Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

CIC
Centro de Investigación en Computación

Laboratorio de Ciberseguridad

Centro de Investigación en Computación(CIC)
Instituto Politécnico Nacional - México.

Cyber security A-15

Dr. Ponciano Jorge Escamilla Ambrosio
pescamilla@cic.ipn.mx
http://www.cic.ipn.mx/~pescamilla/

Cyber security course

2.6. Internet Fraud

2.7. Electronic Evidence

2.8. Cybercrime

Internet Fraud

Internet Fraud

Refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet Fraud

- The Internet has transformed our lives.
- It offers tremendous opportunities to learn, share, connect, shop, and bank.

As we increasingly engage online, criminals follow the traffic!

Internet Fraud

- Fraud on the Internet is aimed mostly at individuals.
- Online fraud victimizes millions of unsuspecting people every year.
- In the USA the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted dollar loss of nearly half a billion dollars.

Internet Fraud

Internet Fraud in Mexico

	2010-2011*
Prevalence: Companies affected by fraud	69%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Corruption and bribery (37%) Theft of physical assets or stock (31%) Information theft, loss, or attack (27%) Internal financial fraud or theft (23%) Vendor, supplier or procurement fraud (21%) Management conflict of interest (21%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (81%) Theft of physical assets or stock (65%) Information theft, loss, or attack (58%)
Increase in Exposure: Companies where exposure to fraud has increased	82%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT Complexity (35%)
Loss: Average percentage of revenue lost to fraud	2.2%

*Insufficient respondents in 2010 to provide comparative data.

Internet Fraud

- There is a clear shift in the nature of the operation of computer criminals.
- In the early days, many hackers simply wanted to gain fame or notoriety by defacing websites.
- There are many more criminals today, and they are more sophisticated and technical experts.

Internet Fraud

Most popular is the theft of personal information such as credit card numbers, bank accounts, Internet IDs, and passwords.

Internet Fraud

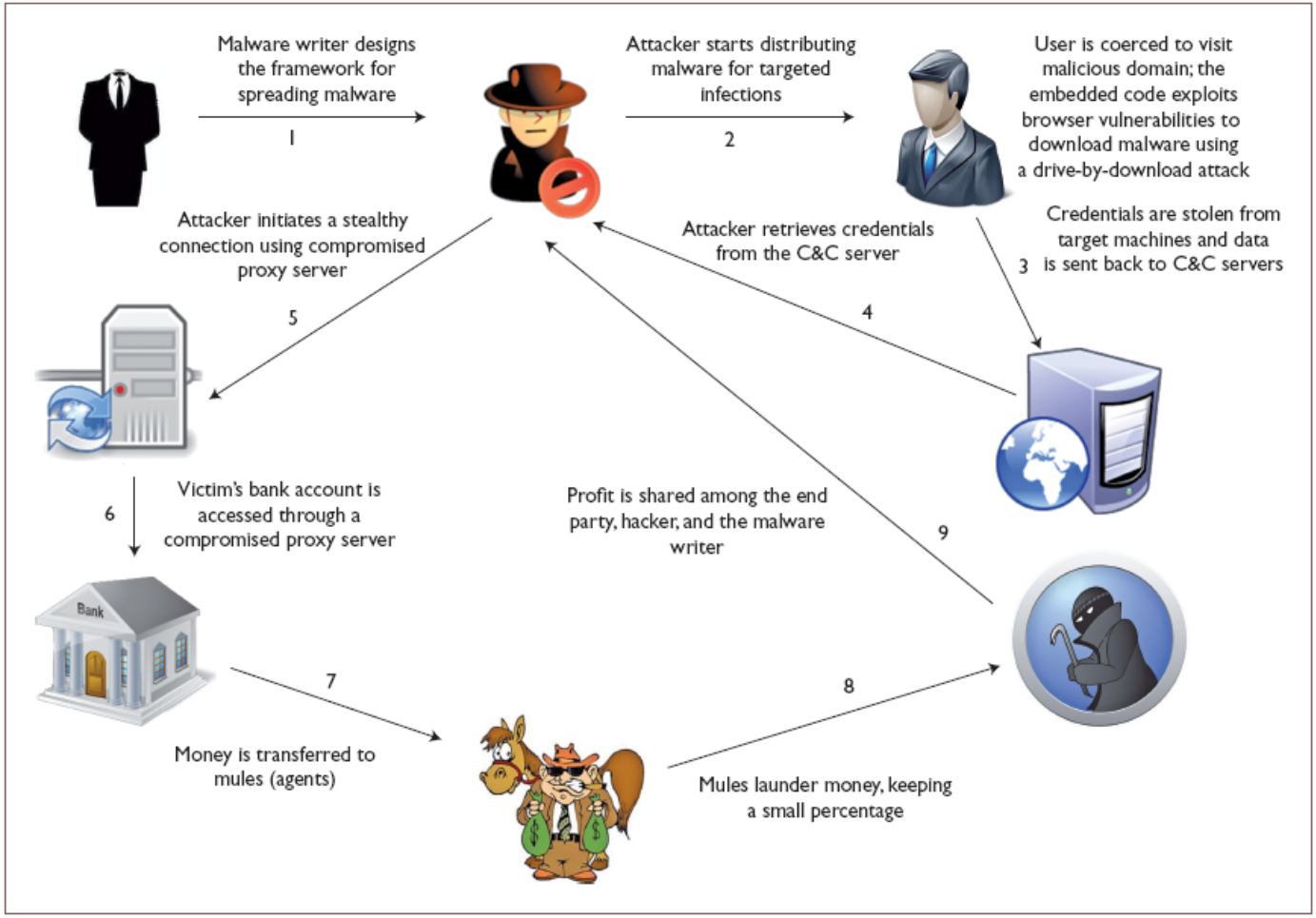
- Today cybercriminals are holding data for ransom and trying to extort payments from their victims.

