Identity Theft

**CJ341 – Cyberlaw & Cybercrime
Lecture #4**

**M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management**

DON'T PANIC*

➢ **This long presentation has a great deal of useful information**
➢ **You should pore over every detail of every slide as you swot for quizzes and exams.**
_____

* See http://video.movies.go.com/hitchhikersguide/

Topics

➢ **Video: USPIS on identity theft**
➢ **Identity Theft and Assumption Deterrence Act (18 USC §1028)**
➢ **Overview of Identity Theft & Consequences**
➢ **Identity Theft Statistics**
➢ **Methods Used by ID Thieves**
  ❑ **Carding**
  ❑ **Dumpster® Diving**
  ❑ **Credit-Card Skimming**
  ❑ **Shoulder Surfing**
  ❑ **Retail Scams**
  ❑ **Internet Scams**
  ❑ **Government Impersonation**
➢ **Responding to ID Theft**

Video: USPIS

Identity Crisis (12')

http://www.mekabay.com/cyberwatch/uspis_ic.zip

What ID Thieves Do

➢ **Locate identifying data**
  ❑ **Social Security Number**
  ❑ **Driver's License**
  ❑ **Home address, telephone number**
  ❑ **Mother's maiden name**
  ❑ **Or just misuse of *handle* (screen name) for forged messages**
➢ **Create new credit cards, bank accounts**
➢ **Default on loans in victim's name**
➢ **Ruin reputations, credit records**
➢ ***Victims have to prove their innocence***

Consequences for Victims

➢ **Credit-card expenses relatively easy to correct IFF**
  ❑ **Victim checks statement immediately and**
  ❑ **Reports questionable transactions within time limit**
➢ **Bank-account thefts much more difficult to correct**
  ❑ **Money stolen is client's, not bank's**
  ❑ **Client has great difficult recovering funds**
➢ **Bill-collectors hound victims relentlessly**
➢ **Bad credit records difficult to correct, ruin plans, cause loss of jobs or interfere with hiring**
➢ **Criminal accusations put victims at serious risk of erroneous arrest or deportation**
➢ **Victims may be nailed for child support of total strangers**

Identity Theft and Assumption Deterrence Act (18 USC §1028)*

- **Identity theft fastest growing form of fraud today**
  - **Criminals use SSN, public records to establish line of credit in victim's name**
  - **Debts assigned to victim**
  - **Burden of proof of *innocence* placed on victim**
  - **Catastrophic results on innocent people**
- **Felony**
  - **Up to 20 years jail**

_____
* http://tinyurl.com/ybralq

Identity Theft Statistics

- **Identity Theft Resource Center**
  http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics.shtml

---

Identity Theft Statistics (cont'd)

- **Victimization Data (individuals)**
  - **2004: US Bureau of Justice Statistics estimated 3.6M new households victimized in ½ of year**
  - **2001 to 2002: Increased 11-20% (Harris Interactive study)**
  - **2002-2003: Increased 80% between**
  - **2006: 15M new victims in USA – 1 new victim every 2 seconds (Gartner Group 2006)**
- **Business Losses**
  - **2005: estimated loss due to identity theft in US: $57B**
  - **Loss of a single laptop computer with unencrypted data can cost $90K due to requirements for victim notification, public relations efforts, class action lawsuits**

Law Enforcement Perspectives

- **2007 ID Analytics study**
  - **Real-people identify theft = 10-15% of all cases**
  - **Made-up identities fabricated with stolen data + false data = 85-90% of cases**
- **Identity Theft becoming #1 crime in USA**
  - **Majority of convictions are of repeat offenders**
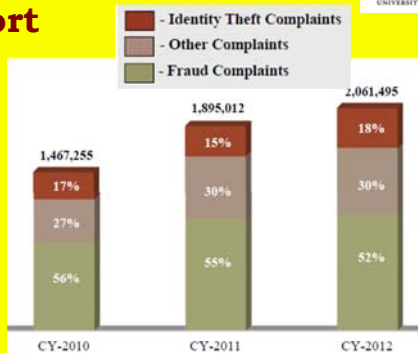 - **Criminals also involved in substance abuse, narcotics trafficking, violent crime & robbery**

Federal Trade Commission 2012 Report

- **Consumer Sentinel Network Complaint Type % 2010-2012**
- **ID theft #1 economic crime in USA**
  - **$21B stolen**
  - **12.6M victims**
- **Visit ITAC (Identity Theft Assistance Center) at**
  http://www.identitytheftassistance.org/pageview.php?cateid=47

