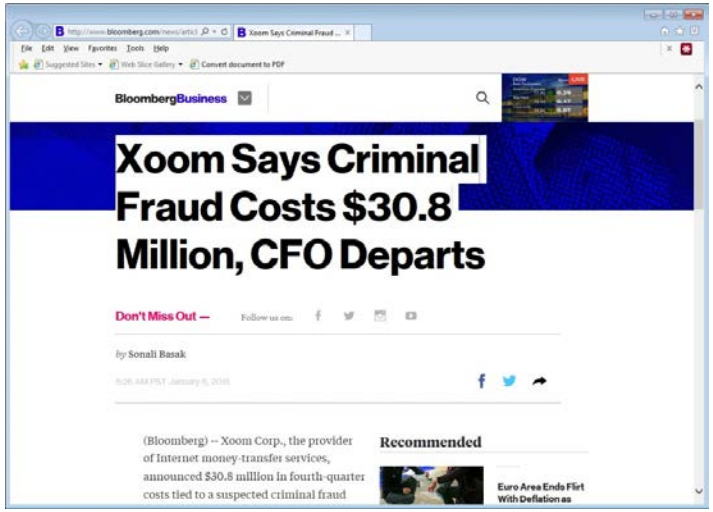
The Case of Efficient Services Escrow Group

- A suspected Trojan allowed hackers access to Efficient Services Escrow Group's computers. The hackers remotely initiated wire transfers to Russia and China on three separate occasions totaling $1.5 million.

Source: Krebs on Security; "$1.5 million Cyberheist Ruins Escrow Firm," http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

The Case of Efficient Services Escrow Group

- Efficient Services Escrow recovered only half of the funds and in March 2013, the firm was shut down by the California Department of Corporations.
- While the downfall of Efficient Services Escrow may have been due to its own shortcomings, the case sheds light on inadequacies of its Bank's security.