http://usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633

Internet Fraud

- Today laptop computers are stolen for two reasons:
  - selling them (e.g., to pawn shops, on eBay)
  - trying to find the owners' personal information (e.g., social security number, driver's license details, and so forth).
- A major driver of data theft and other crimes is the ability to profit from the theft.
  - Today, stolen data are sold on the black market

Online Fraud Life Cycle



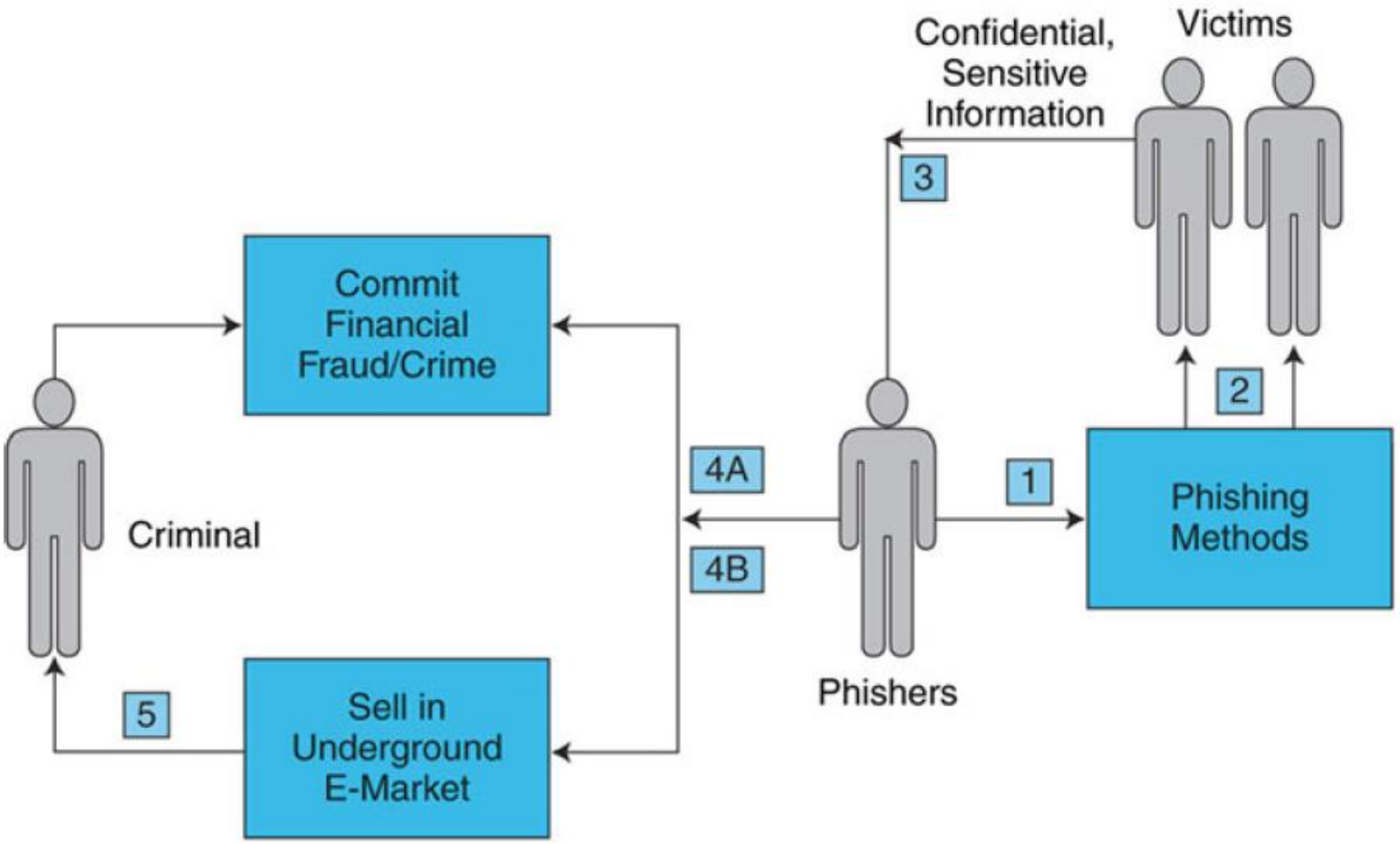
Social Engineering and Fraud

- Social engineering refers to a collection of methods where criminals use human psychology to persuade or manipulate people into revealing their confidential information so they can collect information for illegal activities.