Legend:
- Identity Theft Complaints
- Other Complaints
- Fraud Complaints

1,467,255 — CY-2010: 17% / 27% / 56%
1,895,012 — CY-2011: 15% / 30% / 55%
2,061,495 — CY-2012: 18% / 30% / 52%

http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

---

Techniques used by Identity Thieves

- **Carding**
- **Dumpster® Diving**
- **Skimming**
- **Shoulder Surfing**
- **Retail Scams**
- **Internet Scams**
  - **Phishing**
  - **Pharming**

Carding

- Stealing victim's credit card info
  - Often from unencrypted data on networks, laptop computers & stolen backup media
  - Using for theft
- Create fake credit cards
  - Numbers on cards include *check digits*
  - Programs on 'Net generate fake card numbers with valid check digits
- Deliver goods to real owner's address
  - Or later, to drop-point
- *QUESTION: why don't banks and other credit-card issues take better measures to prevent carding?*

The Shadowcrew Case

- Operation Firewall
  - US Secret Service
  - Investigated *Shadowcrew*
- Discovered international gang w/ 4000 members
  - Massive (>1.5M) credit-card number theft, ID theft
  - Phishing, spamming, sale of stolen goods through eBay, false ID documents (e.g., drivers' licenses) used for ID theft, creation of fake plastic credit cards, interstate wire transfers of illegal gains using e-money
  - Losses > $4M

Shadowcrew Prosecutions

- For full resources, go to
  - http://www.usdoj.gov/criminal/cybercrime/
  - Use search field with "Shadowcrew" as subject
- Indicted 19 leaders October 2004
  - http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm
- By November 2005 12 people had pleaded guilty to charges of conspiracy, trafficking in stolen credit card numbers, and causing more than $4M in losses
  - http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm

Shadowcrew Sentences

- Member sentenced February 2006
  - Kenneth J. Flury, 41, of Cleveland, OH
  - 32 mo in prison + 3 yrs supervised release
  - $300K restitution to CitiBank
  - http://www.usdoj.gov/criminal/cybercrime/flurySent.htm
- Co-founder sentenced June 2006
  - Andrew Mantovani, 24 of Scottsdale, AZ
  - Fined $5K + 32 mo prison + 3 years supervised release
  - 5 others sentenced at same time
  - By June 2006, 18 of 28 suspects arrested had pleaded guilty
  - http://www.usdoj.gov/usao/nj/press/files/mant0629_r.htm

Dumpster® Diving

- Get confidential information from garbage
  - People discard valuable data
    - ✓ Credit-card offers
    - ✓ Bank statements
    - ✓ Bills
    - ✓ Even computer disks, tapes
- NOT ILLEGAL to steal garbage placed on the curb in public space
- But *IS* illegal to use the information for identity theft
- SHRED confidential paper before discarding
- WIPE confidential data on disks or DESTROY magnetic/optical media before discarding

Industrial Espionage: Oracle vs Microsoft

Oracle Dumpster®-Dives vs MS (2000.06)

- Bill Gates complained about Dumpster® Diving of trash of organizations supporting MS in antitrust case
- CEO Larry Ellison of Oracle admitted using private detectives to go through trash of
  - Association for Competitive Technology
  - Independent Institute
  - Citizens for a Sound Economy
- Suggested he would happily ship Oracle trash to MS in spirit of full disclosure.

Credit-Card Skimming

- Criminal employees used to steal carbon papers from credit-card bills
  - Electronic devices don't have carbon papers
- Can dump data from electronic card readers
- New portable devices allow cards to be scanned for future theft
- Some ATMs equipped with fake readers on top of real card slot – record card data for later use or broadcast using wireless link
- CHECK YOUR MONTHLY CREDIT-CARD STATEMENTS RIGHT AWAY

Shoulder Surfing

- Observe key-entry on ATMs or phones from right behind user or even at a distance
- Some gangs caught using telephoto lenses on movie cameras
- Particularly common at crowded areas such as airports and bus terminals
- STAND CLOSE TO THE KEYPAD to block visual access
- WATCH OUT for people standing too close – tell them politely to back off

Retail Scams

- Criminals conspire to trick clerks into quizzing customers
  - Creep #1 stands near checkout
  - Creep #2 phones clerk & claims to be security officer
    - Tells clerk to assure customer that this is a routine security check to prevent fraud
    - Demands details of ID to be read over phone
    - Everything is then OK – but ID theft is in progress