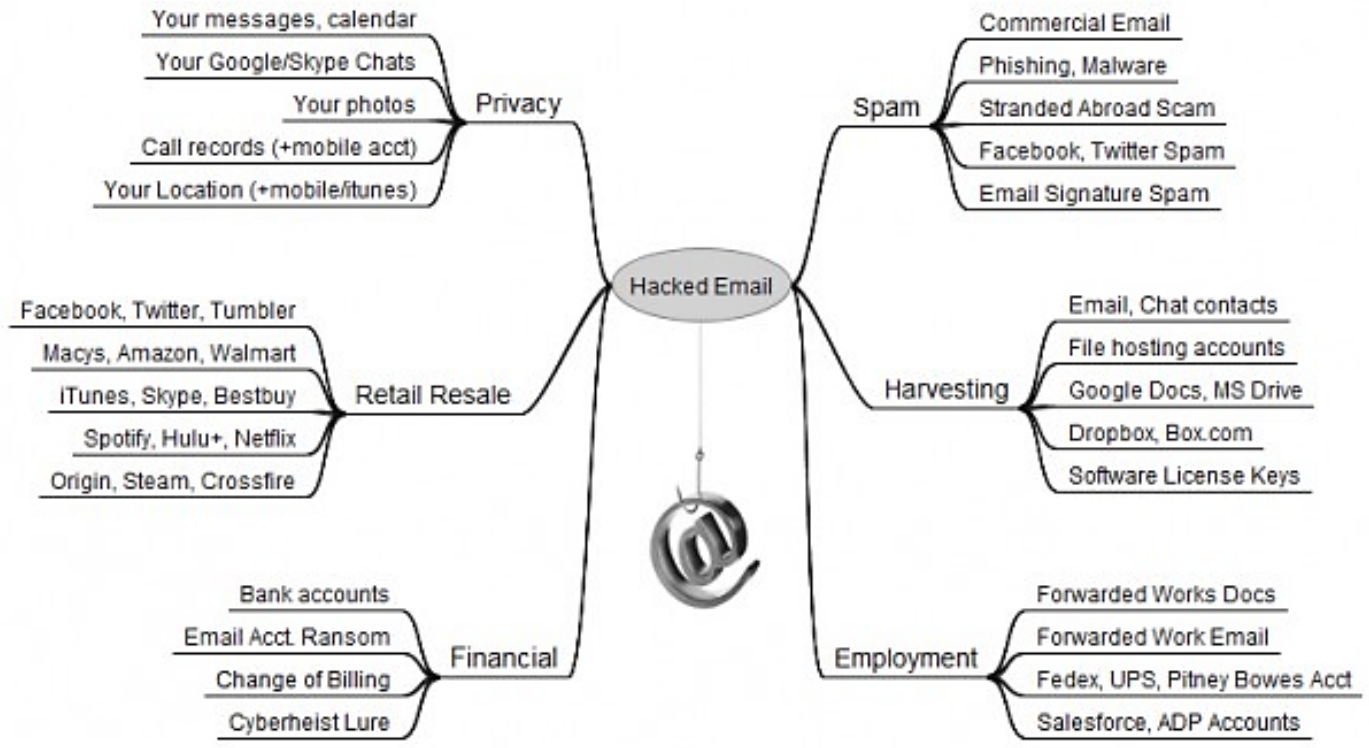


Source: Krebs on Security; "$1.5 million Cyberheist Ruins Escrow Firm," http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

What is Masquerading?

- Masquerading uses a combination of social engineering, phishing and computer intrusion tactics.
- Typically begins with a fraudster phishing an executive to obtain access to their email, or by emailing company employees using a similar email address or domain name that has very minor differences from the actual domain.
  - Ex: If the business domain is @bankofthewest.com. The fraudster might exchange “w” for 2 “v’s” and register @bankofthevvest.com
- Fraudsters impersonate a company executive or known vendor in order to entice a business to transfer money to a fraudulent account. They take time to learn about a company’s business relationships and understand how it operates in order to appear legitimate and convincing.
- The funds ultimately end up in a bogus account set up by the fraudster(s).
- Attacks are typically waged against commercial and small businesses, not the bank itself.
- Fraudsters have also started using masquerading to obtain sensitive employee or customer data such as income tax info, social security numbers, wages, etc.
- Also referred to as Business Email Compromise and CEO Fraud.

Hacked Email Data



Your email account may be worth far more than you imagine.

Source: http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Masquerading Loss Statistics