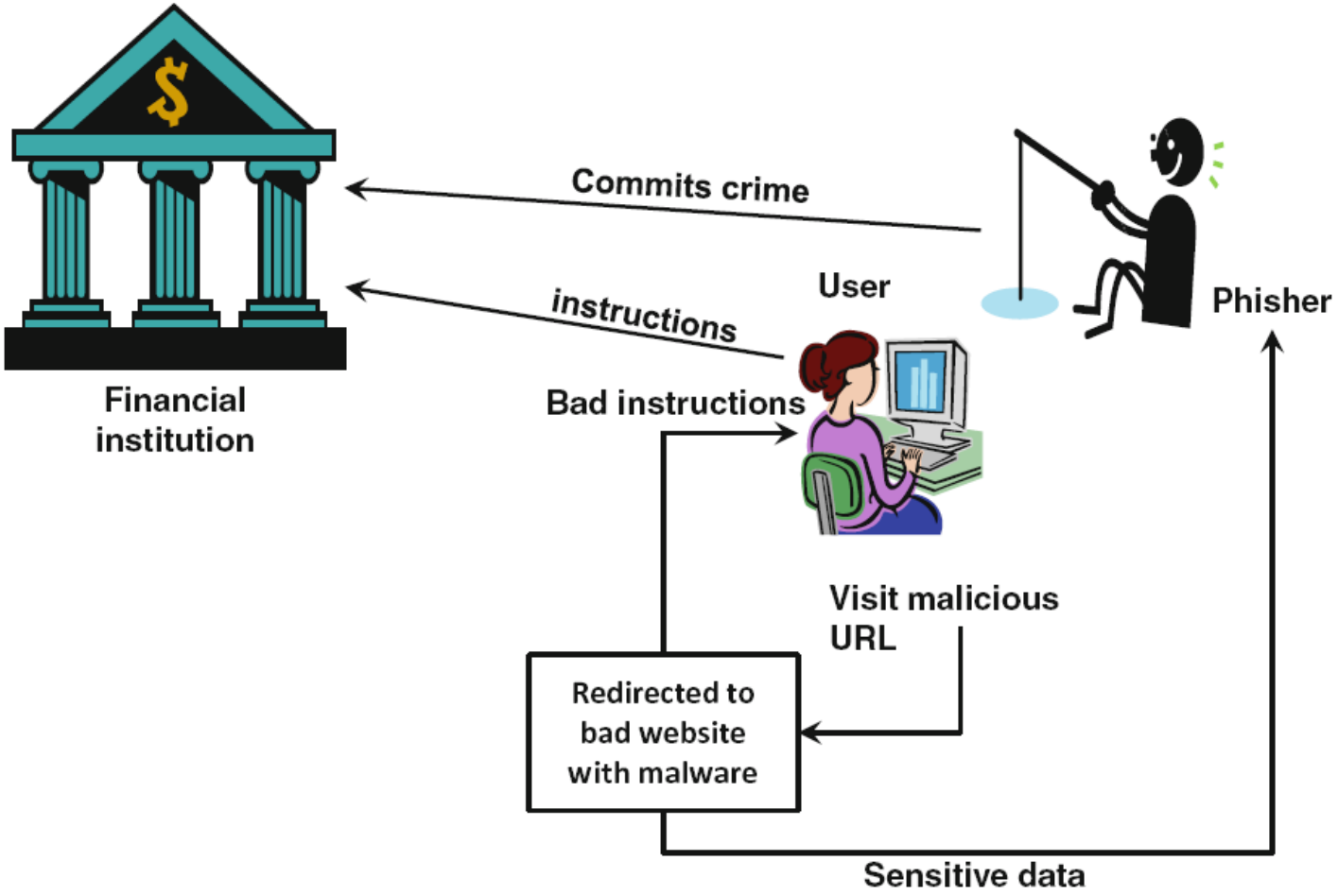
Social Phishing

- Phishing is a fraudulent process of acquiring confidential information, such as credit card or banking details, from unsuspecting computer users.
- Sometimes phishers install malware to facilitate the extraction of information.

Phishing


Confidential,
Sensitive
Information
Victims
3
Commit
Financial
Fraud/Crime
2
4A
1
Phishing
Methods
Criminal
4B
Phishers
5
Sell in
Underground
E-Market

Phishing


Commits crime
instructions
User
Phisher
Financial institution
Bad instructions
Visit malicious URL
Redirected to bad website with malware
Sensitive data

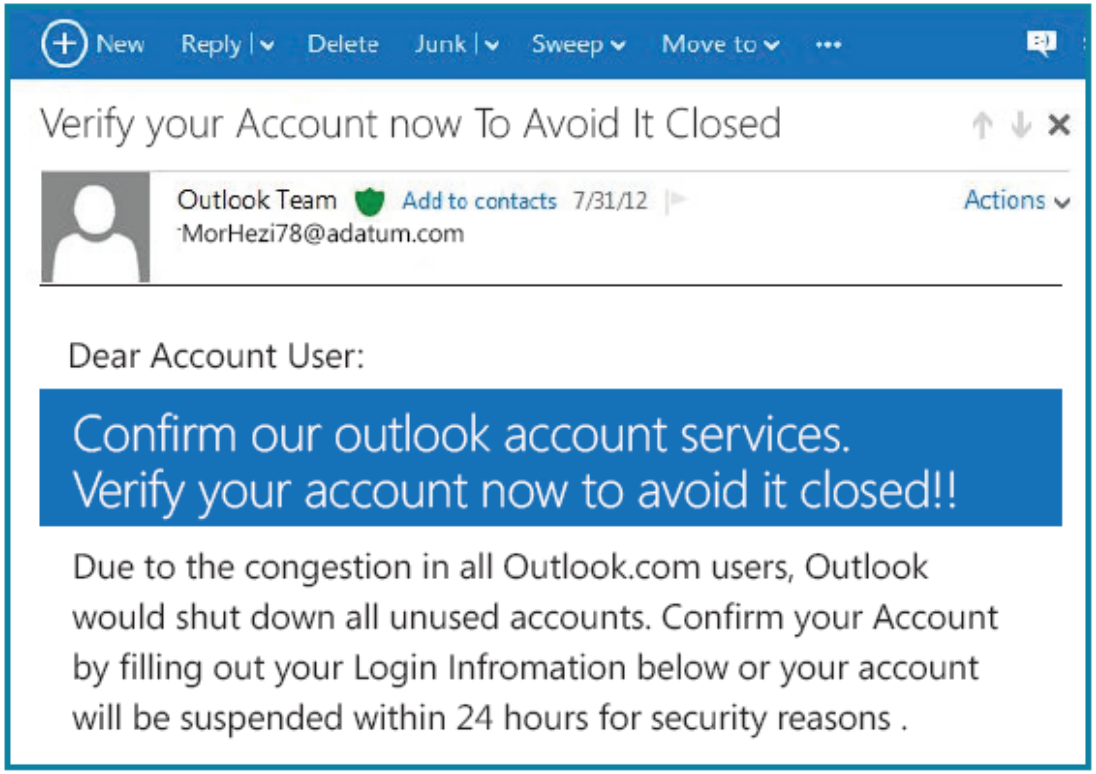
Phishing scams

- These scams use email, text, or social network messages that appear to come from a reputable organization like your bank or a favourite charity—or, for example, the Outlook team. The message is often so realistic that it can be difficult to tell it is not legitimate.

