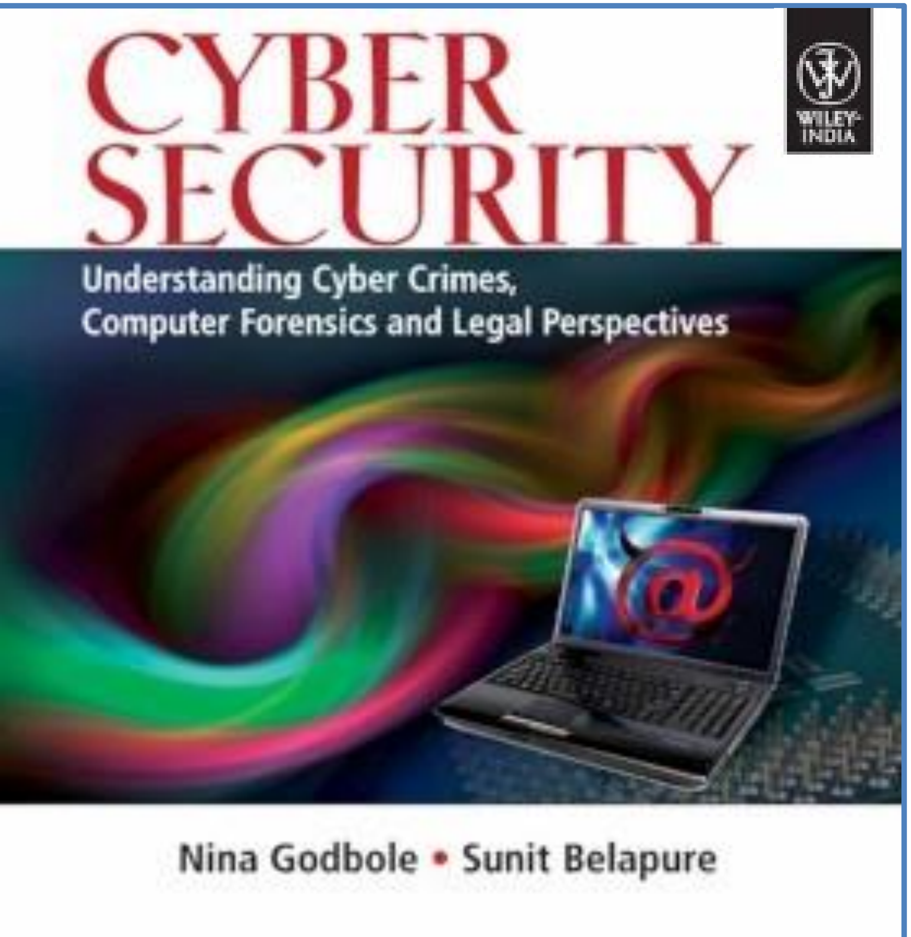
Chapter 5
Phishing and Identity Theft


CYBER SECURITY
Understanding Cyber Crimes, Computer Forensics and Legal Perspectives
WILEY-INDIA
Nina Godbole • Sunit Belapure

Unit-4
Lesson-5

Phishing and Identity Theft

Phishing

- ✓A type of e-mail scam that steals your identity.

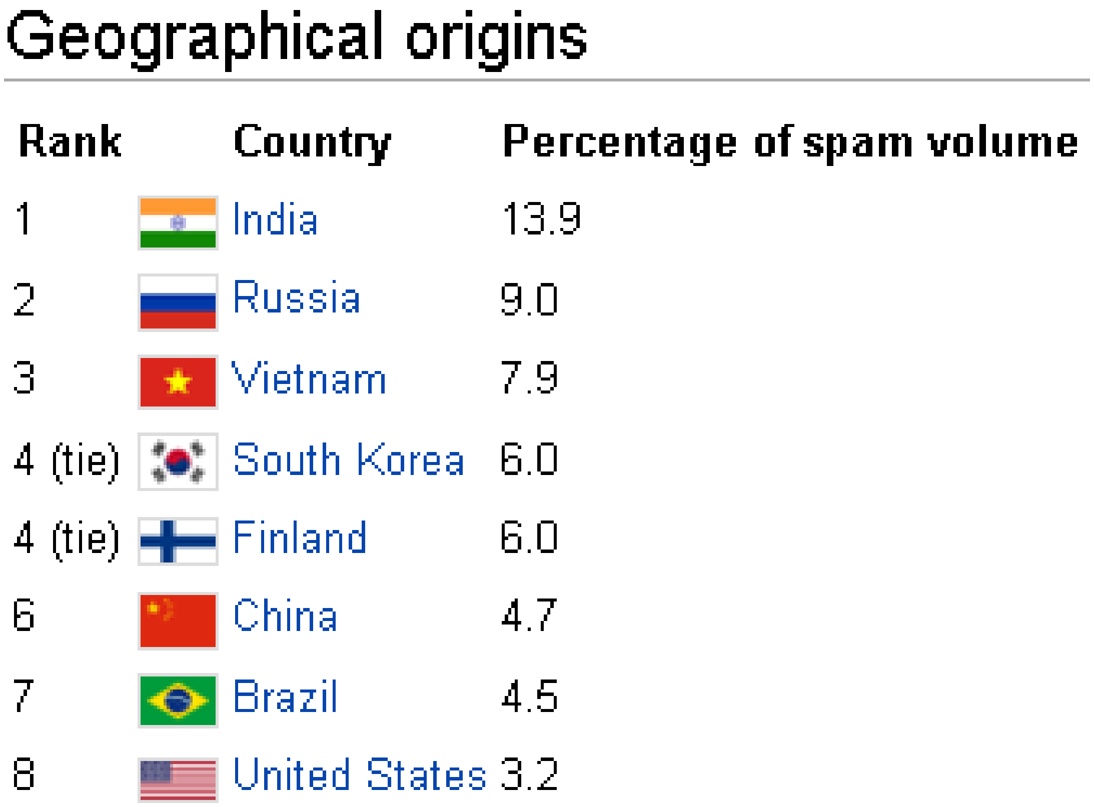
- ✓An e-mail fraud technique in which the culprit sends out e-mails looking legitimate in an effort to accumulate personal and financial information from recipients (messages likely come from well-known and trustworthy sites, viz., PayPal, eBay, MSN, Yahoo, BestBuy, and America Online).

- ✓Phishers use a different social engineering and e-mail spoofings to try to trick their victims.

- ✓The act of sending an e-mail to a user and falsely claiming to be an established legitimate organization to scam the user into giving up private information to be used for identity theft.

- ✓The e-mail steers the user to visit a Web site where they are asked to update their personal information, viz., their passwords and information about their credit cards, bank account numbers, etc.

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.



Geographical origins

Rank	Country	Percentage of spam volume
1	India	13.9
2	Russia	9.0
3	Vietnam	7.9
4 (tie)	South Korea	6.0
4 (tie)	Finland	6.0
6	China	4.7
7	Brazil	4.5
8	United States	3.2

(***Courtesy*** : 2011 Cisco System report)

Spam E-Mails

✓Also known as “junk E-Mails”

✓Identical messages are sent to numerous recipients

✓Popular medium for phishers to scam users to enter personal information on fake websites

✓A person who creates electronic spam is called a *spammer*

Types

1. Unsolicited bulk E-Mail (UBE)

2. Unsolicited commercial E-Mail (UCE)

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Tactics used by a phisher

1. Names of legitimate organizations
2. “From” a real employee
3. URLs that “look right”
4. Urgent messages

Phrases used to entice the user

1. “Verify your account”
2. “You have won the lottery”
3. “If you don’t respond within 48 hours, your account will be closed”

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Hoax E-Mails

✓Deliberate attempt to deceive or trick a user into believing or accepting that something is real.

✓Hoax E-Mails may or may not be Spam E-Mails.

Methods of Phishing

1. Dragnet (use of spammed E-Mails)

2. Rod-and-reel (identifying specific prospective victims in advance and convey false information to them to prompt their disclosure of personal and financial data)

3. Lobsterpot (focuses upon use of spoofed websites)

4. Gillnet (relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites)

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Phishing Techniques

1. URL (weblink) manipulation
2. Filter evasion
3. Website forgery
4. Flash Phishing
5. Social Phishing
6. Phone Phishing

Phishers usually send millions of E-Mail messages, pop-up windows, etc., that appear to be looking official and legitimate.

Spear Phishing

- ✓ A method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.
- ✓ Spear phishers send E-Mail that appears genuine
- ✓ The message might look like as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company (such as the person who manages the computer systems); it could include requests for usernames or passwords.

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Whaling

- ✓ A specific form of “Phishing” and/or “Spear Phishing” – targeting executives from the top management in the organizations, usually from private companies.

- ✓ The objective is to swindle the executives into revealing confidential information.

- ✓ Whaling targets C-level executives sometimes with the help of information gleaned through Spear Phishing, aimed at installing malware for keylogging or other backdoor access mechanisms.

- ✓ E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent from a legitimate business body and/or business authority.

- ✓ Whaling phishers have also forged official looking FBI subpoena E-Mails and claimed that the manager needs to click a link and install special software to view the subpoena.

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Types of Phishing Scams

1. Deceptive Phishing
2. Malware-based Phishing
3. Keyloggers
4. Session hijacking
5. In-session Phishing
6. Web Trojans
7. Pharming
8. System reconfiguration attacks
9. Data theft
10. Content-injection Phishing
11. Man-in-the-middle Phishing
12. Search engine Phishing
13. SSL certificate Phishing

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Distributed Phishing Attack (DPA)

An advanced form of phishing attack that works as per victim’s personalization of the location of sites collecting credentials and a covert transmission of credentials to a hidden coordination center run by the phisher.

✓A large number of fraudulent web hosts are used for each set of lured E-Mails.

✓Each server collects only a tiny percentage of the victim’s personal information.

Phishing Toolkits and Spy Phishing

✓A Phishing toolkit is a set of scripts/programs

✓Quite expensive

✓Phishers use hypertext preprocessor (PHP) to develop the Phishing kits.

✓Most of the Phishing kits are advertised and distributed at no charge and usually these *free Phishing kits* – also called DIY (Do It Yourself) Phishing kits.

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Phishing Countermeasures

✓The countermeasures prevent malicious attacks that phisher may target to gain the unauthorized access to the system to steal the relevant personal information about the victim, from the system.

✓It is always challenging to recognize/judge the legitimacy of a website while Googling.

SPS Algorithm to Thwart Phishing Attacks

✓With Sanitizing Proxy System (SPS), web Phishing attack can be immunized by removing part of the content that entices the netizens into entering their personal information.

✓SPS sanitizes all HTTP responses from suspicious URLs with warning messages.

Identity Theft (ID Theft)

✓Fraud that involves someone pretending to be someone else to steal money or get other benefits.

✓The person whose identity is used can suffer various consequences when he/she is held responsible for the perpetrator’s actions.

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Statistics as per Federal Trade Commission (FTC)

1. Credit card fraud (26%)
2. Bank fraud (17%)
3. Employment fraud (12%)
4. Government fraud (9%)
5. Loan fraud (5%)

Personally Identifiable Information (PII)

Fraudsters attempts to steal the elements mentioned below:

1. Full name
2. National identification number (e.g., SSN)
3. Telephone and mobile phone numbers
4. Driver’s license number
5. Credit card numbers
6. Digital identity (e.g., E-Mail address, online account ID and password)
7. Birth date and Place name
9. Face and fingerprints

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

A fraudster generally searches the following about an individual:

1. First or last name
2. age
3. country, state or city of residence
4. gender
5. name of the school/college/workplace
6. job position, grades and/or salary
7. criminal record

Types of Identity Theft

1. Financial identity theft
2. criminal identity theft
3. identity cloning
4. business identity theft
5. medical identity theft
6. synthetic identity theft
7. child identity theft

Techniques of ID Theft

1. Human-based methods
2. Computer-based technique

Copyright © 2011 Wiley India Pvt. Ltd. All rights reserved.

Questions

- What is identity theft? Explain with examples.
- Differentiate between hoax mails and spam.
- Describe the different types of phishing scams
- What are the different phishing techniques? Explain
- What is spear phishing? Explain with examples.
- What is whaling?
- What are the different types of Identity thefts?
- Describe **Personally Identifiable Information (PII)**