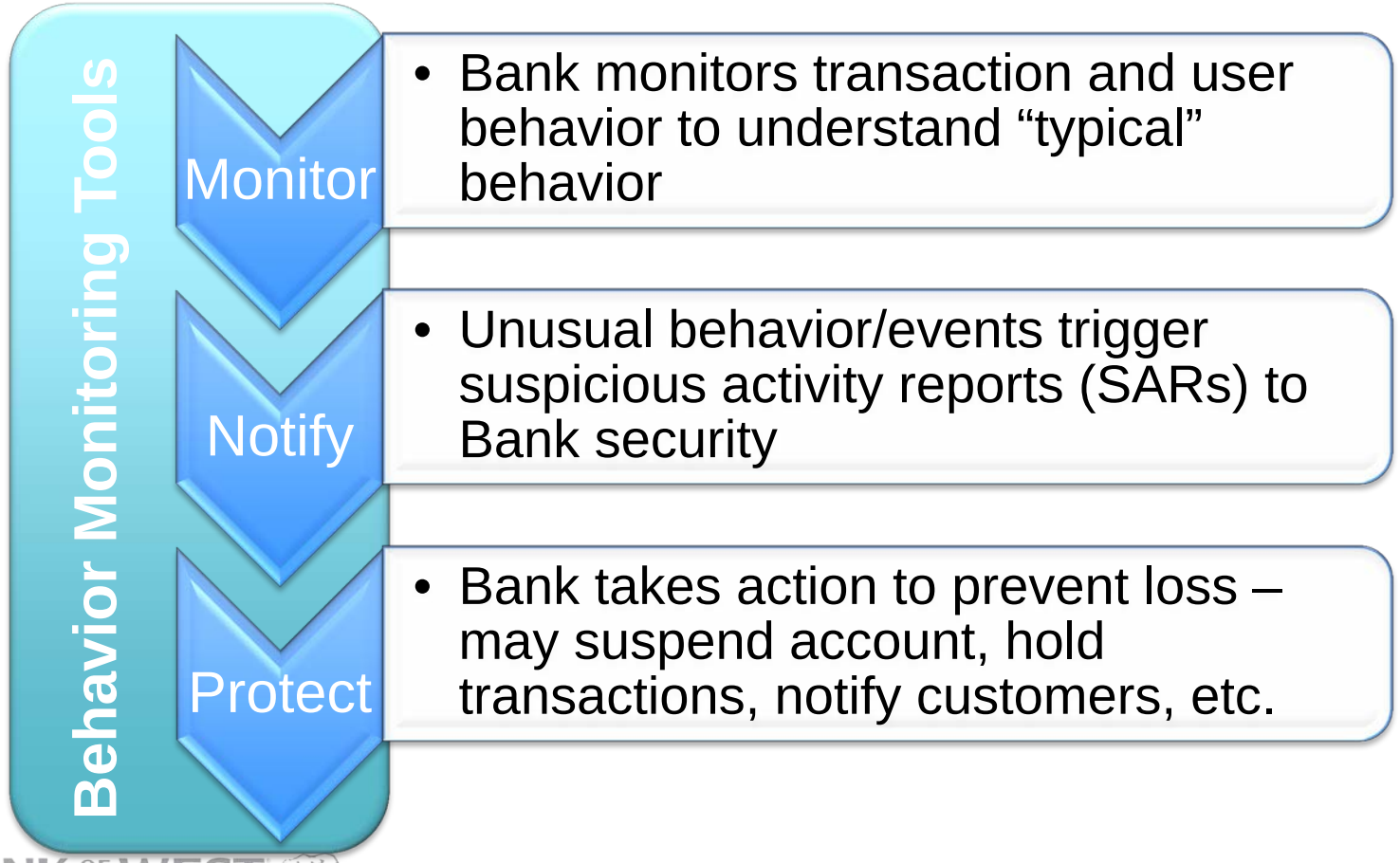
- Between Oct. 2013 and Feb. 2016, the scam was reported in 79 countries and every U.S. state.
- Masquerading/BEC incidents have increased 270% since January 2015
- Nearly 18,000 reports have been filed by victims of the masquerading / BEC scam
- The FBI reports losses amount to more than **$2.3 billion**
- Financial losses have ranged from $25,000 to as much as $90,000,000

Sources: https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

What are six key security questions any business should ask its bank?

Does your bank use behavior monitoring tools?

- A bank's back-office behavior monitoring controls are not always visible to customers but they help protect businesses from loss every day