Phishing scams

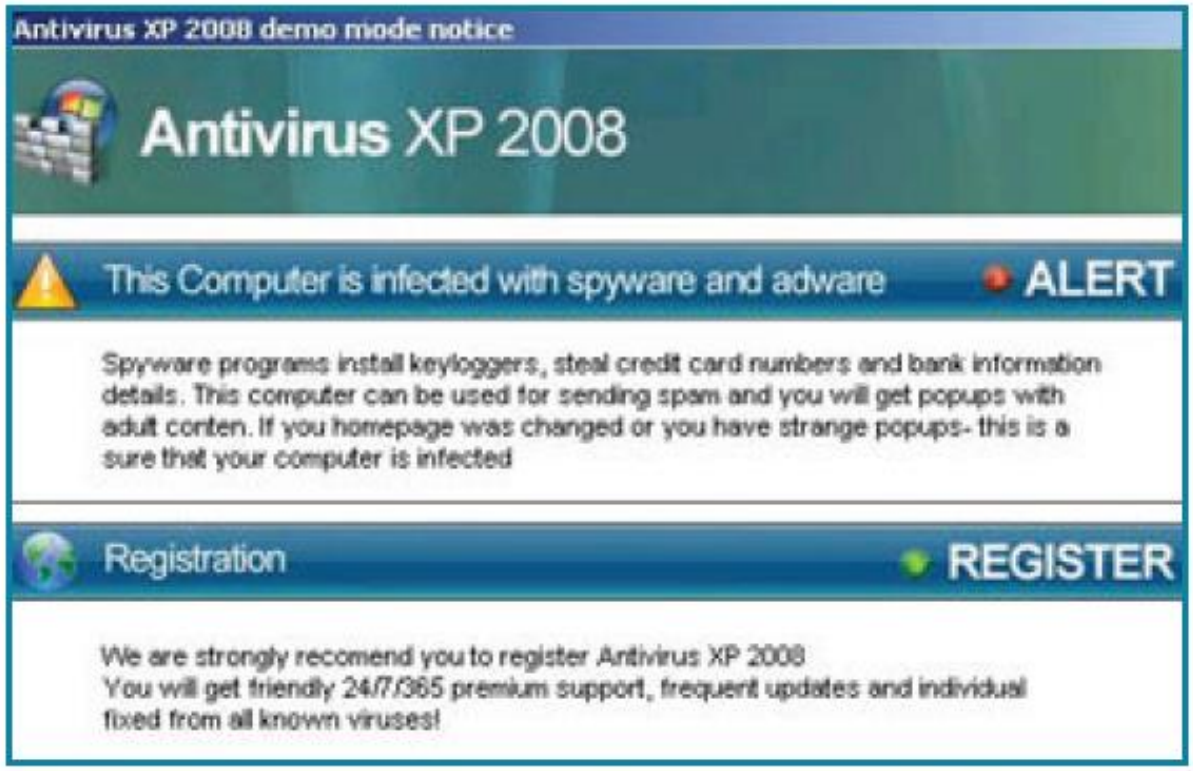
- The convincing message entices you to divulge sensitive information like an account number or password. Or it might ask you to call a phony toll-free number or to click a link that goes to a fake webpage where you're asked to reveal personal data.

