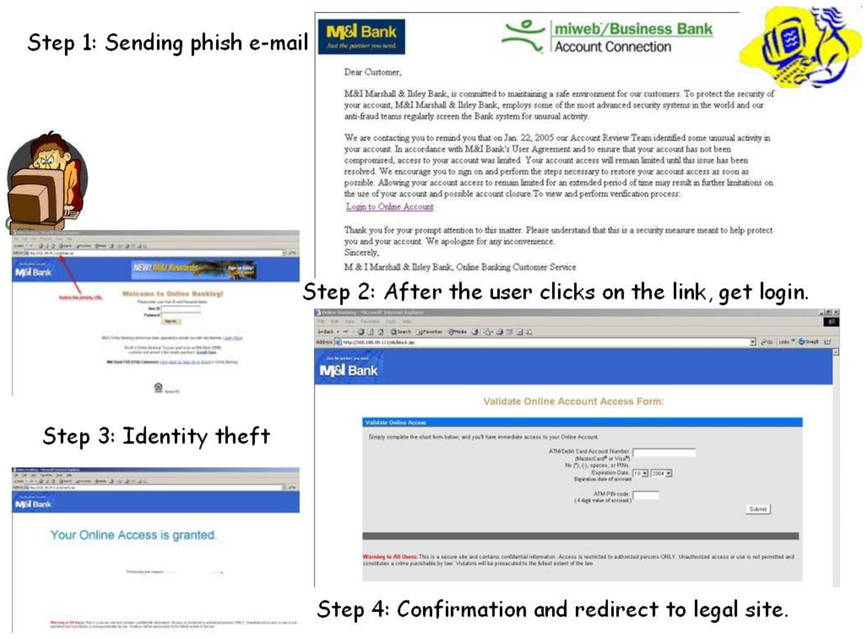
CERIAS

Mitigating Phishing Attacks

Mercan Topkara Mikhail J. Atallah Cristina Nita-Rotaru
CERIAS Purdue University
West Lafayette, IN USA

What is Phishing?

- a form of on-line identity theft
- attackers send e-mails and use fake Web sites that spoof a legitimate business
- lure unsuspecting customers into sharing personal and financial data



Effects of Phishing

- Lost Dollars…
  - 70,000 calls/hour for 12 hours
  - Banks and card issuers lost $1.2 billion in 2003
- Lost Trust …
  - A question of trust, a question of brand.

Consortiums for Fighting Phishing

- The Anti-Phishing working group (more than 600 organizations)
  http://www.antiphishing.org
- The Trusted Electronic Communications Forum (TECF)
  http://www.tecf.org
- WholeSecurity (Microsoft, eBay, Paypal, and Visa)
  http://www.wholesecurity.com/

Phisher

- has to impersonate a trusted source
- has to misuse legitimate content for convincing
- can not have the shared secrets
  - full name, account number etc.
- can carry out man-in-the-middle attack in many cases

Victims

- Legitimate Company:
  - needs to provide trusted online services
  - has large computing power
  - has a database of customer information
  - has the power of creating the original documents that the *phisher* needs to copy
- Average User:
  - busy or lazy
    - disables security options
    - re-uses login/password
    - trusts e-mails
  - not tech savvy
  - uses various computers

Mitigating Phishing Attacks

- Design and deployment of secure e-mail
  - can prevent many forms of phishing attacks
  - requires Public Key Infrastructure
  - has scalability and trust issues for larger communities
  - not widely deployed and adopted
- Client-side defense
  - most studied defense system against phishing
  - designed to provide more accurate information to the user
  - depends on improving the security capabilities of browsers by plug ins
  - can be fooled by attackers having a good understanding of web construction
- Our Approach: Content based defense
  - new approach, not well-studied
  - required for a complete solution
  - Mechanisms that can:
    - analyze what the user sees
    - analyze the e-mail and web page content
    - provide integrity check for these components
  - We will achieve this using:
    - information hiding for authentication of web objects
    - judicious use of Identity-based Encryption
      - which requires the extraction of identity

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center