Overview of computer and communications security

2

Universidad Carlos III de Madrid
Grupo SeTI · Dpto. Informática

Basic security concepts

- Assets
- Threats
- Security services
- Security mechanisms

Assets

- Logical resources
  - Information
  - Money (electronic)
  - Personal data
  - Credit/debit card data
  - Electronic goods (music, software, tickets…)
- Physical resources
  - Goods (clothes, electronic devices, food…)
  - Hardware
  - Buildings
  - People
  - Money (physical)

Threats

- A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

- A threat is a possible danger that might exploit a vulnerability.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Threats

- Intentional threat

  A possibility of an attack by an intelligent entity (e.g., an individual cracker or a criminal organization).

- Accidental threat

  A possibility of human error or omission, unintended equipment malfunction, or natural disaster (e.g., fire, flood, earthquake, windstorm, and other causes listed in).

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Threats

- Passive threat

  The threat of unauthorized disclosure of information without changing the state of the system.

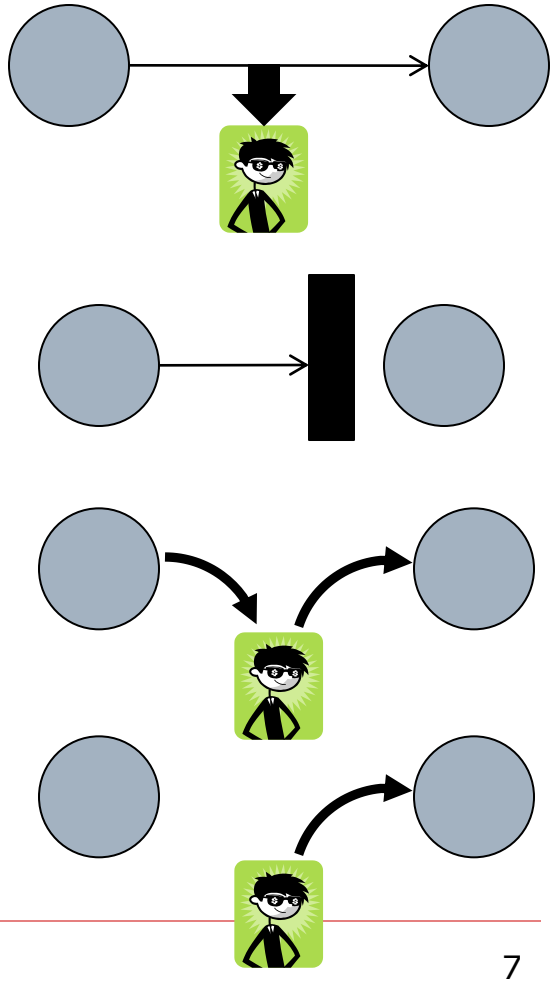
- Active threat

  The threat of a deliberate unauthorized change to the state of the system.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Threats

- Passive
  - Interception
- Active
  - Interruption
  - Modification
  - Generation (fabrication)
  - Unauthorized access
  - Repudiation



Passive threats

- Interception
  - Communications monitored by eavesdropper
  - Tapping telephone wires
  - Sniffers: intercept packets from a network
  - Traffic analysis

➡ In open networks like internet, this is very difficult to detect and impossible to prevent.

Active threats

- Interruption
  - Denial of service (DoS) attack e.g. by flooding: SYN, smurf

W32.Mydoom.M@mm is a mass-mailing worm that drops and executes a backdoor, detected as Backdoor.Zincite.A, that listens on TCP port 1034. The worm uses its own SMTP engine to send itself to email addresses it finds on the infected computer.

The email contains a spoofed From address, and the Subject and Body text will vary. The attachment name will also vary.

Active threats

- Modification
  - Falsification of IP directions
  - Communications tampering
  - “Man in the middle”
  - Masquerade
  - Spoofing / phishing

Active threats

- Generation
  - IP hijacking (session kidnapping)

Threat agents

- Insiders (employees / former employees)
  - Errors
  - Intentional actions (attackers)
- Outsiders (external parties, attackers)
  - Criminals
  - Vandals
- Disasters

Cybercrime

- Cybercrime refers to criminal offenses committed using the Internet or another computer network as a component of the crime. E.g.:
  - The computer or network can be the tool of the crime (used to commit the crime).
  - The computer or network can be the target of the crime (the “victim”).
  - The computer or network can be used for incidental purposes related to the crime (for example, to keep records of illegal drug sales).

Cybercrime (United Nations)

- a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
- b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Computer Crime & Security Survey 2008

- Robert Richardson, Director of CSI (Computer security institute) has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations.
- Over 500 security professionals responded. Their answers are inside the Survey

Source: Computer Security Institute - Computer Crime & Security Survey 2008

Experienced security incidents (%)

- Yes:
  - 2007: 46
  - 2008: 43 (over 517 respondents)
- No:
  - 2007: 45
  - 2008: 44
- Don't Know
  - 2007: 10
  - 2008: 13

Source: Computer Security Institute - Computer Crime & Security Survey 2008

Number of incidents (%)

- 2008 (250 respondents)
  - 1-5: 47
  - 6-10: 14
  - >10: 13
  - Don't know: 26
- Similar figures for previous years

Source: Computer Security Institute - Computer Crime & Security Survey 2008

Key types of incident (%)

- 2008: 433 respondents
  - Virus: 50
  - Insider Abuse: 44
  - Laptop Theft/Fraud: 42
  - Unauth Access: 29
  - Bots: 20
  - Financial Fraud: 12
  - DNS: 8
- Decreasing tendency since 1999-2001
- New types of attackssince 2007: Bots and DNS
- **Average losses** in 2008: 289 thousands of dollars (144 respondents) [vs average losses in 2001: 3149 thousands of dollars)

Source: Computer Security Institute - Computer Crime & Security Survey 2008

Internet Crime report 2008

- "The 2008 Internet Crime Report (IC3) is the eighth annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action."
- "From January 1, 2008 – December 31, 2008, the IC3 website received 275,284 complaint submissions. This is a (33.1%) increase when compared to 2007 when 206,884 complaints were received."
- "These filings were composed of complaints primarily related to fraudulent and non-fraudulent issues on the Internet."

Source: Internet Crime Complaint Center (IC3) - Internet Crime report 2008

Crime complaints

- Main categories (%):
  - Non-delivery: 32,9
  - Auction Fraud: 25,5
  - Credit/Debit Card Fraud: 9
  - Confidence Fraud: 6,2
  - Computer Fraud: 5,4
  - Check Fraud: 5,4
- Main average losses:
  - $100-$999,9 (36,5%)
  - $1.000-$4.999,99 (33,7%)
- Total losses:
  - $264,6 million
- Main contact methods:
  - e-mail (74%)
  - web page (28,9%)

Source: Internet Crime Complaint Center (IC3) - Internet Crime report 2008

Check fraud


Dear Beloved - Thunderbird
File Edit View Go Message Tools Help
Thunderbird thinks this message is junk.
This is Not Junk
Subject: Dear Beloved
From: Mr.Robert Heritage
22/09/2009 14:19
HELP IN DISTRIBUTING FUNDS TO CHARITY ORGANIZATIONS.
From Mr. Robert M.Heritage,
Dear Friend,
This letter may come to you as a surprise due to the fact that we have not yet met.I have to say that I have no intentions of putting you into any form of stress or worries. As you read this, I don't want you to feel sorry for me, because,I believe everyone will die someday.
I am Mr. Robert Mark Heritage,the husband of Mrs.Suzanne Tremblay,both of us,are citizens of Tunisian. my wife worked with the Chevron/Texaco in Russia for twenty years before she died in the year 2003.When my late wife was alive she deposited the sum of 4.8 Million Dollar with a Bank in London, I 'm now in hospital in Germany for diagnosed with prostate and esophagea Cancer.
I have only about just few months to live according to the medical doctor/experts.I would want you to donate this funds to Charity Oganizations and Motherless Babies. Reply me through this id mrrobertheritage05@yahoo.dk
Warmest Regards,
Mr. Robert M.Heritage

Attackers' tools

- Sophisticated tools
  - Hybrid attacks
    - Use several malware to infiltrate or damage a computer system, without the owner's informed consent
    - May affect the web site (losses because unavailability, capture of customers' personal data...)
    - May affect the customer (capture of personal and authentication data -keystroke logging-, use computer as a zombie to send spam or perform DDoS…)

Albert Gonzalez

- http://www.storefrontbacktalk.com/securityfraud/gonzalez-the-al-capone-of-cyber-thieves/
  - "Beginning on or about December 26, 2007, Heartland was the victim of a SQL injection attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding card data."

Albert Gonzalez

http://online.wsj.com/article/SB10001424052748703416204575146152576681126.html

TECHNOLOGY | MARCH 27, 2010

Hacker Sentenced to 20 Years in Massive Data Theft

Article | Comments (29)

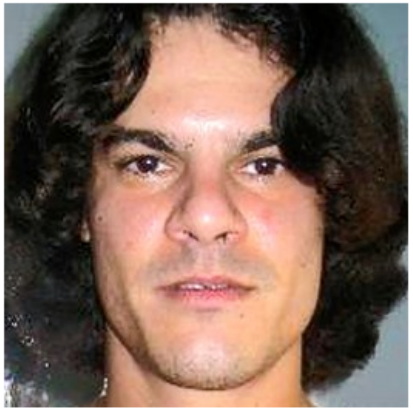
Email | Print | Save This | Like | + More | Text

By SIOBHAN GORMAN

The self-taught computer hacker prosecutors say stole data from millions of credit-card holders and cost businesses hundreds of millions of dollars was sentenced Friday to 20 years and one day in prison—the stiffest sentence ever handed down in a hacking case.

The sentencing in U.S. District Court in Boston wrapped up the cases against Albert Gonzalez, a 28-year-old college dropout and onetime Secret Service informant, in what prosecutors called largest and most costly computer crimes in U.S. history.

In the last of the three cases, Mr. Gonzalez had pleaded guilty in December to conspiracy charges in the theft of data from credit-card processor Heartland Payment Systems Inc. and other businesses. Prosecutors said the scheme stole the data of 130 million credit cards; Heartland says the hack cost the company nearly $130 million.



Agence France-Presse/Getty Images

Prosecutors said Albert Gonzalez, a onetime Secret Service informant, was behind the largest and most costly computer crimes in U.S. history

On Thursday, Mr. Gonzalez had been sentenced Thursday to 20 years in prison in each of the first two cases against him, involving similar theft schemes against TJX Cos., the Dave & Buster Inc. restaurant chain and other businesses.

He will serve all three sentences concurrently.

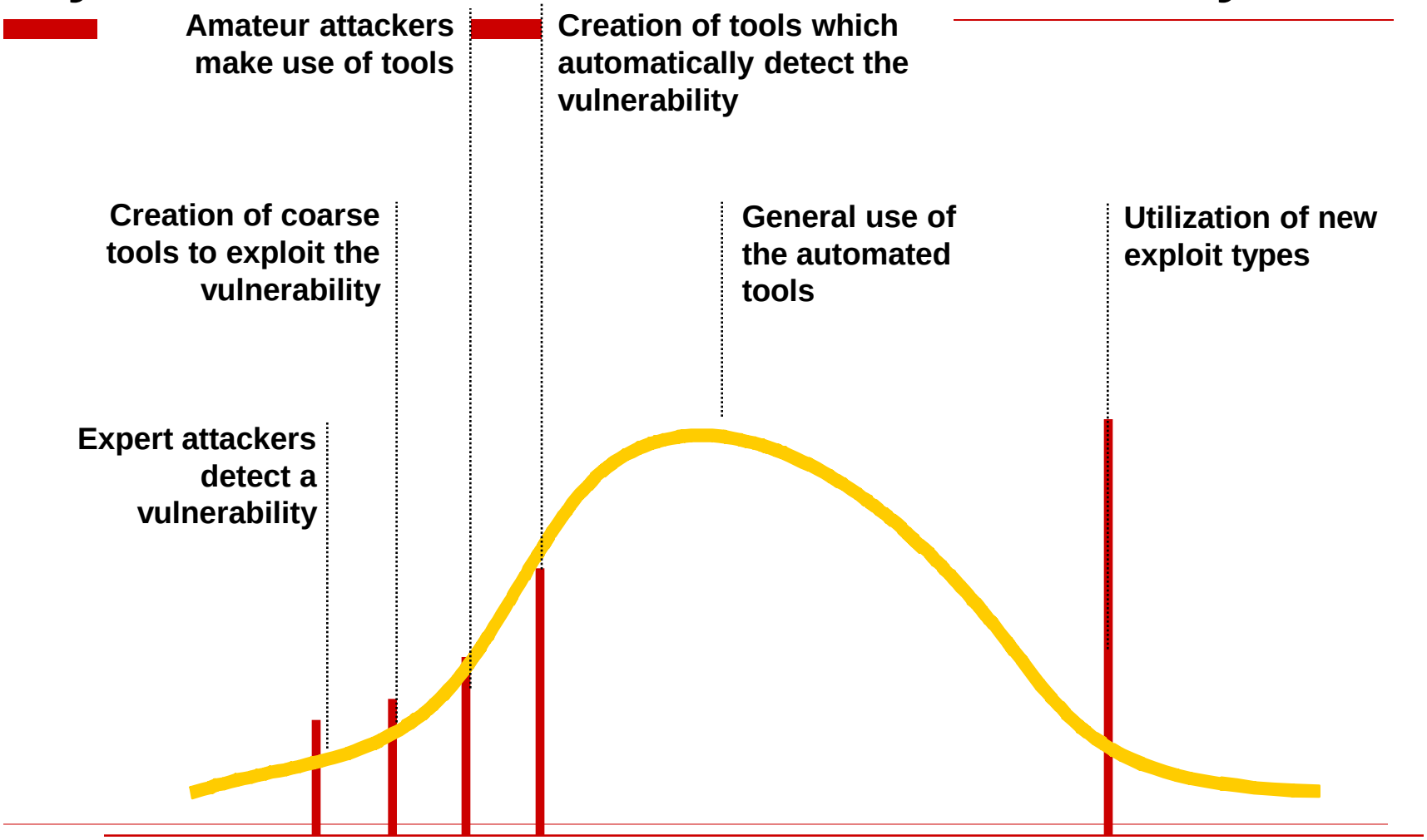
The three schemes ensnared as many as tens of millions of victims, prosecutors said. The direct cost of Mr. Gonzalez's TJX scheme was close to $200 million, they said.

Mr. Gonzales's attorney, Martin Weinberg, disputed those numbers, saying the costs were due in part to corporate negligence. Mr. Weinberg said in a sentencing memo that Mr.

Attackers' tools

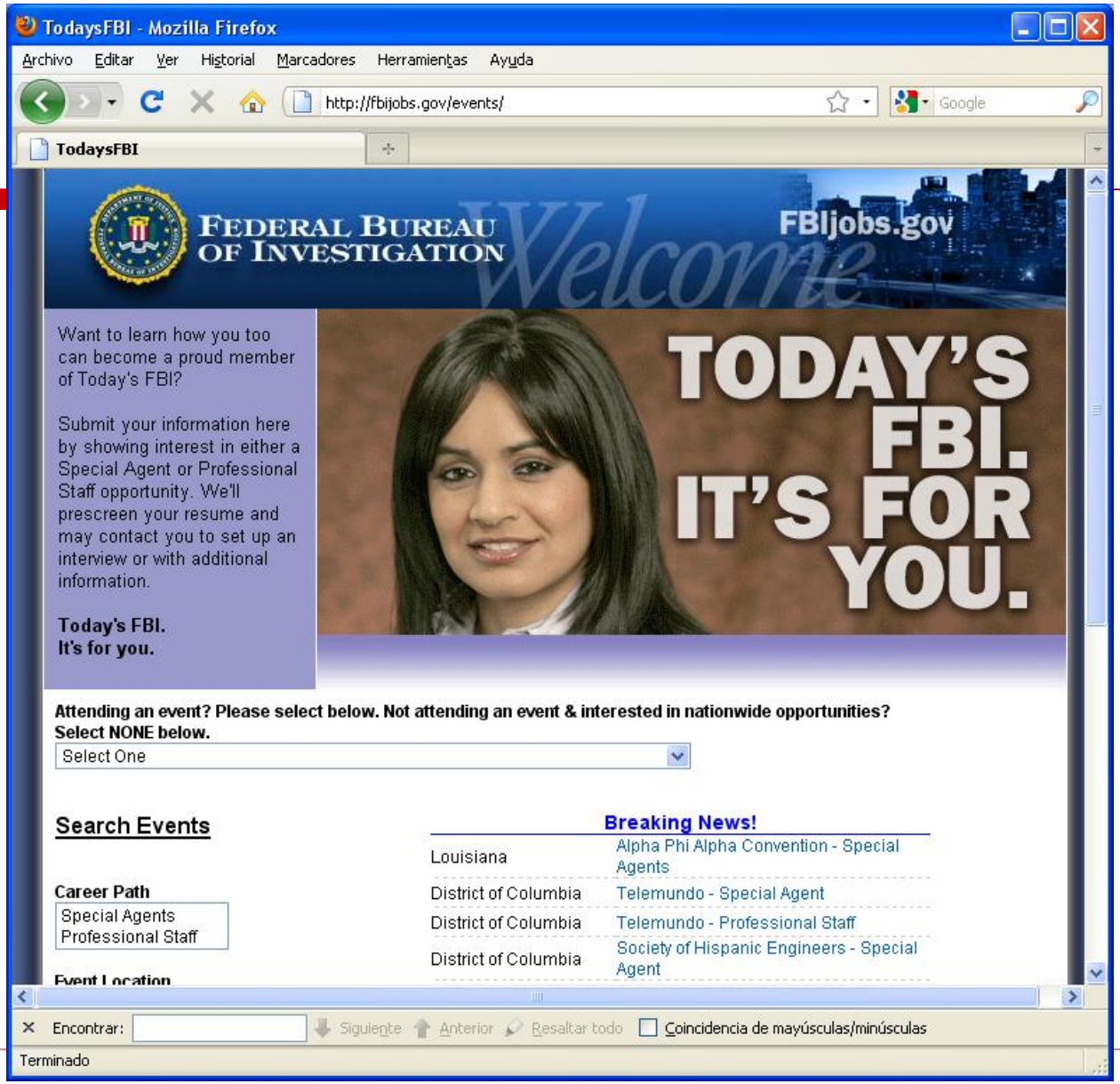
- Automated tools
  - http://www.computerworld.com/s/article/9064238/Hacker_group_releases_automated_Google_hacking_tool

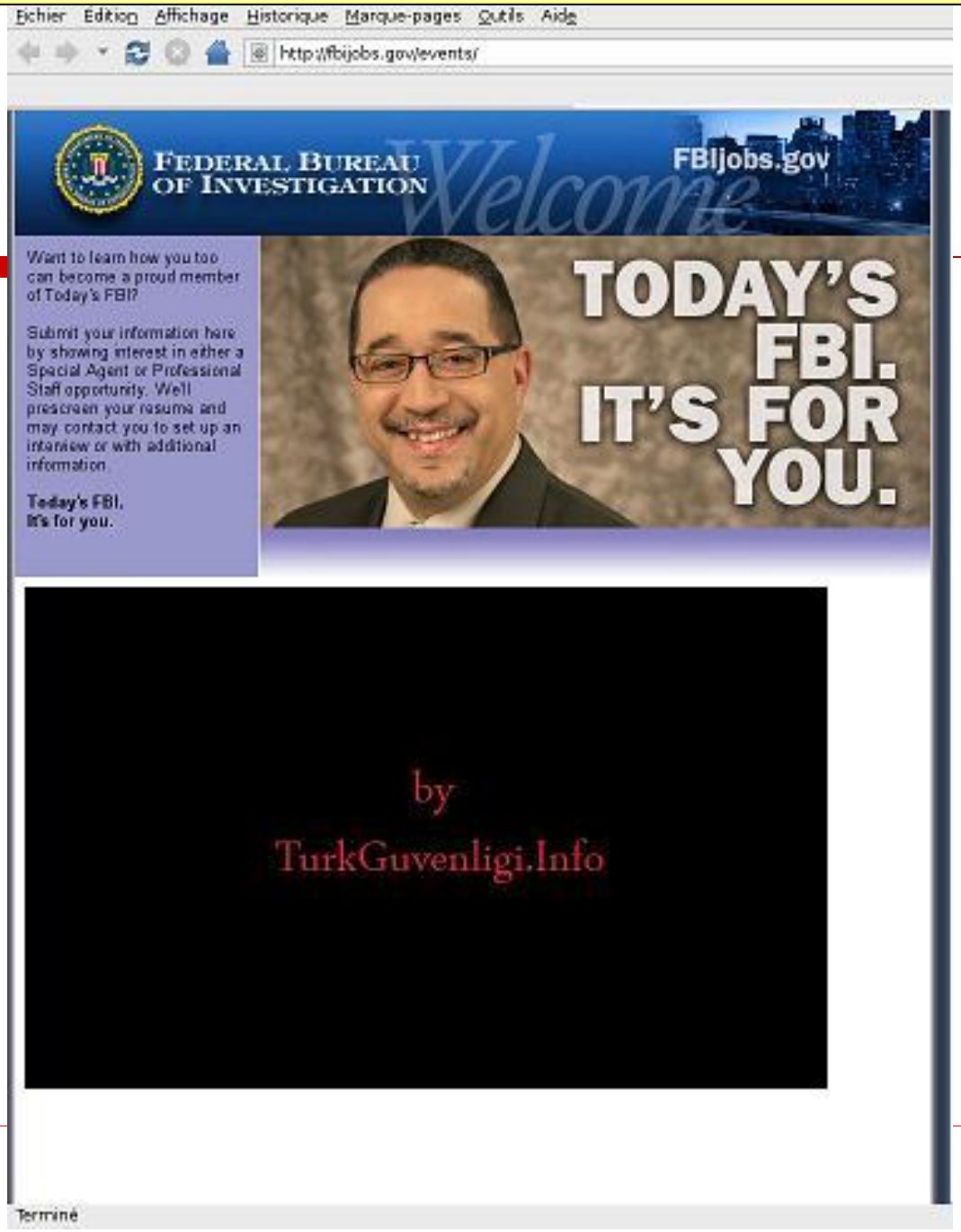
Cycle of exploitation of a vulnerability



Defacement

- A website defacement is an attack on a website that changes the visual appearance of the site.
  - Potential to cause lasting damage to the customer's impression of the business and in particular to the perception of its security


TodaysFBI - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://fbijobs.gov/events/
Google
TodaysFBI
FEDERAL BUREAU OF INVESTIGATION
Welcome
FBIjobs.gov
Want to learn how you too can become a proud member of Today's FBI?
Submit your information here by showing interest in either a Special Agent or Professional Staff opportunity. We'll prescreen your resume and may contact you to set up an interview or with additional information.
Today's FBI.
It's for you.
TODAY'S FBI. IT'S FOR YOU.
Attending an event? Please select below. Not attending an event & interested in nationwide opportunities? Select NONE below.
Select One
Search Events
Career Path
Special Agents
Professional Staff
Event Location
Breaking News!
Louisiana
Alpha Phi Alpha Convention - Special Agents
District of Columbia
Telemundo - Special Agent
District of Columbia
Telemundo - Professional Staff
District of Columbia
Society of Hispanic Engineers - Special Agent
Encontrar:
Siguiente
Anterior
Resaltar todo
Coincidencia de mayúsculas/minúsculas
Terminado


Fichier Edition Affichage Historique Marque-pages Outils Aide
http://fbijobs.gov/events/
FEDERAL BUREAU OF INVESTIGATION
Welcome
FBIjobs.gov
Want to learn how you too can become a proud member of Today's FBI?
Submit your information here by showing interest in either a Special Agent or Professional Staff opportunity. We'll prescreen your resume and may contact you to set up an interview or with additional information.
Today's FBI.
It's for you.
TODAY'S FBI. IT'S FOR YOU.
by
TurkGuvenligi.Info
Terminé

Attackers' tools

Users are the weak link in security

- Social engineering
  - An attack that does not depend on technology as much as it depends upon tricking or persuading an individual to divulge privileged information to the attacker, usually unknowingly.
  - http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/
  - False virus (hoax)
  - Phishing http://www.antiphishing.org/
  - Pharming

Social engineering: Phishing

- Phishing
  - A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person

Social Engineering: Phishing

Dear eBay User,
During our regular update and verification of the accounts,
we couldn't verify your current information.
Either your information has changed or it is incomplete.
If the account information is not updated to current information
within 5 days then, your access to bid or buy on eBay will be suspended.
go to the link below,
and re-enter your account information.

Click here to update your account.
Please Do Not Reply To This E-Mail As You Will Not Receive A Response
Thank you
Accounts Management

Social Engineering: Phishing

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
To: arturo@inf.uc3m.es
Subject: Citibank - Security Update

citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Social Engineering: Phishing

Dear Sky Bank customer,

We recently reviewed your account and suspect that your Sky Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Sky Financial network is our primary concern. Therefore, as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

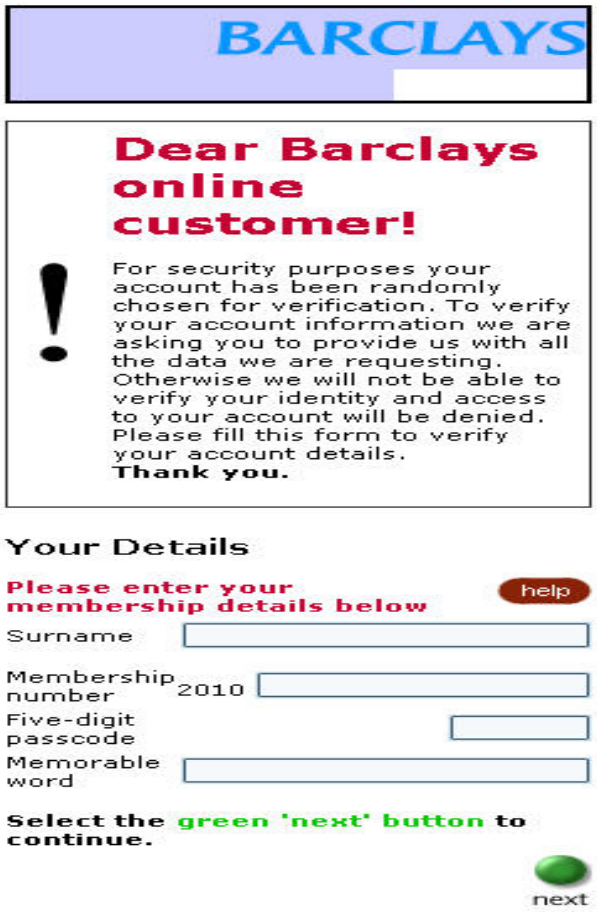
1. Login to your Sky Internet Banking account. In case you are not enrolled for Internet Banking, you will have to fill in all the required information, including your name and your account number.

2. Review your account history for any unauthorized withdrawals or deposits, and check your account profile to make sure no changes have been made. If any unauthorized activity has taken place on your account, report this to Sky Financial Group staff immediately.

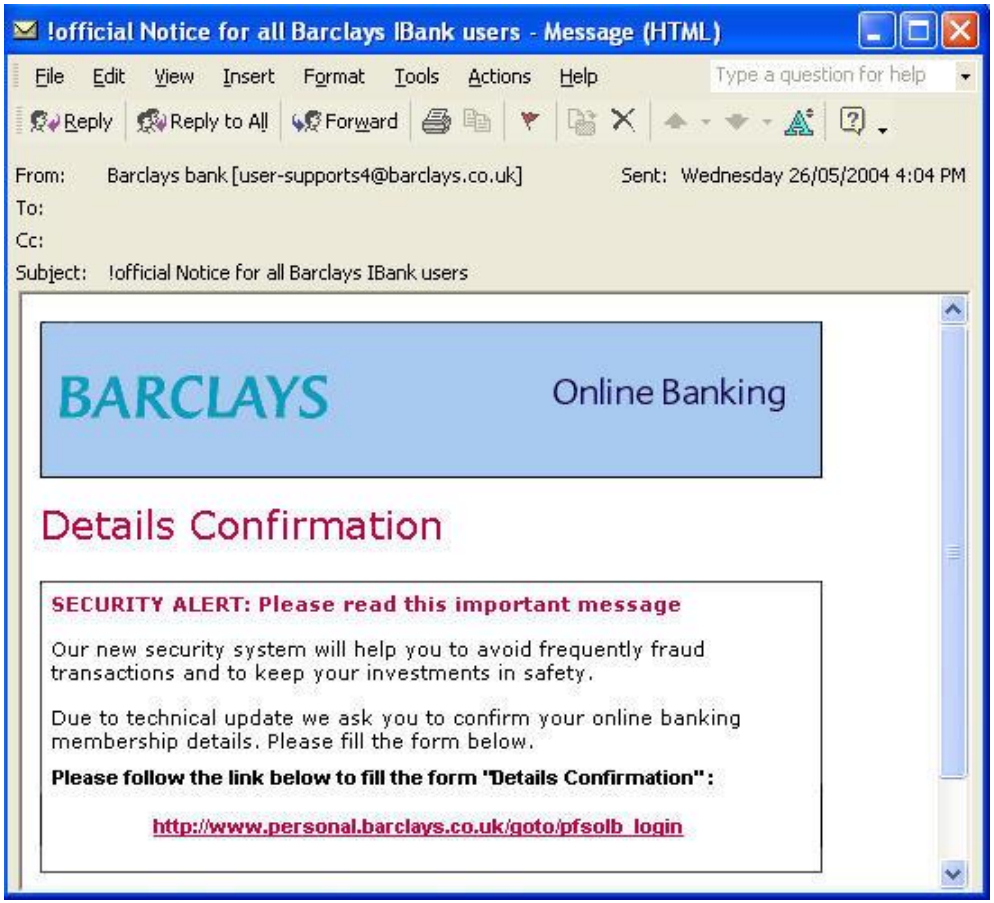
To get started, please click the link below:

SIGN-ON

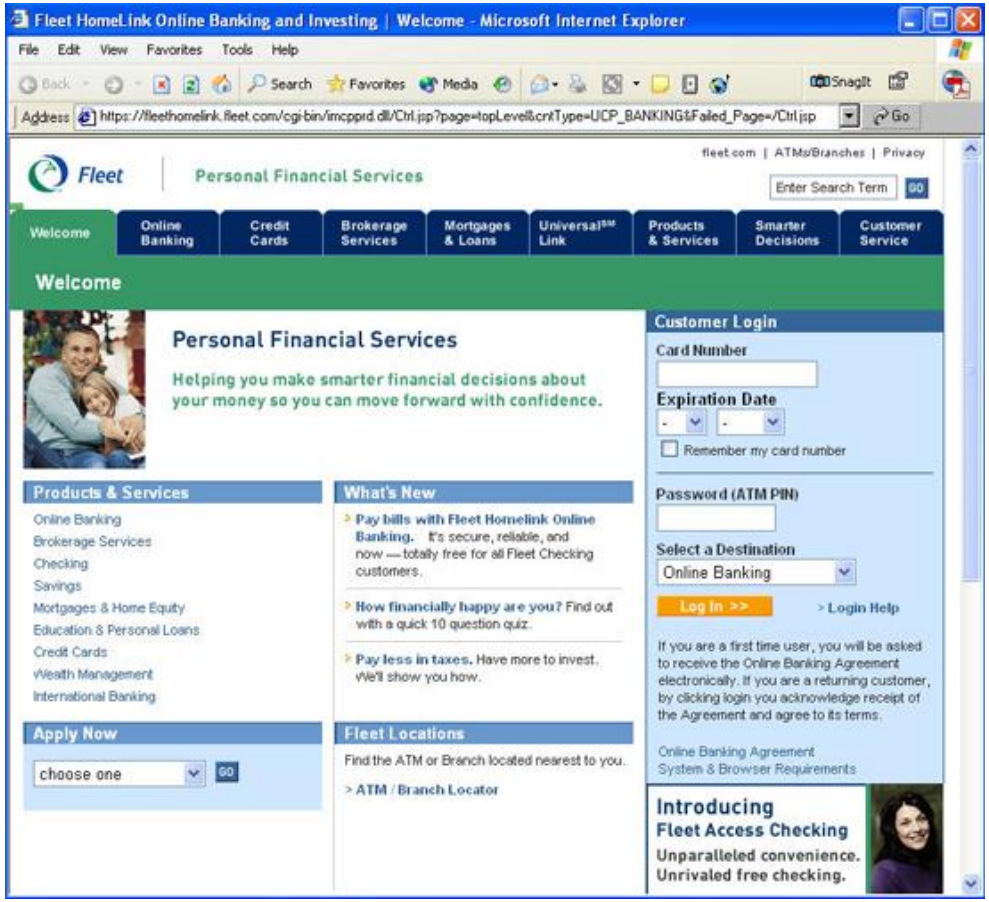
Social Engineering: Phishing



Social Engineering: Phishing

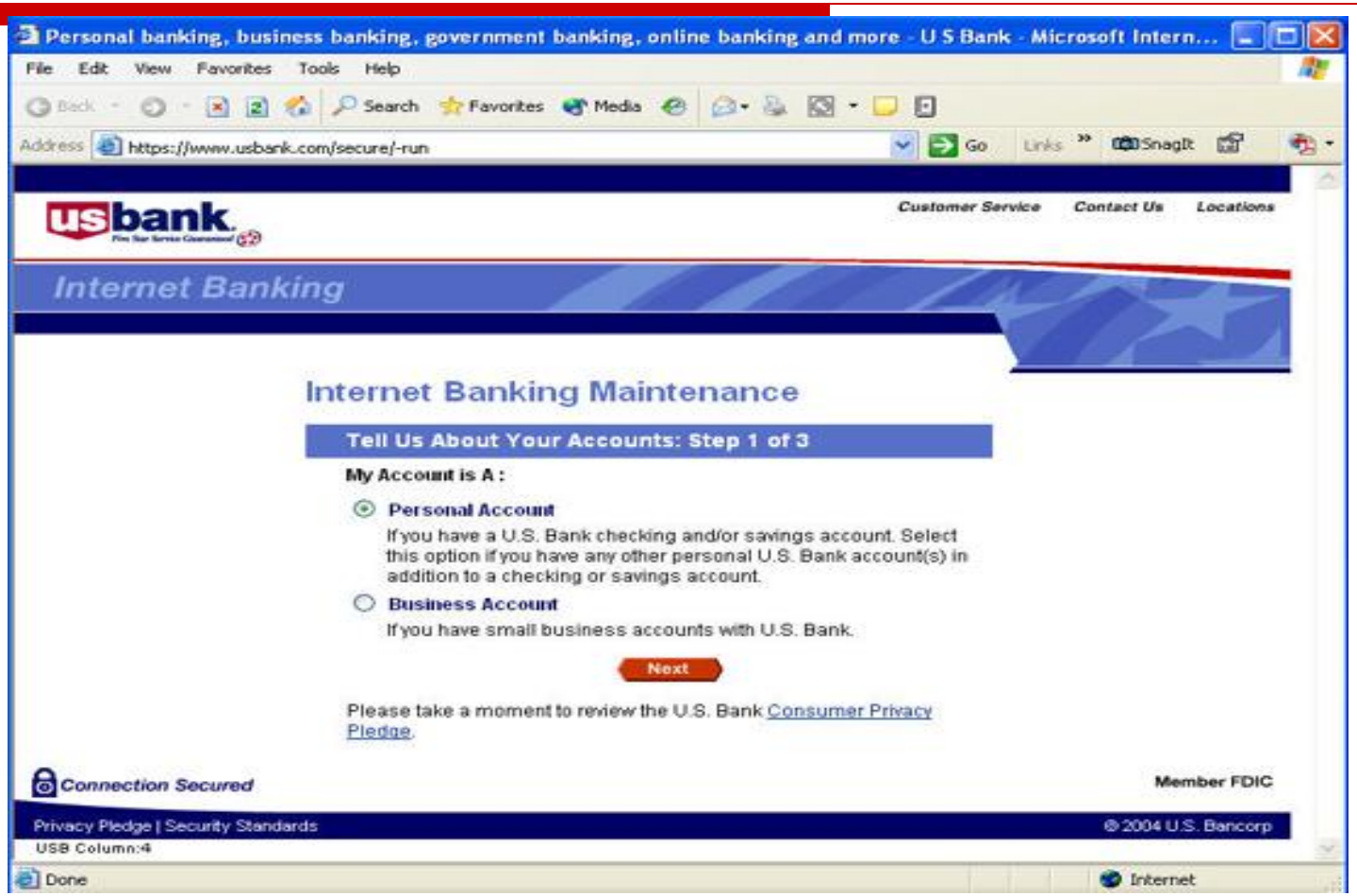


Social Engineering: Phishing web sites

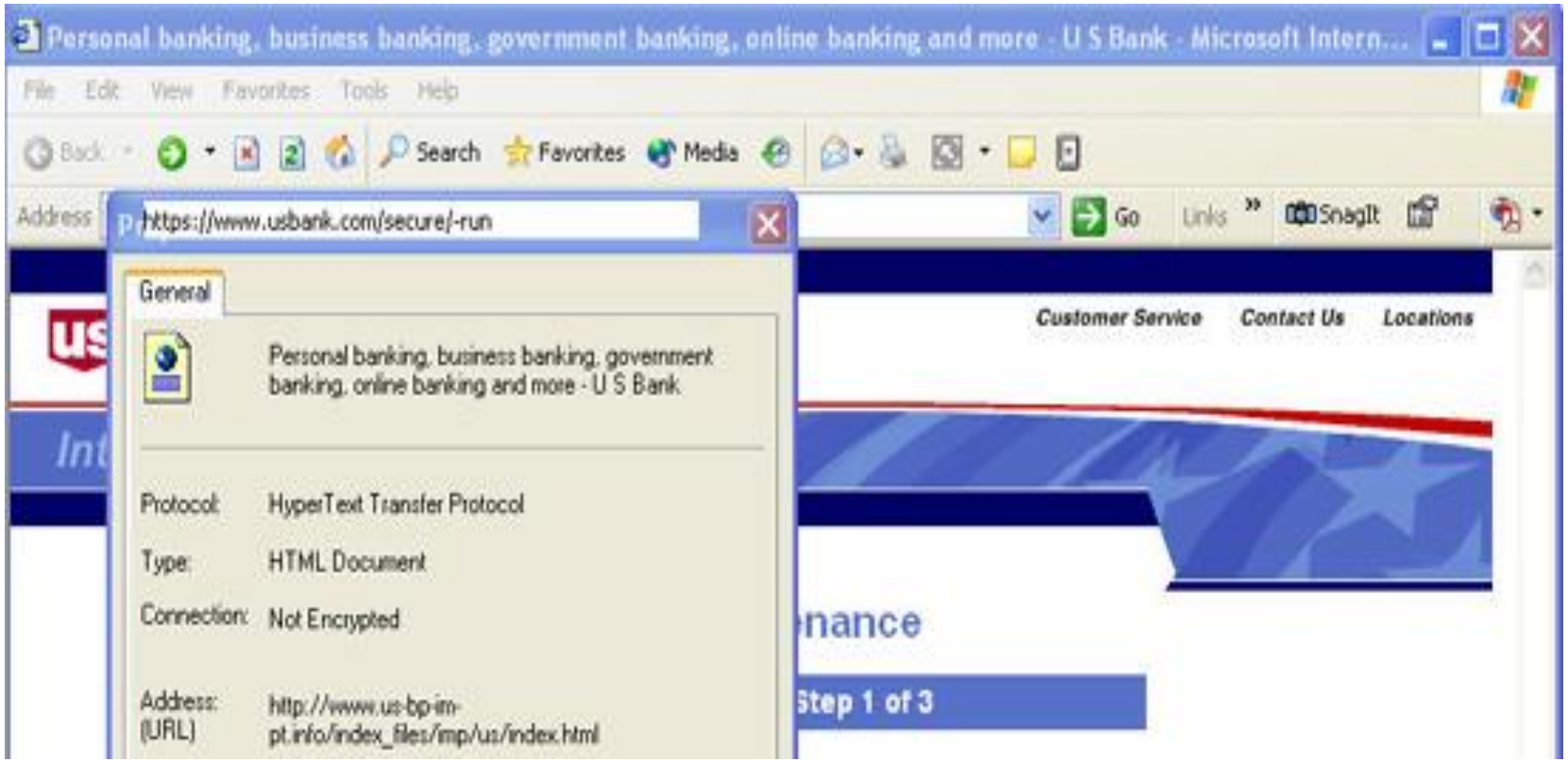


Social Engineering: Phishing web sites

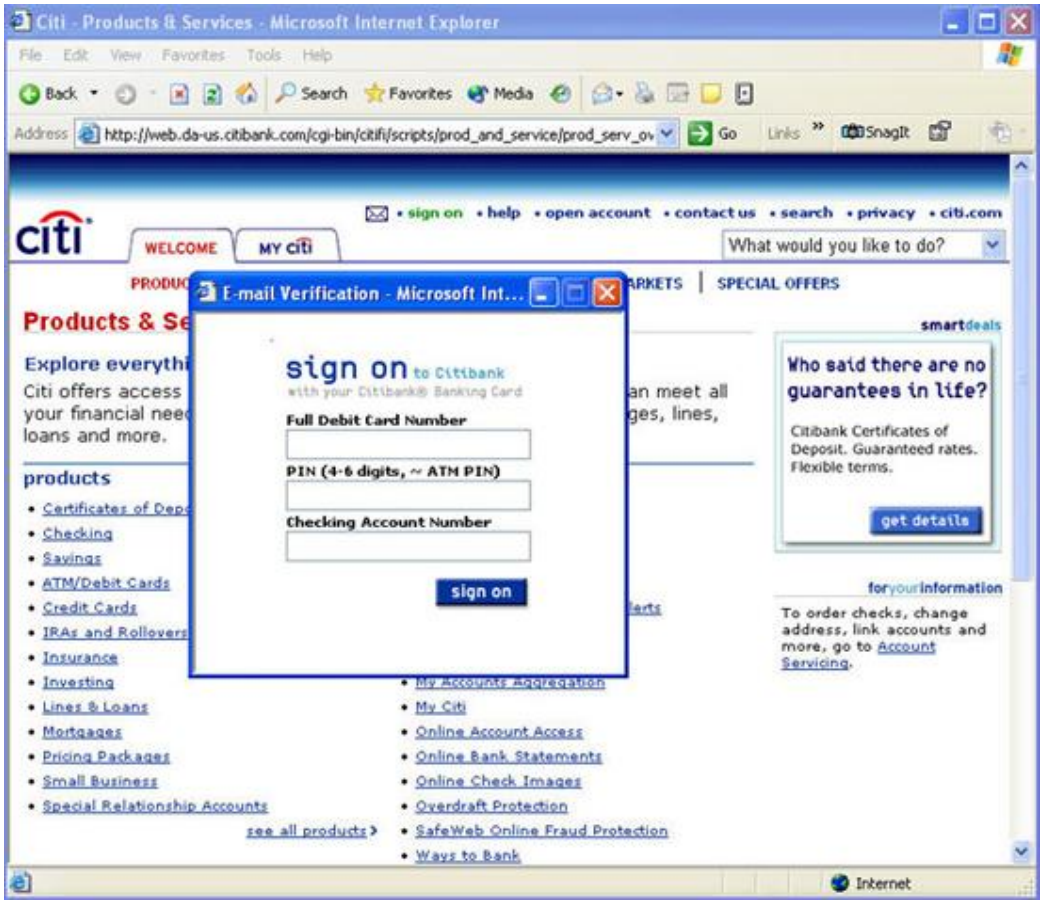
Social Engineering: Phishing web sites



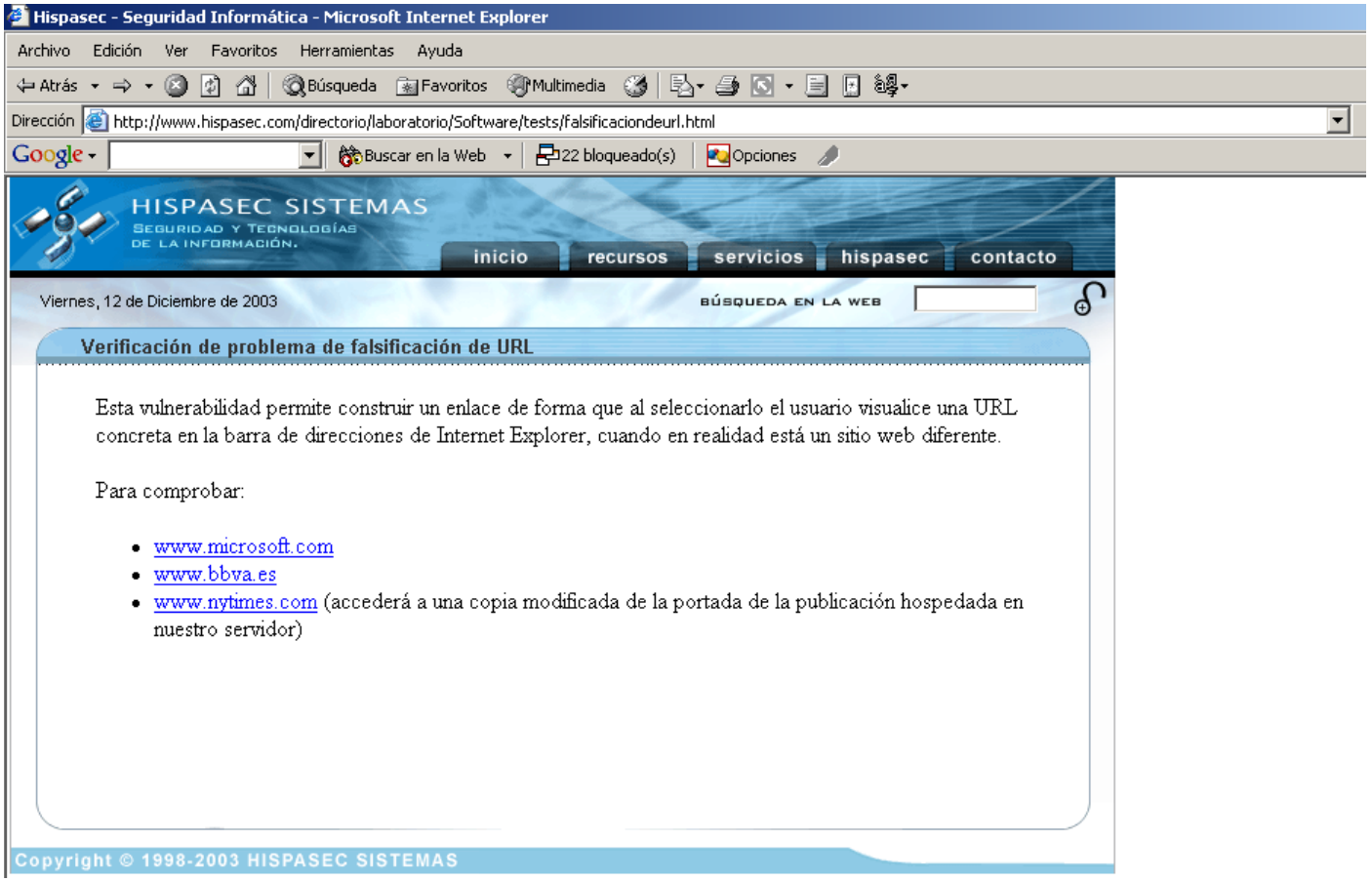
Social Engineering: Phishing web sites



Social Engineering: Phishing web sites



Social Engineering



Social Engineering

Social engineering: Pharming

- A more sophisticated form of MITM attack
- Users session requesting certain URL (real IP address) is redirected to a masquerading website (fake IP address)
  - Changing hosts file
  - Changing the pointers on a DNS server
  - At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real site and conduct transactions using the credentials of a valid user on that website

Pharming

- = domain spoofing
- DNS *poisoning*

> **Just watching the address bar on your Internet browser won't inform you of any hijacks; to you, the URL and possibly even the spoofed financial site will look just fine.**

- Solution: Certificates

Security services

- A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service [Cryptography and Network Security, 4/E W. Stallings, 2008]

- A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. [ISO-7498-2:1989]

Security services

- Confidentiality
  - The property that data is not disclosed to system entities unless they have been authorized to know the data.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security services

- Authentication
  - A security service that verifies an identity claimed by or for an entity
    - data origin authentication service: The corroboration that the source of data received is as claimed
    - peer entity authentication service: The corroboration that a peer entity in an association is the one claimed.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security services

- Integrity
  - The security goal that generates the requirement for protection against either intentional or accidental attempts to violate
    - data integrity (the property that data has not been altered in an unauthorized manner) or
    - system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation)

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security services

- Non repudiation
  - A security service that provides protection against false denial of involvement in an association (especially a communication association that transfers data)
    - non-repudiation with proof of origin:
      - provides the recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny sending the data.
    - non-repudiation with proof of receipt:
      - provides the originator of data with evidence that proves the data was received as addressed, and thus protects the originator against an attempt by the recipient to falsely deny receiving the data.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security services

- Access control
  - Protection of system resources against unauthorized access
  - A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security services

- Availability
  - The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security mechanisms

- A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system
- Designed to prevent, detect and recover from a security attack
- Cryptographic techniques underlie many of the security mechanisms in use

SOURCE: GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-401) **GLOSARIO Y ABREVIATURAS**

Security mechanisms (X.800)

- Specific
  - Encipherment
  - Digital signatures
  - Access controls
  - Data integrity
  - Authentication exchange
  - Traffic padding
  - Routing control
  - Notarization
- Pervasive
  - Trusted functionality
  - Security labels
  - Event detection
  - Security audit trails
  - Security recovery

Relationship between services and mechanisms

Service	Mechanism							
	Encipher-ment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Source: Cryptography and Network Security, 4/E. W. Stallings, 2008