Phishing example



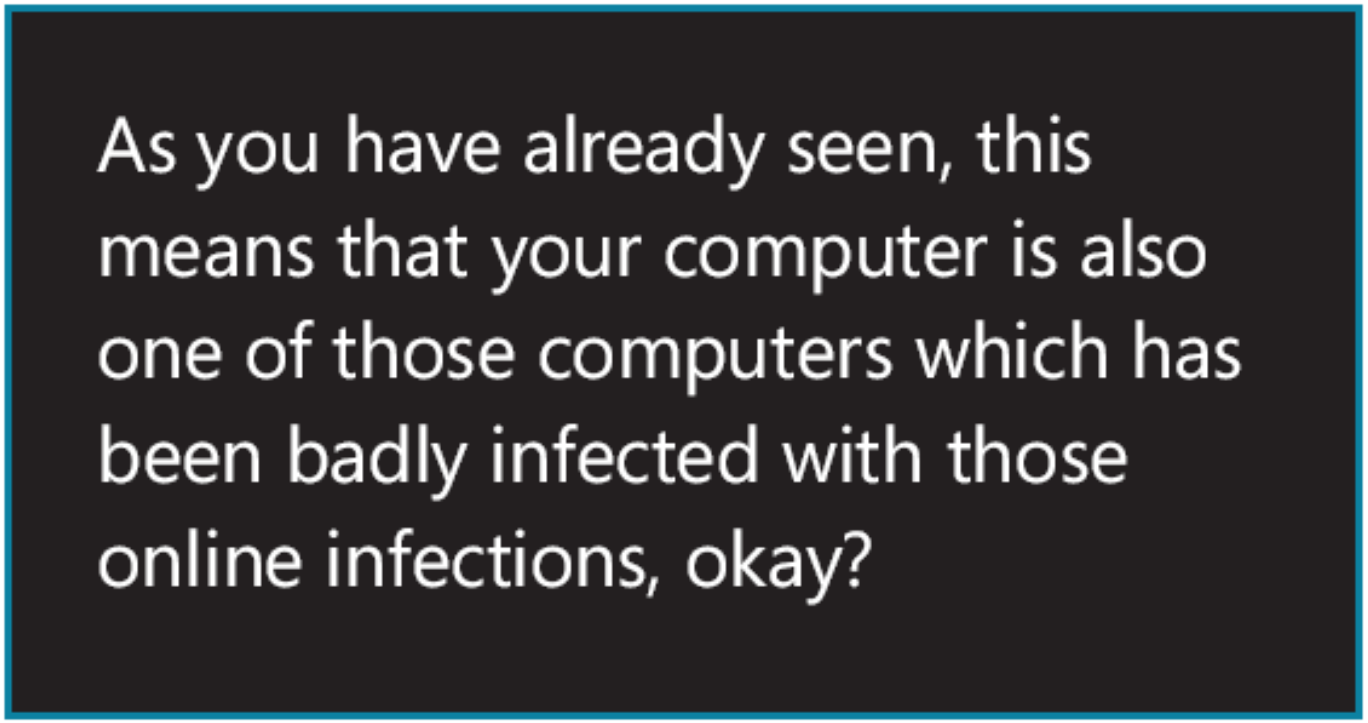
In this example, phishers try to trick Outlook users into giving sensitive information using the threat of account closure.

Rogue security software



This fake warning, disguised as a Microsoft alert, promotes a rogue security program.

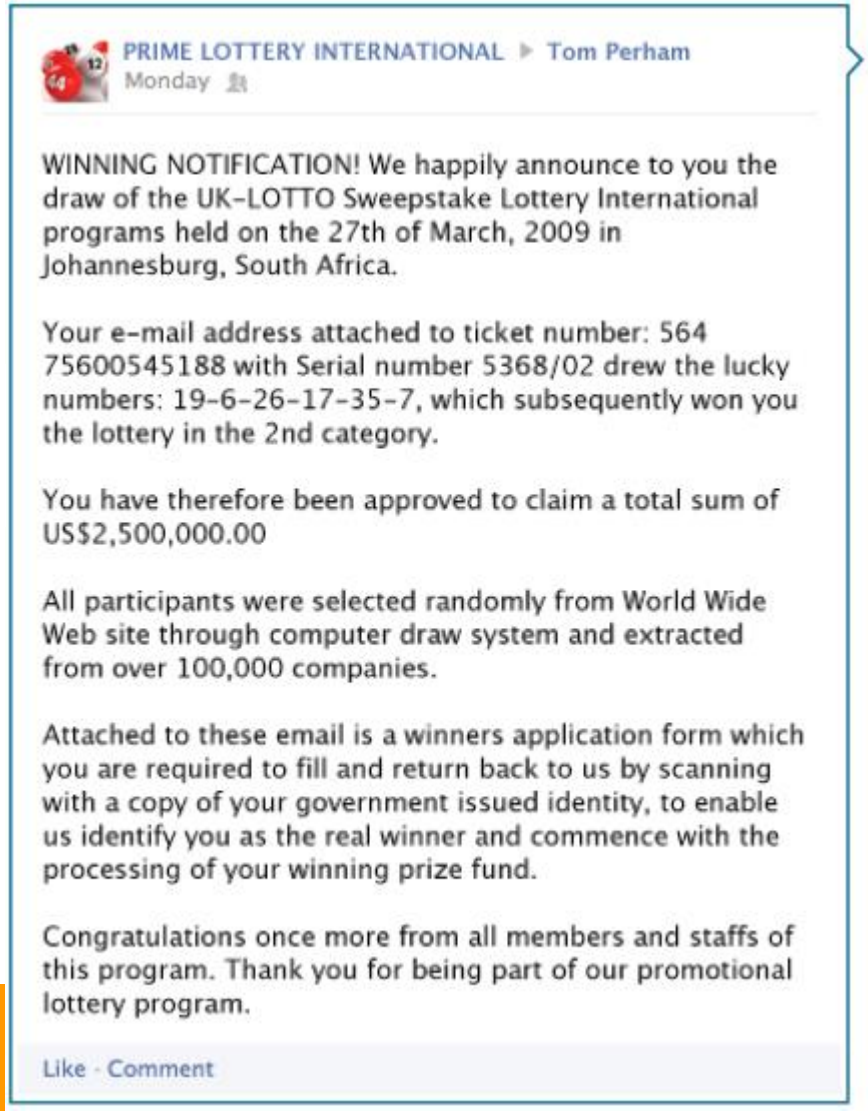
Fake technical support



Here a scammer tried to convince an FTC investigator that her computer was infected with a virus.

Fraudulent contest and winnings

This fake Facebook message claimed that the recipient had won a lottery and asked him to provide a copy of his government-issued identity.



PRIME LOTTERY INTERNATIONAL ▸ Tom Perham
Monday

WINNING NOTIFICATION! We happily announce to you the draw of the UK-LOTTO Sweepstake Lottery International programs held on the 27th of March, 2009 in Johannesburg, South Africa.

Your e-mail address attached to ticket number: 564 75600545188 with Serial number 5368/02 drew the lucky numbers: 19-6-26-17-35-7, which subsequently won you the lottery in the 2nd category.