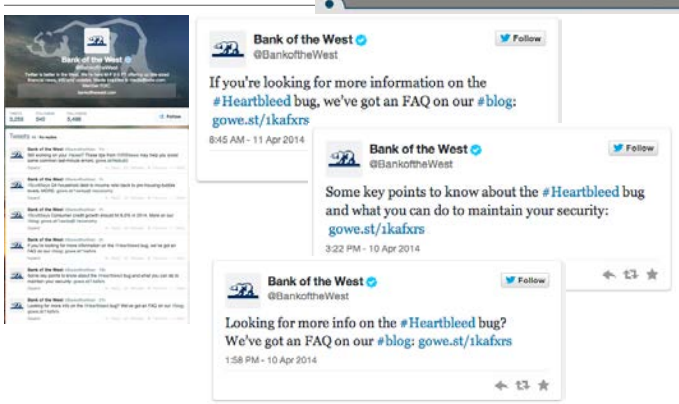


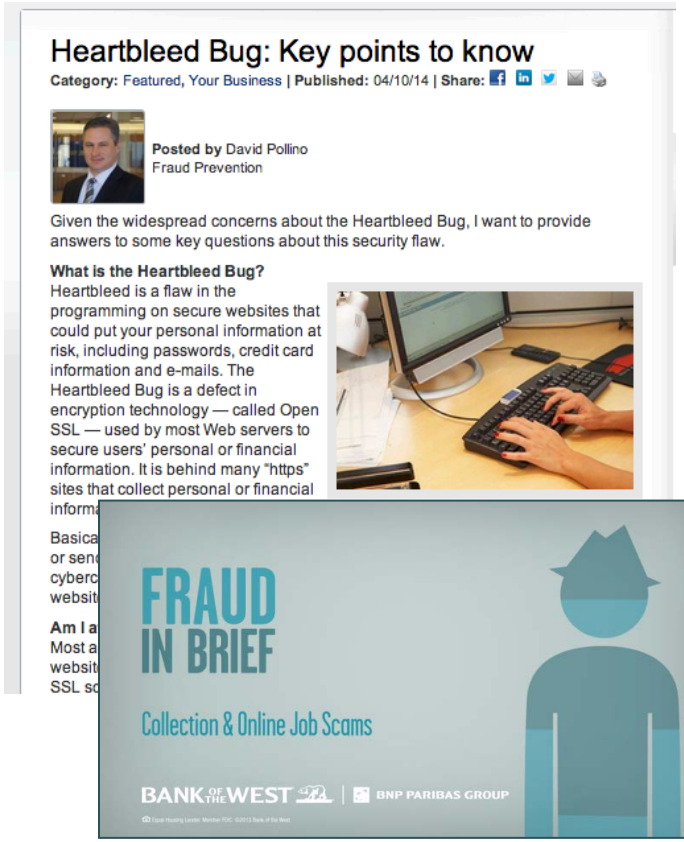
Does your bank offer fraud-preventing products?

- A comprehensive suite of fraud-related products and features is essential to safeguarding against payments fraud

Does your Bank offer fraud education?

- Education and training are also key to generating awareness and compliance to fraud-preventing measures.
  - Fraud videos
  - Info security magazine
  - Employee training
  - Security best practices





Does your bank offer malware protection?

- **Every minute, 232 computers are infected by malware**
- Zeus is the top financial malware, responsible for around 80% of all attacks against financial institutions today and causing over **$1 billion in global losses in the last five years**
- Hackers used a trojan to send wires from Efficient Services Escrow's account, but there are other ways fraudsters can use malware to steal money:





Malware Captures check images in a compromised account

Counterfeit checks are created using specialized paper and ink

Counterfeit checks are typically presented in retail stores

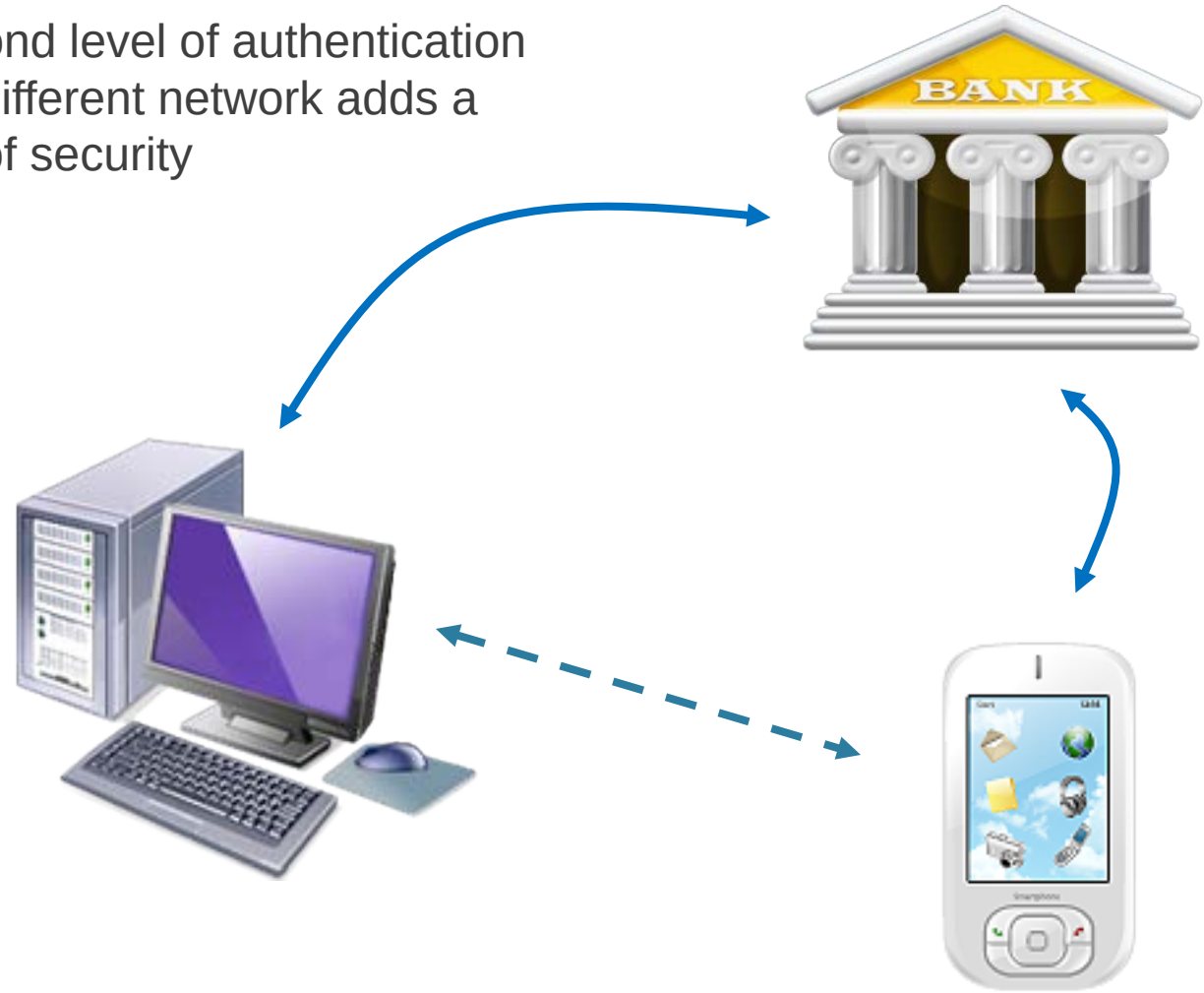
Source: RSA 2012 Cybercrime Trends Report

BANK OF THE WEST
BNP PARIBAS GROUP

Malware Protection

Does your Bank provide out-of-band authentication?

- A second level of authentication via a different network adds a layer of security



Does your Bank help protect your employees?

- Businesses that deal in cash may have their employees handling and transporting large amounts of cash unprotected.

A Bank may provide a cash vault and armored car services to mitigate exposure to employees.

Essential Steps to Prevent Cybercrime

- What else your business should be doing:
  - Use malware detection tools
  - Keep user name and password secure (no sharing)
  - Require strong passwords (mixed case, letters, numbers and special characters, at least 10, no dictionary words even spelled backwards) that differ for each website and must be changed periodically
  - Limit user access and rights, set time-of-day access controls
  - Verify secure session (“https”) in browser for all online banking
  - Avoid login features that save username and password
    - Use 2 factor email authentication = http://blog.bankofthewest.com


Why I use 2-factor authentication for email — and you should, too

Category: Your Business | Published: 04/08/14 | Share:

Posted by David Pollino
Fraud Prevention

Email is one of the most common targets for hackers into individuals' and businesses' computer systems. Some small business owners use personal email to conduct business, and even larger businesses sometimes mingle personal and business email.

Essential Steps to Prevent Cybercrime

- What else your business should be doing:
  - Install a dedicated, actively managed firewall
  - Use a regular operating system and key application security patches
  - Initiate ACH and wires under dual control
  - Consider host-to-host payment file transmission
  - Ensure anti-virus and security software and mechanisms for all computer workstations and laptops used for online banking and payments are robust and up-to-date
  - Restrict functions for computer workstations and laptops that are used for online banking and payments
  - Monitor and reconcile accounts daily