Practice of Basic Informatics [Week 02 Mini Lecture] -Information Security-

Rafik Hadfi

Department of Social Informatics

Kyoto University

Email: rafik.hadfi@i.kyoto-u.ac.jp

A part of the slides are referred from Mark Zimmerman.

Overview of Information Security

What Is Information Security?

- Deals with several different "trust" aspects of information and its protection
- The U.S. Government's National Information Assurance Glossary defines **INFOSEC** as:

> *"Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats."*

Aspects of Information Security

What Is Information Security?

- Three widely accepted elements or areas of focus (referred to as the “CIA Triad”):
  - Confidentiality（機密性）
  - Integrity（完全性）
  - Availability（可用性）
- Includes Physical Security as well as Electronic

Aspects of Information Security (Cont.)

- Confidentiality: protecting information from unauthorized parties
  - Protecting against the **leakage** of information assets (data) to third parties
  - Taking actions against **interception**（傍受）, **eavesdropping** (盗聴) of ID and passwords
- Integrity: protecting information from modification by unauthorized users or by system itself
  - Protecting against data **corruption**, maintaining **complete** and **accurate** data
  - Taking action against the **falsification** (改ざん) or **vandalization**（破壊）of data, databases, web pages and E-mail header information
- Availability: making the information available to authorized users
  - Preventing system **downtime**, allowing information to be used at **all times** while also being in accordance with established procedures
  - Taking action against **vandalization** attempts such as “mail-bomb” attacks

Definitions: Malware

Malware:

- Hostile, intrusive, or annoying software or program code ("malicious" + "software“)
- Includes computer viruses, worms, trojan horses, bots, spyware, adware, etc.
- Software is considered malware based on the intent of the creator rather than any particular features

Definitions: Internet Bot

Internet bot:

– Also known as **web robots**, are automated internet applications controlled by software agents

– These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a humanlike manner (i.e., computer game bot)

– Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes.

– Botnet - a network of "zombie" computers used to do automated tasks such as spamming or reversing spamming

Definitions: Adware

Adware:

- **Advertising-supported software** is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- Adware is software integrated into or bundled with a program, typically as a way to recover programming development costs through advertising income

Definitions: Spyware

Spyware:

- A broad category of software designed to **intercept** or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user
- In simpler terms, spyware is a type of program that **watches** what users do with their computer and then sends that information over the internet

Definitions: Spyware (Cont.)

<u>Spyware</u>:

- Spyware can collect many different types of information about a user:
  - Records the types of websites a user visits
  - Records what is typed by the user to intercept passwords or credit card numbers
  - Used to launch “pop up” advertisements
- Many legitimate companies incorporate forms of spyware into their software for purposes of advertisement(Adware)

Definitions: Spam

Spam:

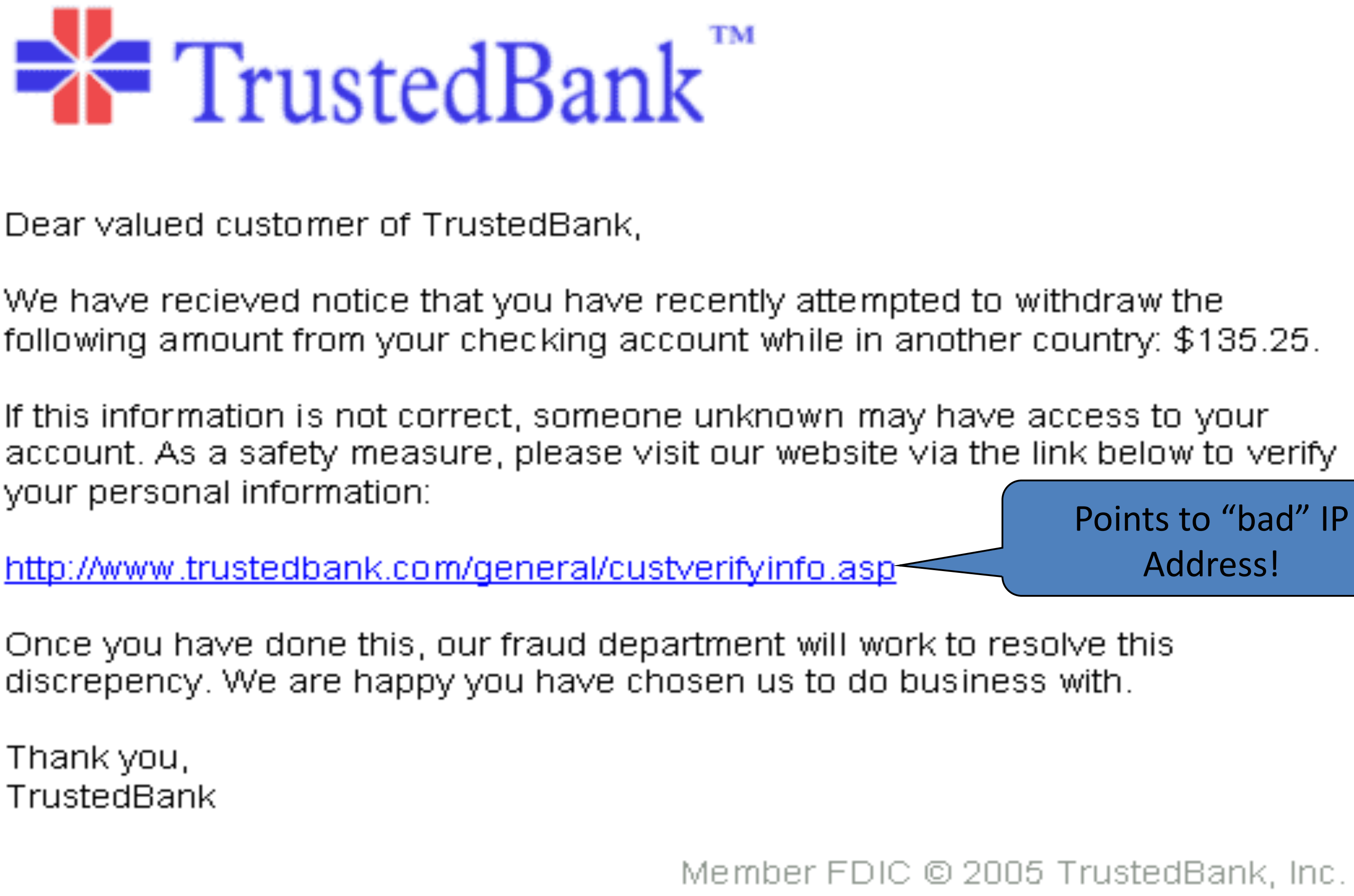
- **Spamming** is the abuse of electronic messaging systems to send unsolicited（迷惑）, undesired bulk messages
- Spam media includes:
  - e-mail spam (most widely recognized form)
  - instant messaging spam
  - Newsgroup spam
  - Web search engine spam
  - spam in blogs, SNS(twitter, facebook, etc.)
  - mobile phone messaging spam

Definitions: Phishing

Phishing:

- A criminal activity using social engineering techniques.
- An attempt to acquire sensitive data, such as passwords and credit card details, by masquerading（なりすまし）as a trustworthy person or business in an electronic communication.
- Typically carried out using email or an instant message

Phishing Example



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Points to "bad" IP Address!

Definitions: Keystroke Logging

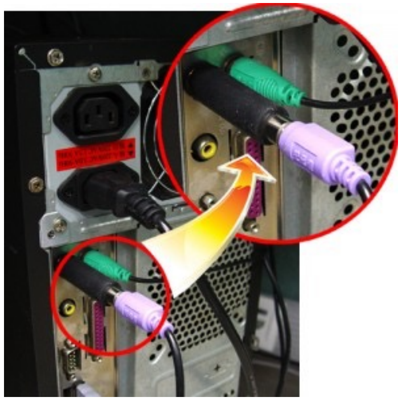
Keystroke Logging:

- Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes
  - Useful to determine sources of error in computer programs
  - Used to measure employee productivity on certain clerical tasks
- Highly useful for law enforcement and espionage（スパイ行為）
  - Obtain passwords or encryption keys and thus bypassing other security measures
- Widely available on the internet and can be used by anyone for the same purposes

Definitions: Keystroke Logging (Cont.)

Keystroke Logging:

- Can be achieved by both hardware and software means
- Hardware key loggers are commercially available devices which come in three types:
  - Inline devices that are attached to the keyboard cable
  - Devices installed inside standard keyboards
  - Keyboards that contain the key logger already built-in



Practice of Basic Informatics-E2 (Week 02)

Mini lecture of this week finished.