You have therefore been approved to claim a total sum of US$2,500,000.00

All participants were selected randomly from World Wide Web site through computer draw system and extracted from over 100,000 companies.

Attached to these email is a winners application form which you are required to fill and return back to us by scanning with a copy of your government issued identity, to enable us identify you as the real winner and commence with the processing of your winning prize fund.

Congratulations once more from all members and staffs of this program. Thank you for being part of our promotional lottery program.

Like · Comment

Financial scams

These are examples of false promises made in financial scams.

Pharming

- Similarly to phishing, pharming is a scam where malicious code is installed on a computer and used to redirect victims website's traffic to a bogus websites without their knowledge or consent.
- Pharming is directed towards large groups of people at one time via domain spoofing.
- Pharming can be used for identity theft scams.

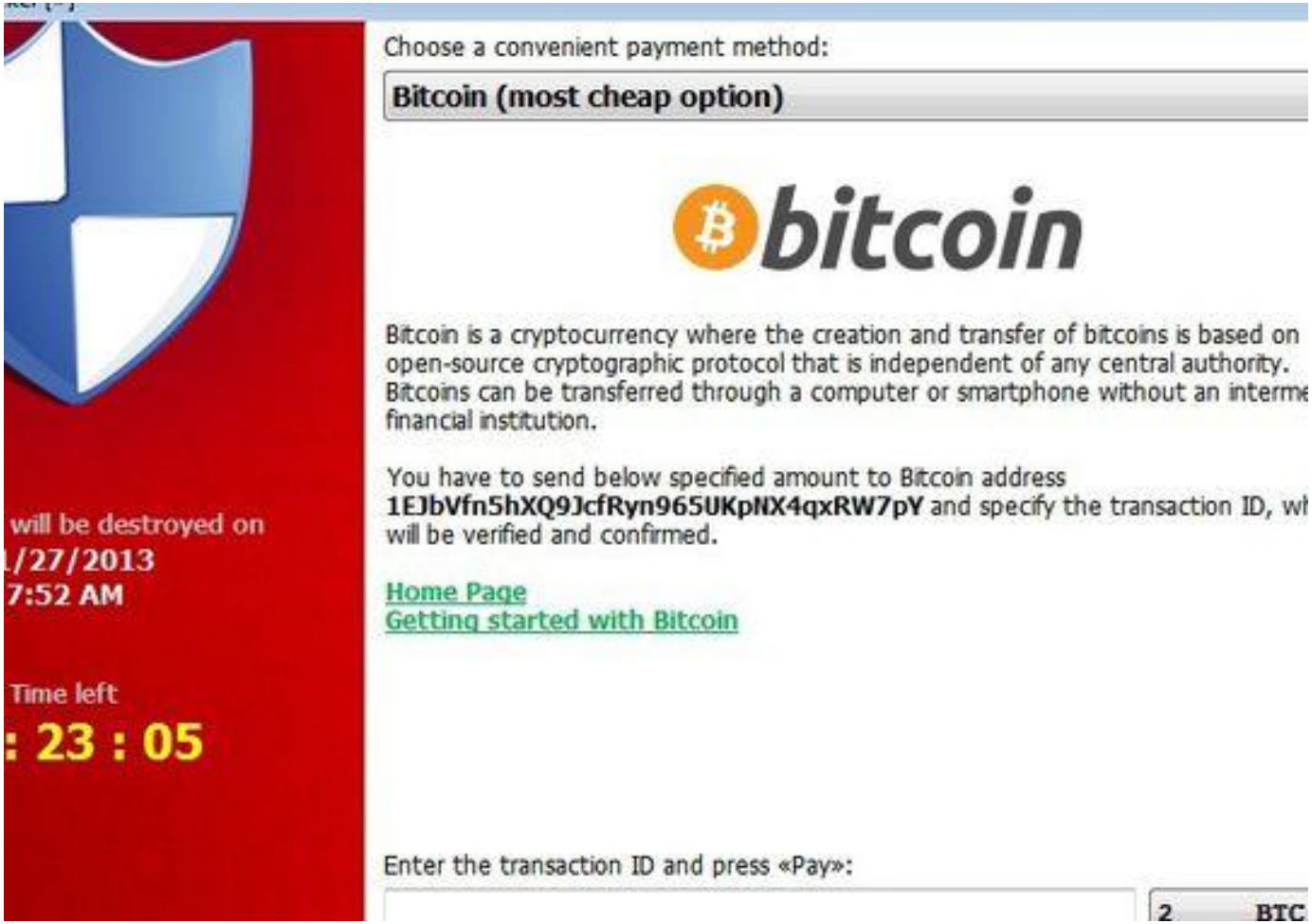
Ransomware

Example of monitor display when a computer is infected with Reveton ransomware.