Retail Scams (2)

- Some stores offering automated access to new store credit-cards
  - Terminals ask for SSN as sole identifier
  - Criminals use someone else's SSN to set up card
  - *Jackpot* the card at victim's expense
- Suborning employees
  - Criminals bribe employees to release list of credit-card transactions
  - Access to dozens or hundreds of valid card #s and names

Internet Scams

- Packet sniffing
  - Capture TCP/IP traffic with identifying data
  - Need access to server where data are received
  - Or can use keystroke logger on victim's own computer
- Phishing ("subscriber account update")
  - See following slides taken from presentation to a meeting of NE ISSA (New England Information Systems Security Association)
- Pharming: putting up fake Web sites

Phishing

- Come with me, little child
- Phishing Basics
- Examples of Attacks
- Effects
- Anti-Phishing Measures
- Public Education
- Possible Solutions

Image provided courtesy of
How Stuff Works.com
http://computer.howstuffworks.com

Come With Me, Little Child

Microsoft   All Products | Support | Search | Microsoft.com Guide
Microsoft Home

Microsoft Customer

This is the latest version of security update, the 'September 2003, Cumulative Patch' update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three new vulnerabilities. Install now to help maintain the security of your computer from these vulnerabilities. This update includes the functionality of all previously released patches.

25

Phishing Basics (1)

- Pronounced "fishing"
- Scam to steal valuable information such as credit cards, social security numbers, user IDs and passwords.
- Also known as "brand spoofing"
- Official-looking e-mail sent to potential victims
  - Pretends to be from their ISP, retail store, etc.,
  - Due to internal accounting errors or some other pretext, certain information must be updated to continue the service.

26

Phishing Basics (2)

- Link in e-mail message directs the user to a Web page
  - Asks for financial information
  - Page looks genuine
    - ✓ Easy to fake valid Web site
    - ✓ Any HTML page on the real Web can be copied and modified
- E-mails sent to people on selected lists or to any list
  - Some % will actually have account
- "Phishing kit"
  - Set of software tools
  - Help novice phisher imitate target Web site
  - Make mass mailings
  - May include lists of e-mail addresses

> From *Computer Desktop Encyclopedia v17.4*
> *http://www.computerlanguage.com/*

27

Serious Problem

"Illegal access to checking accounts, often gained via phishing scams, has become the fastest-growing form of consumer theft in the United States, accounting for a staggering $2.4 billion in fraud in the previous 12 months."

-- Gartner Group

28

Examples of Attacks

- People's Bank - 'New Mail'
- Citibank - 'Alert Service'
- Paypal - 'Your Account Will Be Suspended'
- Sovereign Bank - 'Unauthorized Account Access'
- Citibank - 'Security Alert on Microsoft Internet Explorer'
- eBay - 'TKO NOTICE: Verify Your Identity'
- Verizon - 'Update your Verizon billing profile'
- Washington Mutual Bank – 'Internet Banking Account'

29

People's Bank

peoples.com

Dear People member.
We ask you to confirm immediately of your parity the account to given e-mail.

www.people-onlinebank.net

Otherwise we stop temporarily service of your account.
Thank you for using Suntrust Bank!

Please do not reaply this letter.
Again, thank you for using People.com

> Not the proper domain for peoples.com

30

Citibank (Nov 10)

Dear Citibank Customer

We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking here.

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

Links to http://82.90.165.65/citi

PayPal (1)

PayPal®

Security Center

Military Grade Encryption is Only the Start

At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.

PayPal (2)

Actually links to http://212.45.13.185/.paypal/index.php

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend to verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,
PayPal Account Review Department
PayPal, an eBay Company

PayPal VERIFIED

Citibank (Nov 1, 2004)

Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced some new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

This security update will be effective immediately. Please sign on to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.