New Internet Scam

'Ransomware' Locks Computers, Demands Payment

Ransomware

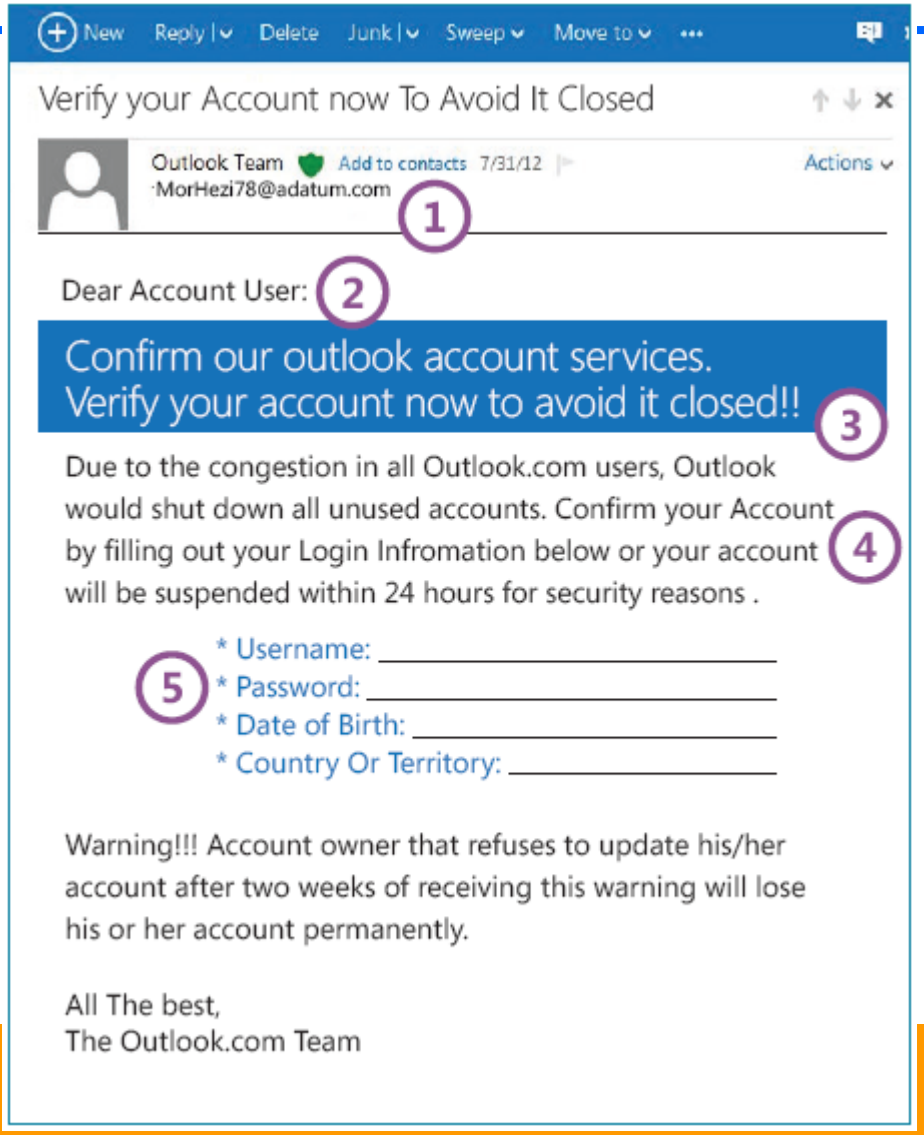

Choose a convenient payment method:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an interme financial institution.
You have to send below specified amount to Bitcoin address 1EJbVfn5hXQ9JcfRyn965UKpNX4qxRW7pY and specify the transaction ID, wh will be verified and confirmed.
Home Page
Getting started with Bitcoin
will be destroyed on
1/27/2013
7:52 AM
Time left
: 23 : 05
Enter the transaction ID and press «Pay»:
2 BTC

Identity Theft and Identity Fraud

- **Identity theft** refers to wrongfully obtaining and using the identity of another person in some way to commit crimes that involve fraud or deception (e.g., for economic gain).
- **Identity fraud** refers to assuming the identity of another person or creating a fictitious person and then unlawfully using that identity to commit a crime.

Spot the signs of online fraud

1. A suspicious email address. (Note that although it says it's from the Outlook team, the email address is not an Outlook address.)
2. Generic salutations rather than using a name.
3. Alarmist messages or urgent requests to download or install something. The scammer is trying to create a sense of urgency so you'll respond without thinking.
4. Grammatical errors and misspellings, which are used to break through phishing filters.
5. Requests to verify or update your account, stop payment on a charge, and the like.



Defense against Internet fraud

- If it sound to good to be true, suspect!!

① Treat suspicious messages cautiously

The most dangerous scams are those that look genuine.
In general, be wary of the sender, even someone you know or a company you trust.

- Don't respond to the message even to remove your address from the sender's list. Responding lets the sender know that you exist and could result in even more messages.
- Think before you click links or call a number in a message, even if you know the sender; the links, phone number, and sender's identity could all be phony. Instead, confirm with him or her, using a different device and another account, that the message is genuine.

Defense against Internet fraud

② Protect sensitive information

Don't put sensitive information in an email, instant, or text message or unexpected pop-up windows.

Look for evidence that a webpage is secure and legitimate before you enter sensitive data.

- Check the web address for https ("s" stands for secure) and a closed padlock. (The lock might also appear in the lower right corner of the window.)

- Make sure that you're on the correct site—for example, on your bank's website, not a fake. One sign of trustworthiness is a green address bar, like the one above.

Save banking, shopping, downloading software, and other sensitive business for your home computer. When you use a public computer, or your own computer or mobile device over a public wireless connection, the security may be unreliable.

Defense against Internet fraud

Back up your data regularly. Make it a habit to save your data using either a cloud service or a detached hard drive (ideally, both). That way, you can recover it in case of loss.

Review your bank and credit card statements monthly. Look for unexplained charges or inquiries that you didn't initiate.

Keep your primary email address private. Only share it with people you know or with reputable organizations. Avoid listing your address or name on Internet directories and job-posting sites.

Windows Internet Explorer emphasizes the domain name in the address bar with black type and the remainder of the address is gray to make it easier to see a website's true identity.

Defense against Internet fraud

③ Strengthen your computer's defenses

Criminals try to install malware on computers that haven't been updated by exploiting older weaknesses in their software.

Keep all software up to date, including your web browser (like Windows Internet Explorer), operating system (like Windows), word processing, and other programs.