Citibank Online

Copyright © 2004 Citicorp

Links to http://200.189.70.90/citi/

---

eBay (1)

eBaY

Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below.

https://scgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo

If your account information is not updated within **48 hours** then your ability to sell or bid on eBay will become restricted.

http://signin-ebay.com-cgi-bin.tk/eBaydll.php

---

eBay (2) – Detailed Analysis

Received by MK 2004-11-17

Welcome to eBay

— **Dear valued customer**   ⑦ Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

TRUSTe site privacy statement

eBay(2) Source Code

Extract of relevant section:

<p><STRONG><FONT face=arial>We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please </FONT><A

href="**http://203.251.21.2/**signin.ebay.com/ws2/eBayISAPI.dll/b2baf0b6a57d39abd6c44b48d6fe3559112c21e54b7e705ecc5116b3c7c38c37949e8aa81848934faf0821be04210e8c2ded3c4159edbee3ee1439f3892a3e91/"

target=_blank><FONT face=arial color=#0000ff>click here</FONT></A></STRONG><FONT face=arial> and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.
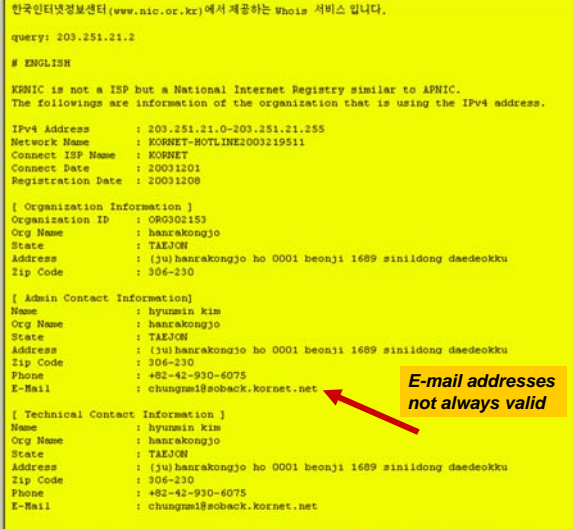
---

eBay (2) Reverse IP Lookup
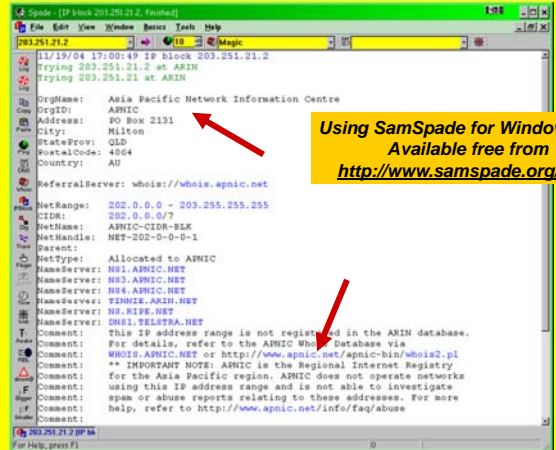
Using SamSpade for Windows v1.4 Available free from http://www.samspade.org/ssw/

---

eBay (2) APNIC R-IP Lookup

Asia-Pacific Network Information Center Routes to KoreaNIC

---

eBay (2) KRNIC R-IP Lookup

E-mail addresses not always valid

Get a Job – and Lose Money

➢ **Free training offer is another spam scam**
- ❑ **By John Leyden**
- ❑ **Published Tuesday 2nd November 2004 12:35 GMT**
- ❑ **http://www.theregister.com/2004/11/02/training_spam_scam/**

➢ **Apply for "training" and "job" at Credit Suisse**

➢ **Fill in banking details (!)**

➢ **Lose control over your financial information to criminals**

Phishing Harms Firms

➢ **Harmful at many levels**
- ❑ **Threatens effective communication**
- ❑ **Undermines goodwill and trust**

➢ **Customers**
- ❑ **Direct harm from stolen IDs, passwords**
- ❑ **Could perceive business as not taking adequate steps to protect users**

➢ **Diminishes value of brand**
- ❑ **Could affect shareholders**
- ❑ **Possibility of liability for failure to exercise due diligence in protecting trademark**

Anti-Phishing Measures

Proclaim, Protect, Pursue
- **Proclaim in all correspondence the use of an official mark (e.g. TrustedSender stamp)**
- **Protect all messages, Web pages with the mark**
- **Pursue all impostors – actively seek reports of phishing**

Certified By **ePrivacy** GROUP. **TRUSTED SENDER™** CLICK TO VERIFY 19SEP 2002
From: customerservice@smartcompany.com
To: joseph.consumer@address.com

43

Public Education

- **Use digitally-signed documents ONLY**
  - **Don't release unsigned documents**
  - **Get consumers used to idea that an unsigned document is an untrustworthy document**
- **Use public education campaigns**
  - **"No one will ever ask you to confirm your password"**
  - **"Don't believe alerts that address you as 'Dear Customer.'"**
  - **Link to APWG documents; e.g.,**
  - **http://www.antiphishing.org/consumer_recs.html**

44

Possible Solutions

- **Strong Website authentication**
- **Mail server authentication**
- **Digitally-signed e-mail with desktop verification**
- **Digitally-signed e-mail with gateway verification**

AWPG: *Proposed Solutions to Address the Threat of Email Spoofing Scams*
http://tinyurl.com/5bo55

45

Authenticating a Website to a Registered User

Bank of America

Confirm that your SiteKey is correct

If you recognize your SiteKey image, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey image is also how you'll know that it's safe to enter your Passcode.

Your SiteKey:

My Totem Animal

If you don't recognize your personalized SiteKey, don't enter your Passcode.

* Passcode :

(8 - 20 Characters, case sensitive)

- **User chooses from large range of photos**
- **Associates a specific photo with logon**
- **After entering userID, user sees login page with chosen image**
- **If image matches recollection, user can safely enter password**
- **See Kabay, M. E. (2007). "SiteKey tries to counter phishing."** *Network World Security Strategies.* **http://tinyurl.com/3mepsz**

APWG Resources Page (Sep 2009)
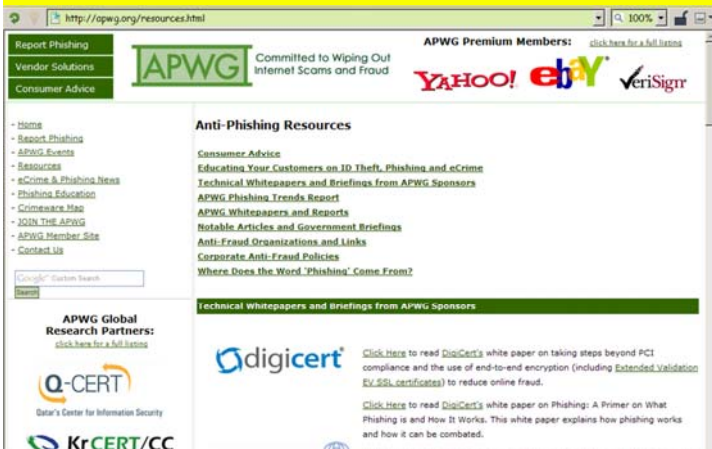
Government Involvement

- **Criminals forge government IDs for social engineering**
- **Some agencies are lax in verifying identity when issuing identifying documents**
- **Some government agencies post confidential data on Web without adequate safeguards**
  - **Include unnecessary details such as SSN**
- **Theft from USPS system can provide valuable documents**
  - **Applications, new credit cards, new documents**
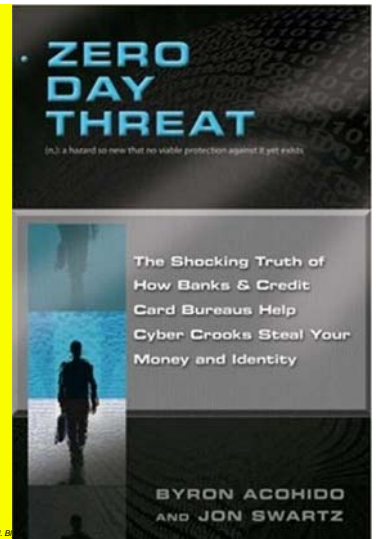
48

Responding to ID Theft

- Prevent theft: restrict access to your SSN and other personal data
  - SSN may be required by SSA, IRS employer, financial institution, lender
  - Corner store or video rental should NOT be given SSN
- NEVER give out credit-card or other personal data over the phone to someone *who has called you*. Ask for written documents.
- Shred papers that include confidential info before discarding.
- Destroy computer media before discarding.

49

Interesting Book (2008)

- Journalists
- Appeal to non-technical readers
- Good stories of specific computer criminals followed chapter by chapter
- Analysis of structural weaknesses in banking and credit systems
- ISBN 1-402-75695-X
- 304 pp, $13.57 (Amazon, Sep 2008)

50

ZERO DAY THREAT

(n.): a hazard so new that no viable protection against it yet exists

The Shocking Truth of How Banks & Credit Card Bureaus Help Cyber Crooks Steal Your Money and Identity

BYRON ACOHIDO AND JON SWARTZ

Now go and study

51