Subscribe to automatic updates whenever they are offered. For example, to automatically update all Microsoft software, go to www.update.microsoft.com.

Install antivirus and antispyware software from a trusted source. For example, Microsoft Security Essentials is a free program that helps guard against viruses, spyware, and other malware: www.microsoft.com/security-essentials.

Protect your wireless router with a strong password.

Never turn off the firewall on your computer. Turning it off even for a minute increases risk.

Don't follow the instructions of unsolicited callers or let them take control of your computer.

Defense against Internet fraud

④ Create strong passwords

Criminals often use automated programs to break into accounts guarded by simple passwords, such as "password" or "12345678."

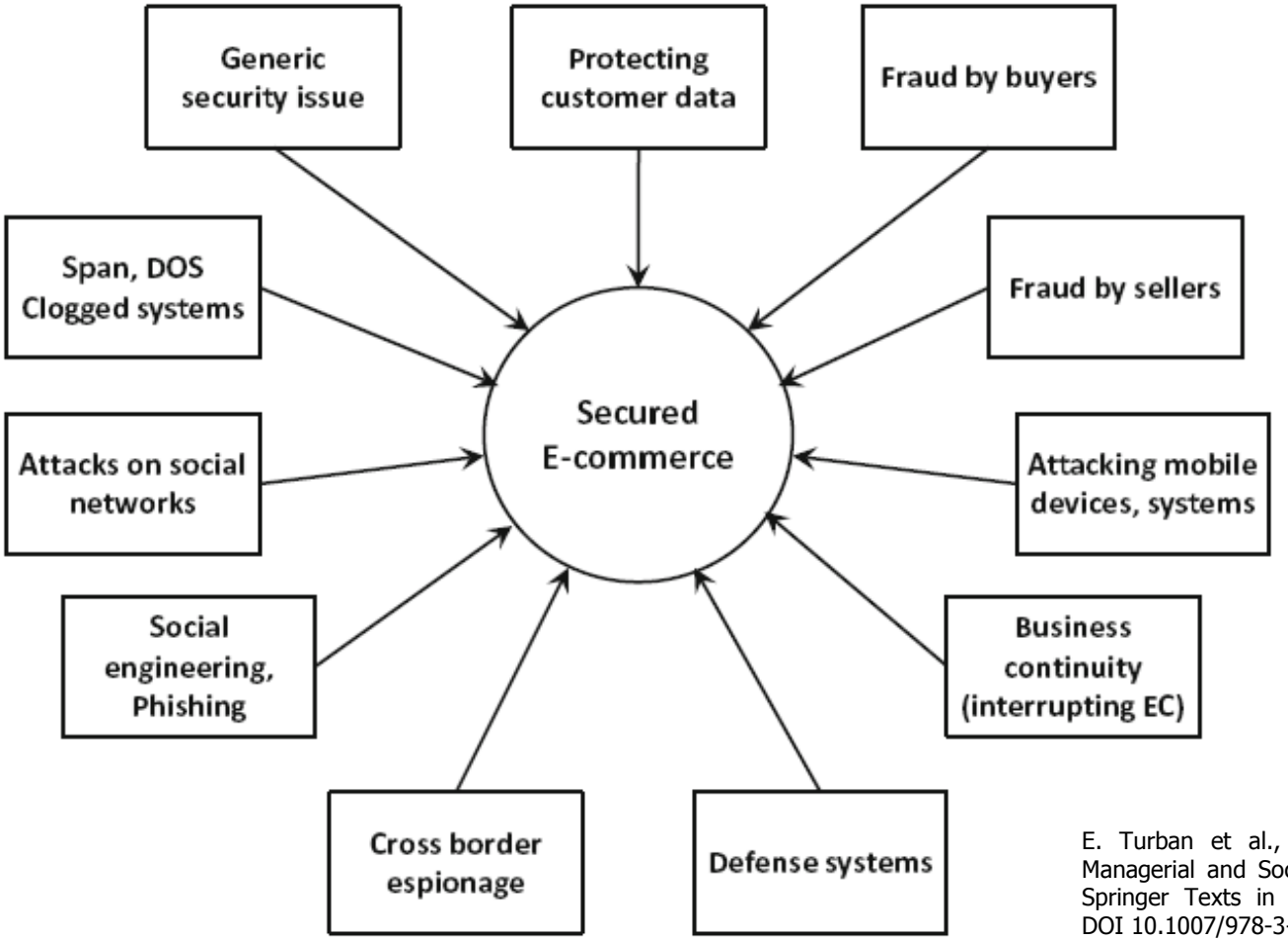
Strong passwords are long (phrases or sentences) that mix capital and lowercase letters, numbers, and symbols. They are easy for you to remember but difficult for others to guess.

Don't share your passwords with anyone.

Don't use the same password everywhere. If someone steals it, all the information that password protects is at risk.

Remember your passwords by storing them on a well-protected piece of paper away from your computer.

EC Security management concerns



E. Turban et al., Electronic Commerce: A Managerial and Social Networks Perspective, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-10091-3_10

The Information Assurance (IA) model

- CIA security triad:

  1. Confidentiality is the assurance of data secrecy and privacy. Namely, the data is disclosed only to authorized people. Confidentiality is achieved by using several methods, such as encryption and passwords.

  2. Integrity is the assurance that data are accurate and that they cannot be altered. The integrity attribute needs to be able to detect and prevent the unauthorized creation, modification, or deletion of data or messages in transit.

The Information Assurance (IA) model

- CIA security triad:

  3. Availability is the assurance that access to any relevant data, information websites, or other EC services and their use is available in real time, whenever and wherever needed. The information must be reliable.

Electronic Evidence

- Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer.
- Computer-based electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination.