Unit V – Phishing and Identity Theft

Content

- **Phishing:**
- Methods of Phishing
- Phishing Techniques, Spear Phishing
- Types of Phishing, Scams
- Phishing Toolkits and Spy Phishing
- Phishing Countermeasures
- **Identity Theft (ID Theft):**
- Personally Identifiable Information (PII)
- Types of Identity Theft
- Techniques of ID Theft
- Identity, Theft-Countermeasures
- Protecting one's Online Identity

INTRODUCTION

- Phishing is an online method used to “fish” for your personal information.
- Often people are not even aware that their personal information is being accessed online.
- When someone goes phishing for personal information and has obtained it, they can use it in a variety of ways.
- They may steal a person’s identity, open up new bank accounts, sign up for credit cards, or wipe out a person’s entire bank account.
- Victims of phishing believe that they are giving up their personal information to trusted and legitimate financial institutions, government agencies, and businesses.

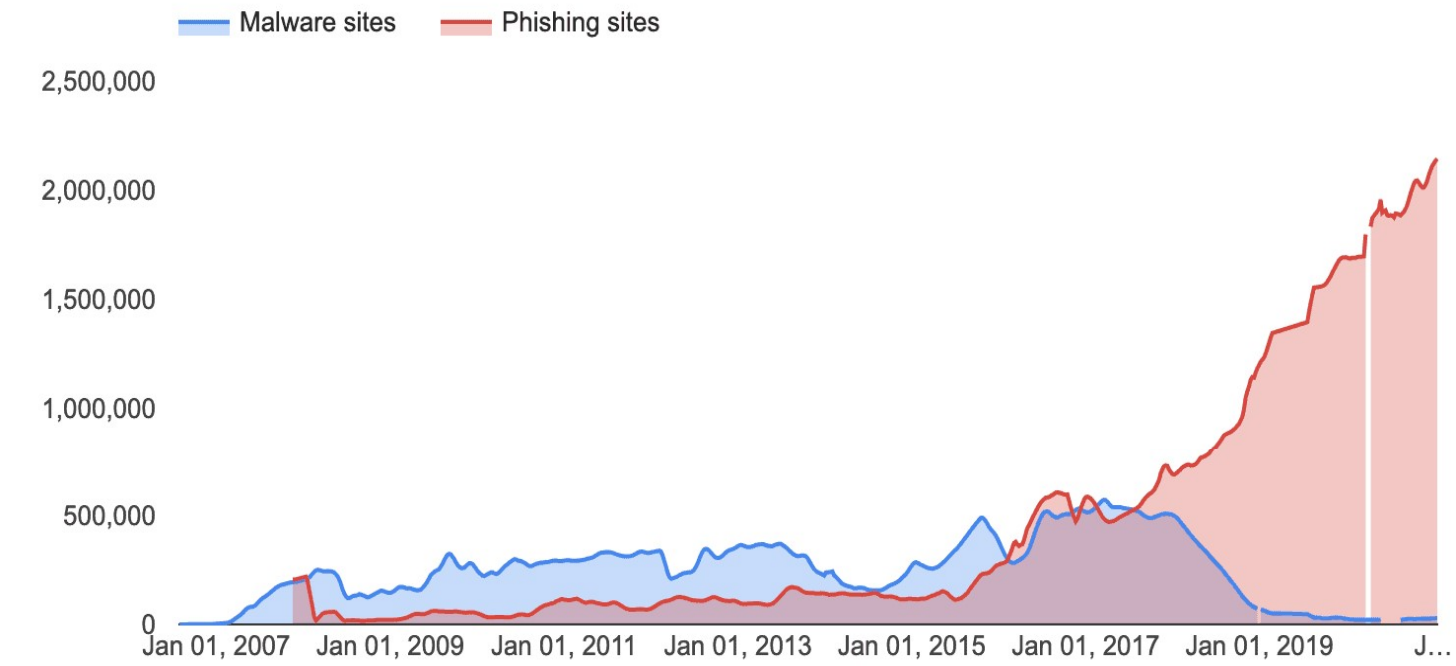
What is Phishing?

- **Section 66A of Indian IT Act** states that "*whosoever fraudulently dishonestly make use of the electronic signature, password or any other unique identification of any other person, shall be punished with imprisonment of either description for a term which may extend three years and shall also be liable to fine which may extend to rupees one lakh.*"
- **Section 66D of the Indian IT Act** states that, "*whoever, by means for any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend three years and shall also be liable to fine which may extend to rupees one lakh*"
- Phishing is the use of social engineering tactics to trick users into revealing their confidential information.

Phishing statistics worldwide

- Since 2016, phishing has replaced malware as the leading type of unsafe website.
- While there were once twice as many malware sites as phishing sites, there are now nearly 75 times as many phishing sites as there are malware sites.
- Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months).
- This compares to malware sites rising from 21,803 to 28,803 over the same period (up 32%).
- 96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone.
- When it's done over the telephone, we call it vishing and when it's done via text message, we call it smishing.

Phishing statistics worldwide



- According to the FBI, phishing was the most common type of cybercrime in 2020—and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019, to 241,324 incidents in 2020.
- The FBI said there were more than 11 times as many phishing complaints in 2020 compared to 2016.

Phishing statistics worldwide

- The frequency of attacks varies industry-by-industry
- But 75% of organizations around the world experienced some kind of phishing attack in 2020.
- The most common subject lines
- According to Symantec's 2019 Internet Security Threat Report (ISTR), the top five subject lines for business email compromise (BEC) attacks:
  - Urgent
  - Request
  - Important
  - Payment
  - Attention

https://www.tessian.com/blog/phishing-statistics-2020/

Phishing statistics worldwide

- Analysis of real-world phishing emails revealed these to be the **most common subject lines in Q4, 2020**:
- IT: Annual Asset Inventory Changes to your health benefits
- Twitter: Security alert: new or unusual Twitter login
- Amazon: Action Required | Your Amazon Prime Membership has been declined
- Zoom: Scheduled Meeting Error
- Google Pay: Payment sent
- Stimulus Cancellation Request Approved
- Microsoft 365: Action needed: update the address for your Xbox Game Pass for Console subscription
- RingCentral is coming!
- Workday: Reminder: Important Security Upgrade Required

Phishing statistics worldwide

- The most common malicious attachments
- Many phishing emails contain malicious payloads such as malware files. ESET's Threat Report reports that in Q3 2020, these were the most common type of malicious files attached to phishing emails:
- Windows executables (74%)
- Script files (11%)
- Office documents (5%)
- Compressed archives (4%)
- PDF documents (2%)
- Java files (2%)
- Batch files (2%)
- Shortcuts (>1%)
- Android executables (>1%)

Phishing statistics worldwide

- The data that's compromised in phishing attacks
- The top three "types" of data that are compromised in a phishing attack are:
  - Credentials (passwords, usernames, pin numbers)
  - Personal data (name, address, email address)
  - Medical (treatment information, insurance claims)
- When asked about the impact of successful phishing attacks, security leaders around the world cited the following consequences:
  - 60% of organizations lost data
  - 52% of organizations had credentials or accounts compromised
  - 47% of organizations were infected with ransomware
  - 29% of organizations were infected with malware
  - 18% of organizations experienced financial losses

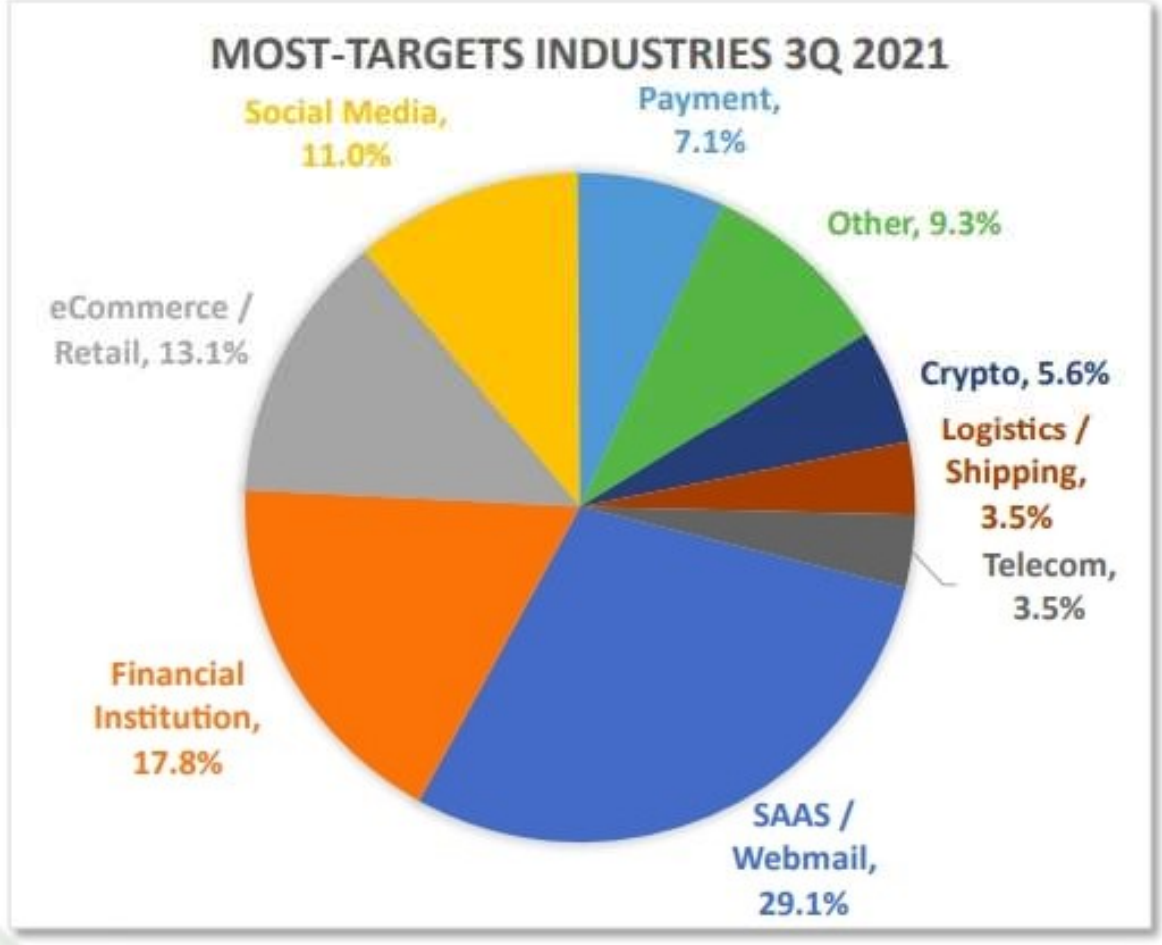
Phishing statistics worldwide

- The cost of a breach
- According to IBM's Cost of a Data Breach Report, the average cost per compromised record has steadily increased over the last three years.
- In 2019, the cost was $150. For some context, 5.2 million records were stolen in Marriott's most recent breach. That means the cost of the breach could amount to $780 million.
- But, the average breach costs organizations $3.92 million. This number will generally be higher in larger organizations and lower in smaller organizations.
- According to Verizon, organizations also see a 5% drop in stock price in the 6 months following a breach.
- Losses from business email compromise (BEC) have skyrocketed over the last year.
- The FBI's Internet Crime Report shows that in 2020, BEC scammers made over $1.8 billion—far more than via any other type of cybercrime.

Phishing statistics worldwide

- According to the **Anti-Phishing Working Group's** Phishing Activity Trends Report, the average wire-transfer loss from BEC(Business email compromise) attacks in the second quarter of 2020 was $80,183. This is up from $54,000 in the first quarter.
- This cost can be broken down into several different categories, including:
- Lost hours from employees
- Remediation
- Incident response
- Damaged reputation
- Lost intellectual property
- Direct monetary losses
- Compliance fines
- Lost revenue, Legal fees
- Costs associated remediation generally account for the largest chunk of the total.

Phishing statistics worldwide



https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

Phishing statistics worldwide

- The most targeted industries
- Costs associated remediation generally account for the largest chunk of the total. The most phished industries vary by company size.
- Nonetheless, it's clear Manufacturing and Healthcare are among the highest risk industries.
- The industries most at risk in companies with 1-249 employees are:
    1. Healthcare & Pharmaceuticals
    2. Education
    3. Manufacturing
- The industries most at risk in companies with 250-999 employees are:
    1. Construction
    2. Healthcare & Pharmaceuticals
    3. Business Services

Phishing statistics worldwide

- <u>The most targeted industries</u>
- The industries most at risk in companies with 1,000+ employees are:
  1. Technology
  2. Healthcare & Pharmaceuticals
  3. Manufacturing

Small (1-249)	Medium (250-999)	Large (1000+)
44.7% Healthcare and pharmaceuticals	49.7% Construction	55.9% Technology
41.1% Education	49.2% Healthcare and pharmaceuticals	49.3% Healthcare and pharmaceuticals
40.9% Manufacturing	43.5% Business services	46.8% Manufacturing

Phishing statistics worldwide

- <u>The most impersonated brands</u>
- New research found the brands below to be the most impersonated brands used in phishing attacks throughout Q4, 2020.
- In order of the total number of instances the brand appeared in phishing attacks:
  - Microsoft (related to 43% of all brand phishing attempts globally)
  - DHL (18%)
  - LinkedIn (6%)
  - Amazon (5%)
  - Rakuten (4%)
  - IKEA (3%)
  - Google (2%)
  - PayPal (2%)
  - Chase (2%)
  - Yahoo (1%)

2021 Tessian research found these to be the most commonly impersonated brands in phishing attacks:

- Microsoft
- ADP
- Amazon
- Adobe Sign
- Zoom

Box 5.1 Anti-Phishing Working Group (APWG)

The APWG (www.antiphishing.org which is now https://apwg.org/) is an international consortium founded in 2003 by Davis Jevans, to bring security products and services companies, law enforcement agencies, trade association, regional international treaty organizations and communications companies together, who are affected by phishing attacks.

- It has more than 3200+ members from more than 1700 organizations and agencies across the globe. E.g. Leading security companies like Symantec, McAfee, VeriSign and IronKey, and financial industry companies like ING Group, Visa, MasterCard, American Bankers Association, etc.
- APWG focuses on eliminating identity theft that results from the growing attacks of phishing and E-mail spoofing.
- It provides platform to discuss phishing issues, define the scope of the phishing problem in terms of costs and share information about best practices to eliminate these attacks/scams.

https://expertinsights.com/insights/50-phishing-stats-you-should-know/

Some definitions

- Wikipedia: it is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Webopedia: it is an act of sending an e-mail to falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for ID theft.
- The e mail directs the user to a website where they are asked to update personal information. The site however is bogus and set up only to steal the users information.
- TechEncyclopedia: it's a scam to steal valuable information such as credit card and SSN numbers, user IDs, and passwords. It is also known as "brand spoofing".
- An official looking mail is sent to the victim pretending to be from their bank or retail establishment.

Phishing

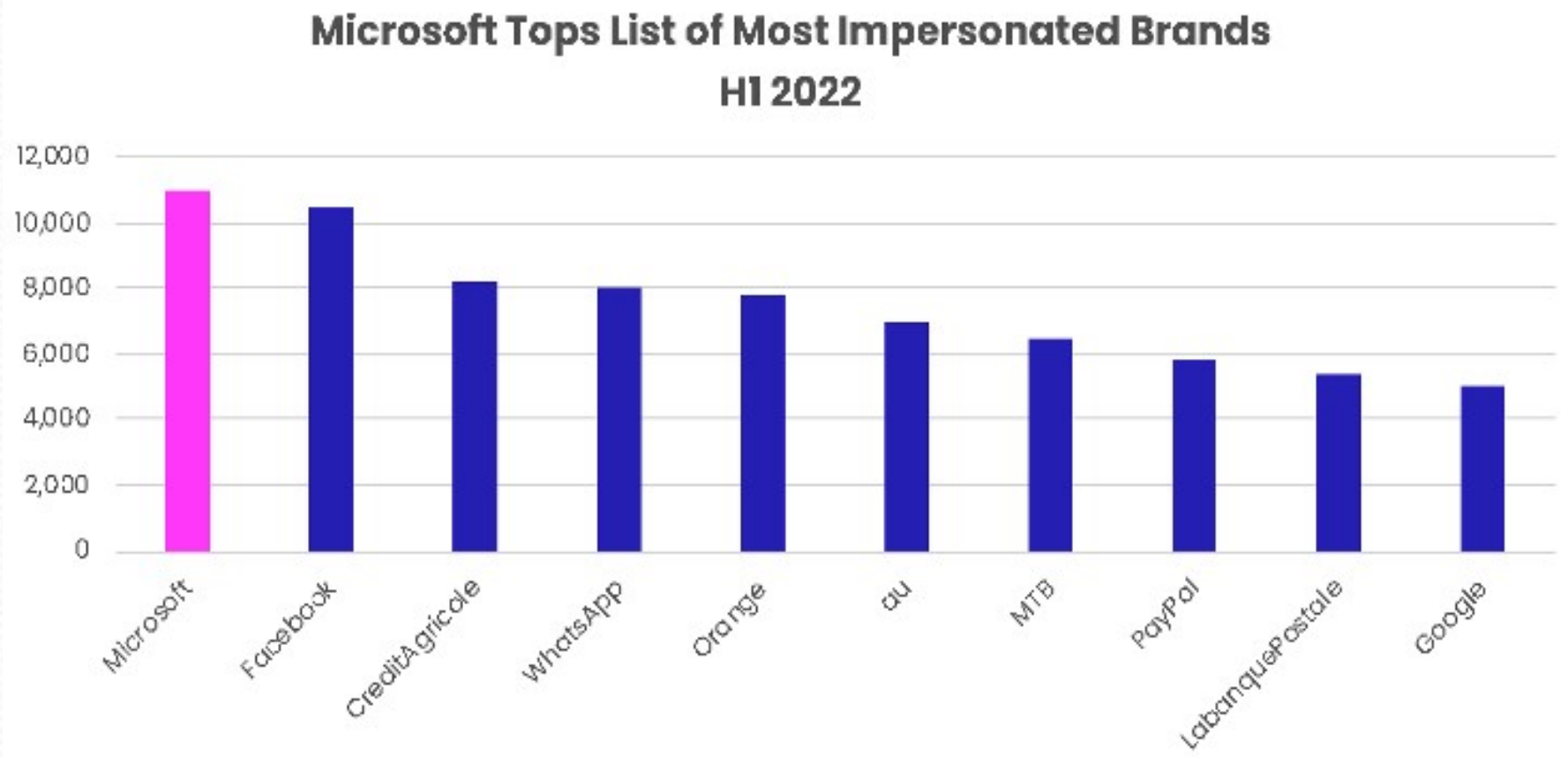
- In summary, phishing is a type of deception to steal your identity.
- It is important to understand the difference between phishing e mails and spam emails because not all phishing e mails are spam emails.
- **A. Spam Emails**
- Also known as "junk E-Mails" they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s.
- Botnets, networks of virus-infected computers, are used to send about 80% of Spam. Types of Spam E-Mails are as follows:

1. Unsolicited bulk E-Mail (UBE): It is synonym for SPAM unsolicited E-Mail sent in large quantities (see Box 5.2).
2. Unsolicited commercial E-Mail (UCE): Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Phishing

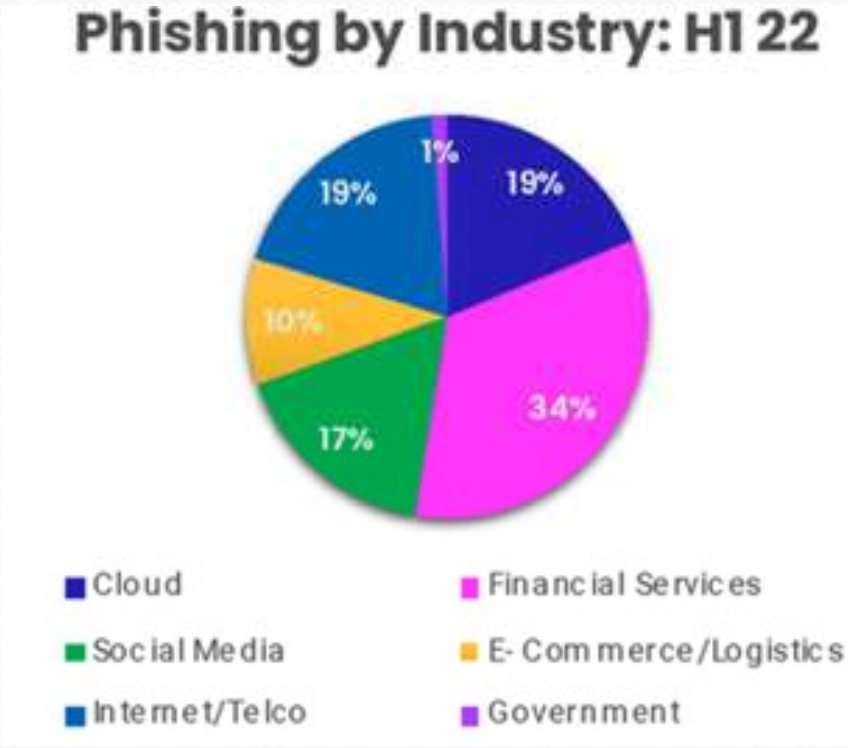
- Examples:
- 1. HSBC, Santander, CommonWealth Bank: International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fish.
- 2. eBay: It is a popular auction site, often mimicked to gain personal information.
- 3. Amazon: It was the top brand to be exploited by phishers till July 2009.
- 4. Facebook: Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail.
- One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

Phishing



https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022

Phishing



https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022

Phishing

- The E-Mail will usually ask the user to provide valuable information about himself /herself or to "verify" information that the user may have provided in the past while registering for online account.
- To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:
- 1. Names of legitimate organizations: Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.
- 2. "From" a real employee: Real name of an official, who actually works for the organization.
- This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.

Phishing

- 3. URLs that "look right": The E-Mail might contain a URL (i.e. weblink) which seems to be original website wherein user can enter the information the phisher would like to steal.
- 4. Urgent messages: Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account **or**
- E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.
- Here are a few examples of phrases used to entice the user to take the action.
- **"Verify your account"**
- **"You have won the lottery" also called "advanced fee fraud"**
- **"If you don't respond within 48 hours, your account will be closed"**

Phishing

- Let us understand the ways to reduce the amount of Spam E-Mails we receive.[11]
- 1. Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.
- 2. Never reply or open any Spam E-Mails .
- 3. Disguise the E-Mail address on public website or groups by spelling out the sign “@” and the DOT (.);
- For example, RajeevATgmailDOTcom. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.
- 4. Use alternate E-Mail addresses to register for any personal or shopping website . Never ever use business E-Mail addresses.
- 5. Do not forward any E-Mails from unknown recipients .
- 6. Make a habit to preview an E-Mail before opening it.

Phishing

- 7. Never use E-Mail address as the screen name in chat groups or rooms.
- 8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.
- **B . Hoax E-Mails (deceive or trick E-Mail)**
- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- It is difficult sometimes to recognize whether an E-Mail is a “Spam” or a hoax.”
- The websites mentioned below can be used to check the validity of such “hoax” E-Mails.

Phishing

- **B . Hoax E-Mails (deceive or trick E-Mail)**
- 1. www.breakthechain.org: This website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails.
- One can search the subject line or any phrase from the email on this website to know whether it is spam of a legitimate email.
- 2. www.hoaxbusters.org: This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy.
- It contains information almost about every scam that exist on internet.
- E.g. mail with the subject as “Breaking News” may contain the text as “Barack Obama refused to be the president of the US” and will end with the email signature as “CNN”.

Methods of Phishing

- Lets discuss most frequent methods used by the phishers to entice netizens to reveal their personal information on the internet:
- Dragnet:
- This method involves the use of spammed E-Mails, bearing falsified corporate identification (e.g., corporate names, logos and trademarks), which are addressed to a large group of people- to websites or pop-up windows with similarly falsified identification.
- E.g., customers of a particular financial institution or members of a particular auction site.
- Dragnet phishers do not identify specific prospective victims in advance.
- Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims - typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop-up windows where they are requested to enter bank or credit card account data or other personal data.

Methods of Phishing

- Rod-and-reel
- In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.
- For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the "sale" and the information is available to the phisher easily.

Methods of Phishing

- Lobsterpot
- This method focuses upon use of spoofed websites.
- It consists of creating of bogus/phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out example of a deceptive URL address linking to a scam website.
- The phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears to be a legitimate website or possibly a pop-up window that looks exactly like the official site.
- These fake sites are also called "spoofed" websites. Once the netizens is into one of these spoofed sites, he/she might unwittingly send personal information to the con artists.
- Then they often use your information to purchase goods, apply for a new credit card or otherwise steal your identity.

Methods of Phishing

- Gillnet:
- This technique relies far social engineering techniques and phishers introduce Malicious Code into E-Mails and websites.
- They can, for example, misuse browser functionality by injecting hostile content into another site's pop-up window.
- Merely by opening a particular email, or browsing a particular website, Internet users may have a Trojan horse introduced into their systems.
- In some cases, the malicious code will change settings in user's systems, so that users who want to visit legitimate banking websites will be redirected to a look alike phishing site.
- In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then transmit those data to phishers for later illegal access to users' financial accounts.

Box 5.4 Website Spoofing, XSS and XSRF

- **Website Spoofing:**
- Website spoofing attacks have become increasingly prevalent in recent years for two simple reasons: they're easy to execute and they work.
- Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.
- Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
- Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack.

Box 5.4 Website Spoofing, XSS and XSRF

- **Website Spoofing:**
- Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an advanced persistent threat or a man-in-the-middle attack.
- Even unsophisticated attackers can register a domain that's very close to the domain of a trusted brand and build a site that looks identical to the brand's website.
- Then, using phishing emails, attackers can lure the brand's customers, partners, and others to the site and trick them into revealing sensitive information like credit card numbers, Social Security numbers or login credentials.
- Website spoofing is incredibly difficult to identify.
- Because the scam takes place outside of an organization's security perimeter, website spoofing is typically only uncovered after number of users have already fallen prey to the attack.

Box 5.4 Website Spoofing, XSS and XSRF

- **XSS**
- Cross-Site scripting allows an attacker to execute arbitrary JavaScript within the browser of a victim user.
- In a cross-scripting attack (XSS), the attacker can execute malicious code in the victim's browser. This code is usually injected by the attacker when the victim browses a trusted site.
- There are three types of XSS — Stored XSS, Reflected XSS, and DOM-based XSS.
- An attacker who exploits XSS will be able to harvest credentials, redirect victims to phishing pages, and hijack a user session using cookies.
- XSS attacks are quite popular and victims include Twitter, eBay, and Yahoo.

Box 5.4 Website Spoofing, XSS and XSRF

- **XSRF**
- Also called as one-click attack or session riding and is a malicious exploit of a website.
- Cross-site request forgery, allows an attacker to induce a victim user to perform actions that they do not intend to.
- In a Cross-site request forgery (CSRF), the attacker sends a request to the browser that seems like it was made by the user.
- To do this, the victim is first tricked into clicking a link. This is followed by sending a seemingly legitimate request to the website.
- This request with cookies is the one with which victim has been associated with the website. **A CSRF attack can work only when the victim is logged in to an account.**
- CSRF vulnerabilities have been discovered in many applications including McAfee and INGDirect.
- The consequences of XSS vulnerabilities are generally more serious than for CSRF vulnerabilities

Box 5.4 Website Spoofing, XSS and XSRF

- CSRF often only applies to a subset of actions that a user is able to perform.
- Many applications implement CSRF defenses in general but overlook one or two actions that are left exposed.
  - Conversely, a successful XSS exploit can normally induce a user to perform any action that the user is able to perform, regardless of the functionality in which the vulnerability arises.
- CSRF can be described as a "one-way" vulnerability, in that while an attacker can induce the victim to issue an HTTP request, they cannot retrieve the response from that request.
  - Conversely, XSS is "two-way", in that the attacker's injected script can issue arbitrary requests, read the responses, and exhilarate data to an external domain of the attacker's choosing.

Box 5.5 Phishing vis-à-vis Spoofing

1. Objective

- The difference between Spoofing and Phishing based on the primary purpose of carrying out the scam is that in Phishing, the aim is at extracting sensitive personal data of the recipient; and in Spoofing, the goal is identity theft.

2. Nature of scam

- When you compare Phishing vs Spoofing, you need to understand that Spoofing is not a fraud because the attacker is not accessing the email or phone number of the user. No information is being stolen in this case.
- However, where Phishing is concerned, it is a type of online scam or fraud because the attacker aims at stealing the data of the user.

3. Which one is the subset of the other?

- Spoofing is a subset of Phishing because often attackers online steal the identity of a legitimate user before committing the phishing fraud. However, vice versa is not valid. Phishing cannot be part of Spoofing.

Box 5.5 Phishing vis-à-vis Spoofing

4. Method of phishing spoofing

- For Phishing, no malicious software is used and is done using social engineering techniques.
- However, in the case of Spoofing, malicious software needs to be installed on the target computer.

5. Types of spam phishing spoofing

- There are two different types of activities – Phishing types are email phishing, phone phishing, clone phishing, spear phishing, vishing, Smishing, and Angler phishing.
- Spoofing types include email spoofing, website spoofing, IP spoofing, Caller ID Spoofing, and DNS Server Spoofing.

Box 5.5 Phishing vis-à-vis Spoofing

Sr. No.	Key	Spoofing	Phishing
1	Definition	Spoofing is an identity theft where a person is trying to use the identity of a legitimate user.	Phishing is where a person steals the sensitive information of user like bank account details.
2	Category	Spoofing can be phishing in part.	Phishing is not a part of spoofing.
3	Way	For Spoofing, someone has to download a malicious software in user's computer.	Phishing is done using social engineering.
4	Purpose	Spoofing is done to get a new identity.	Phishing is done to get confidential information.
5	Examples	IP Scoofing, Email Scoofing, URL Scoofing.	Phone Phishing like asking OTP or getting bank account details, Clone phishing.

Phishing Techniques

- Common techniques used to launch the phishing attacks.
- 1. URL (weblink) manipulation: URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website. In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www. abcbank.com, URL is provided as www. abcbankl.com.
- 2. Filter evasion: This technique uses graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
  - Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is not enabled by default.
  - Firefox 2.0 and above has inbuilt "Google Phishing filter," duly licensed from Google. It is enabled by default.
  - The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+

Phishing Techniques

- Common techniques used to launch the phishing attacks.
- 3. Website forgery: In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands.
- As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily.
- Another technique used is known as "cloaked" URL - domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.
- 4. Flash Phishing: Anti-Phishing toolbars are installed/enabled to help checking the webpage content for signs of Phishing, but have limitations that they do not analyze flash objects at all.
- Phishers use it to emulate the legitimate website.
- Netizens believe that the website is "Clean" and is a real website because anti-Phishing toolbar is unable to detect it.

Phishing Techniques

- Common techniques used to launch the phishing attacks.
- 5. Social Phishing: Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.,
- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
- The victim calls the bank on the phone numbers displayed in the mail.
- The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
- Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank.
- For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity?"
- Phisher gets the required details swimmingly.

Phishing Techniques

- Common techniques used to launch the phishing attacks.
- 6. Phone Phishing: Besides such attacks, phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords.
- Conclusion:
- Phishers generally take a broad approach by sending millions of E-mails that appears to come from popular banks, online auction houses and other famous businesses.
- Unsuspecting users often responds to these requests/mails for credit card numbers, passwords, account information or other personal and financial data.

Box 5.6 Homograph attack

- **A homograph attack** is based on standards of modern Internet that allow to create (and display in web browsers) URLs with characters from various language sets (with non-ASCII letters).
- These attacks rely on the similarity of non-Roman alphabet characters to Roman characters. Different languages may contain different but very similar characters.
- Attackers can register their own domain names that are similar to the existing web addresses.
- Then they can create their own websites that are, again, the same or very similar to the existing original sites (that usually belong to banks, corporations, email or news services).
- The phony websites are used for stealing data from users who happened to visit them.
- In the simplest version of such attacks, a fake URL may consist only of simple ASCII alphanumeric characters. The intruder uses symbols that are similar to each other. Often the letter q may be confused with g, or o with o.
- Such URLs may fool some less experienced users:
  - http://bloomberg.com
  - http://www.google.co.uk
  - http://www.rnicrosoft.com

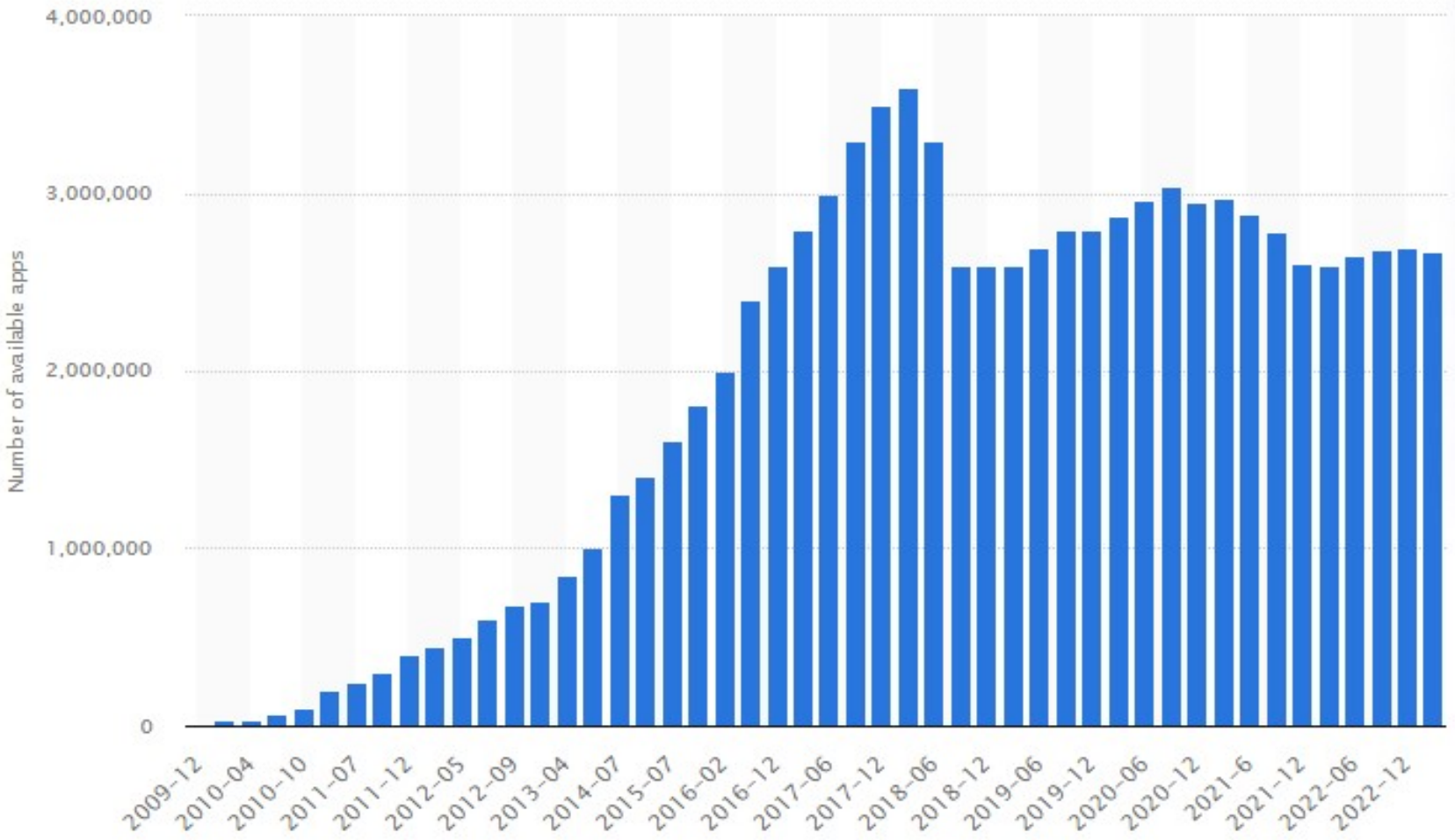
Box 5.7 Phishing attack launched through Android Market

- Android is an open source operating system for mobile phones, based on the Linux kernel. Development efforts are being coordinated by a consortium of companies known as the Open Handset Alliance, which includes big names such as Google, Intel, HTC, NVIDIA, Motorola, LG, Samsung, T-Mobile, Sprint, Sony Ericsson, Vodafone.
- The operating system has recently seen a spike in popularity with the release of Google's Nexus One phone, a clear contender for the iPhone.
- The Android Market is the equivalent of the iPhone App Store, but the application screening is apparently not as strict as on Apple's platform. There are currently over several millions of applications available on the Android Market as seen below:
-

Number of apps on Top Android App Stores, in millions

Name	Available Apps
Google Play	2.7 million
Amazon AppStore	0.48 million
GetJar	0.85 million
Aptoide	0.7 million
Opera Mobile Store	0.3 million

Number of available applications in the Google Play Store from December 2009 to March 2023



Box 5.7 Phishing attack launched through Android Market

- A malware writer succeeded in getting a rogue phishing application listed on the Android Market website.
- The software posed as a shell for mobile-banking applications, but, instead, was being used to steal online banking credentials.
- According to an alert issued by Travis Credit Union (TCU), the rogue piece of software was posted on the Android application store during the first week of December by a developer called 09Droid.
- "Your mobile device may be at risk if you downloaded an application provided by 09Droid from the Android Marketplace; applications from 09Droid are NOT an authorized or legitimate downloadable application for TCU Mobile Banking," the credit union stresses.
- The credit union chose to notify its customers via its website, Facebook page and e-mail, even though its services were not targeted by the rogue application.
- A similar warning was issued by the First Tech Credit Union, which states that the application tries to steal financial information from consumers, for the likely purpose of identity theft.

Spear Phishing

- "Spear Phishing" is 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 to all the employees or members within a certain company, government agency, organization or group.
- 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.
- Unfortunately, through the modus operandi of the Spear phishers, the E-Mail sender information has been faked or "spoofed."
- While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company's entire computer system.

Spear Phishing

- If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.
- Spear Phishing also describes scams that target people who use a certain product or website.
- Scam artists use any information they can to personalize a Phishing scam to as specific a group as possible.
- Thus, "Spear Phishing" is a targeted E-Mail attack that a scammer sends only to people within a small group, such as a company.
- The E-Mail message might appear to be genuine, but if you respond to it, you might put yourself and your employer at risk.

Spear Phishing

- Spear phishing is a targeted form of phishing. Almost all online scams start with some form of phishing, but many of these attempts randomly target a large audience.
- For example, you might get an email telling you you're about to receive some money, but you just need to provide some personal details first. This is a form of phishing, but it isn't targeted.

Bank Name: SunTrust Bank
Contact Person: Mary Alken
General Auditor
E-mail: maryaiken.frs04@accountant.com

Provide the following information below to the bank for processing and remittance of your payment.
Full name:.....
Age : .....
Occupation: .....
Address:.....
Mobile number:.....
Home Phone#: .....

https://www.tessian.com/blog/5-real-world-examples-of-phishing-attacks/

Spear Phishing

TESSIAN

TESSIAN.COM/BLOG

Must-Know Phishing Statistics

HOW MANY PHISHING ATTACKS WAS YOUR COMPANY TARGETED BY?

Attacks faced by companies in 2019.

75%

75% of organizations around the world experienced some kind of phishing attack in 2020.

Spear Phishing

TOP 5 SUBJECT LINE KEYWORDS FOR BUSINESS EMAIL COMPROMISE:

Fw: Urgent Invoice

Payment is Urgent Do Not Ignore!

Important: Please Read

RE: Finance Request for CEO of Acme

Attention: Credentials needed for login to secure mainframe

96% of phishing attacks arrive by email.

Spear Phishing

Phishing	Applies to both	Spear-phishing
High-volume: spammed to hundreds or thousands of people.	Coercive language or a sense of urgency will motivate the target to act.	Low-volume: sent to one person or a small group of people, like the finance department.
Non-personalized: generic greetings, etc.	Delivered via email.	Highly personalized: attackers will research their targets in order to craft an email that's believable.
Generally delivered via malicious links or attachments.	Hackers are after login credentials, sensitive information, or money.	Zero-payload attacks are common.
	Rely on impersonation.	

https://www.tessian.com/blog/5-real-world-examples-of-phishing-attacks/

Spear Phishing

- Whaling
- This is a specific form-of "Phishing" and/or "Spear Phishing" - targeting executives from the top management in the organizations, usually private companies.
- The objective is to swindle the executives into revealing confidential information.
- Whaling targets C-level executives sometimes with the help of information gained 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.
- The content of an E-Mail usually involves some kind of falsified industry-wide concern and is meant to be tailored for executives.

Types of Phishing

- 1. Deceptive Phishing: Phishing scams started by broadcasting deceptive E-Mail messages with the objective of ID theft.
- 2. Malware-based Phishing: It refers to scams that involve running Malicious Code on the netizens system.
- Malware can be launched as an E-Mail attachment or as a downloadable file from a website or by exploiting known security vulnerabilities.
- 3. Keyloggers: Malware can embed a keylogger to track keyboard input and send relevant information, maybe the keylogger log, to the phisher through the Internet.
- 4. Session hijacking: It is an attack in which user's activities are monitored until they establish their bonafide credentials by signing into their account or begin the transaction.

Types of Phishing

- 5. In session Phishing: It is a Phishing attack based upon one web browsing session being able to detect the presence of another session, (such as visit to an online banking website) on the same web browser and then a pop-up window is launched that pretends to be opened from the targeted session.
- 6. Web Trojans: It pops up to collect netizen's credentials and transmit them to the phisher while netizens are attempting to log in. Such pop-ups are usually invisible.
- 7. System reconfiguration attacks: Phisher can intrude into the netizens system (i.e., computer) to modify the settings for malicious purposes.
- 8. Content-injection Phishing: In this type of scam, phisher replaces part of the content of a legitimate website with false content to mislead the netizen to reveal the confidential personal information.

Types of Phishing

- 9. Search engine Phishing: It occurs when phishers create websites with attractive sounding offers (often found too good to be true) and have them indexed legitimately with search engines.
- Netizens find websites during their normal course of search for products or services and are trapped to reveal their personal information.
- 10. SSL certificate Phishing: It is an advanced type of scam. Phishers target web servers with SSL certificates to create a duplicitous website with fraudulent WebPages displaying familiar "lock" icon.

Box 5.8 Avoid Spear Phishing Scams

- There are some precautions you can take to avoid making yourself a victim of Phishing scam.
- Never reveal personal or financial information in a response to an email request, no matter whoever the sender is.
- If you receive suspicious email message, call the person/organization listed in the from line before responding or opening any attachments.
- Never click a link in an email that requests for financial information. Enter that web address in the browser window itself.
- Report any email that you suspect might be a spear phishing campaign.
- Use the phishing filter. It scans identity suspicious websites, and provides up-to-the-hour updates and reports about known phishing sites.

Box 5.10 Three Ps of Cybercrime – Phishing, Pharming and Phoraging

- Pharming: It is an attack aiming to redirect a website's traffic to another bogus website.
- Here an attacker cracks the vulnerability in an ISP's DNS server and hijacks the domain name of a commercial site. So anyone going to the legitimate site is then redirected to an identical but bogus site.
- Antivirus and Spyware software cannot protect against pharming attacks. The best practice is to use secure connections like HTTPS and accept valid public-key certifications issued by trusted sources only.
- Phoraging: it is a process of collecting data from many different online sources to build up the identity of someone with the ultimate aim of committing Identity Theft.

Phishing Toolkits and Spy Phishing

- A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics (i.e., images and logos) displayed on these websites.
- Phishing toolkits are developed by groups or individuals and are sold in the underground economy.
- These sophisticated kits are typically difficult to obtain, are quite expensive, and are more likely to be purchased and used by well-organized groups of phishers, rather than average users.
- Phishers use hypertext preprocessor (PHP) to develop the Phishing kits.
- PHP is a general purpose scripting language that was originally designed for web development of dynamic WebPages.
- PHP code is embedded into the HTML source script and interpreted by a web server with the help of a PHP processor module.

Phishing Toolkits and Spy Phishing

- Most of the Phishing kits are advertised and distributed at no charge and usually these Phishing kits- also called DIY (Do It Yourself) Phishing kits- may hide backdoors through which the phished information is sent to recipients (may be to the authors of Phishing kits) other than the intended users.
- Following are few examples of such toolkits:
- 1. Rock Phish: It is a Phishing toolkit popular in the hacking community since 2005. It allows non-techies to launch Phishing attacks.
- The kit allows a single website with multiple DNS names to host a variety of phished WebPages, covering numerous organizations and institutes.
- 2. Xrenoder Trojan Spyware: It resets the homepage and/or the search settings to point to other websites usually for commercial purposes or porn traffic.
- 3. Cpanel Google: It is a Trojan Spyware that modifies the DNS entry in the host's file to point to its own website.
- If Google gets redirected to its website, a netizens may end up having a version of a website prepared by the phisher.

Phishing Countermeasures

- 1. Keep antivirus up to date: Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits.
- This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS).
- 2. Do not click on hyperlinks in E-Mails: It should always be practiced that, in case an E-Mail has been received from unknown source, clicking on any hyperlinks displayed in an E-Mail should be avoided.
- This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system.
- Instead, to check out the link, manually retyping it into a web browser is highly recommended.
- 3. Take advantage of anti-Spam software: Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-Spam software, many types of Phishing attacks are reduced because the messages will never end up in the mailboxes of end-users,

Phishing Countermeasures

- 4. Verify https (SSL): Ensure the address bar displays "https://" rather than just "http://" along with a secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information.
- One may like to check by double-clicking the lock to guarantee the third-party SSL certificate that provides the https service.
- Always ensure that the webpage is truly encrypted.
- 5. Use anti-Spyware software: Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot.
- If for some reason your browser is hijacked, anti-Spyware software can often detect the problem and provide a fix.
- 6. Get educated: Always update the knowledge to know new tools and techniques used by phishers to entice the netizens and to understand how to prevent these types of attacks.
- Report any suspicious activity observed to nearest cyber- security cell.

Phishing Countermeasures

- 7. Firewall: Firewall can prevent Malicious Code from entering into the system and hijacking the browser.
- Hence, a desktop (software) such as Microsoft's built-in software firewall in Windows-XP and/or network (hardware) firewall should be used.
- It should be up to date in case any cyber security patches have been released by the vendor.
- 8. Use backup system images: Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play.,
- 9. Secure the hosts file: The attacker can compromise the hosts file on desktop system and send a netizens to a fraudulent site.
- Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe.

Box 5.13 How to Recognize legitimate websites?

1. Using General Tips

- Type the website's name into a search engine and review the results. If the site in question is a hazard (or simply an overwhelmingly illegitimate site), a cursory Google check will be enough to inform you accordingly.
- Look at the website's connection type. Also check the website's URL .
- Watch out for invasive advertising.
- Most sites provide a Contact page so that users can send questions, comments, and concerns to the owner of the site.
- If you can, call or email the provided number or email address to verify the legitimacy of the website
- Use a "WhoIs" search to research who has registered the website's domain. All domains are required to display contact information for the person or company who has registered the domain.
- You can get WhoIs info from most domain registrars, or from services such as https://whois.domaintools.com/. Some things to look out for.

Box 5.13 How to Recognize legitimate websites?

- Open the Google Transparency Report webpage. You can quickly run a website's address through this service to see its safety rating from Google. https://transparencyreport.google.com/?hl=en
- Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites.
- Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised.
- When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.
- Use different websites providing free checking of similar types:
- Check if a website is a scam website or a legit website. Scamadviser helps identify if a web shop is fraudulent or infected with malware, or conducts phishing. https://www.scamadviser.com/

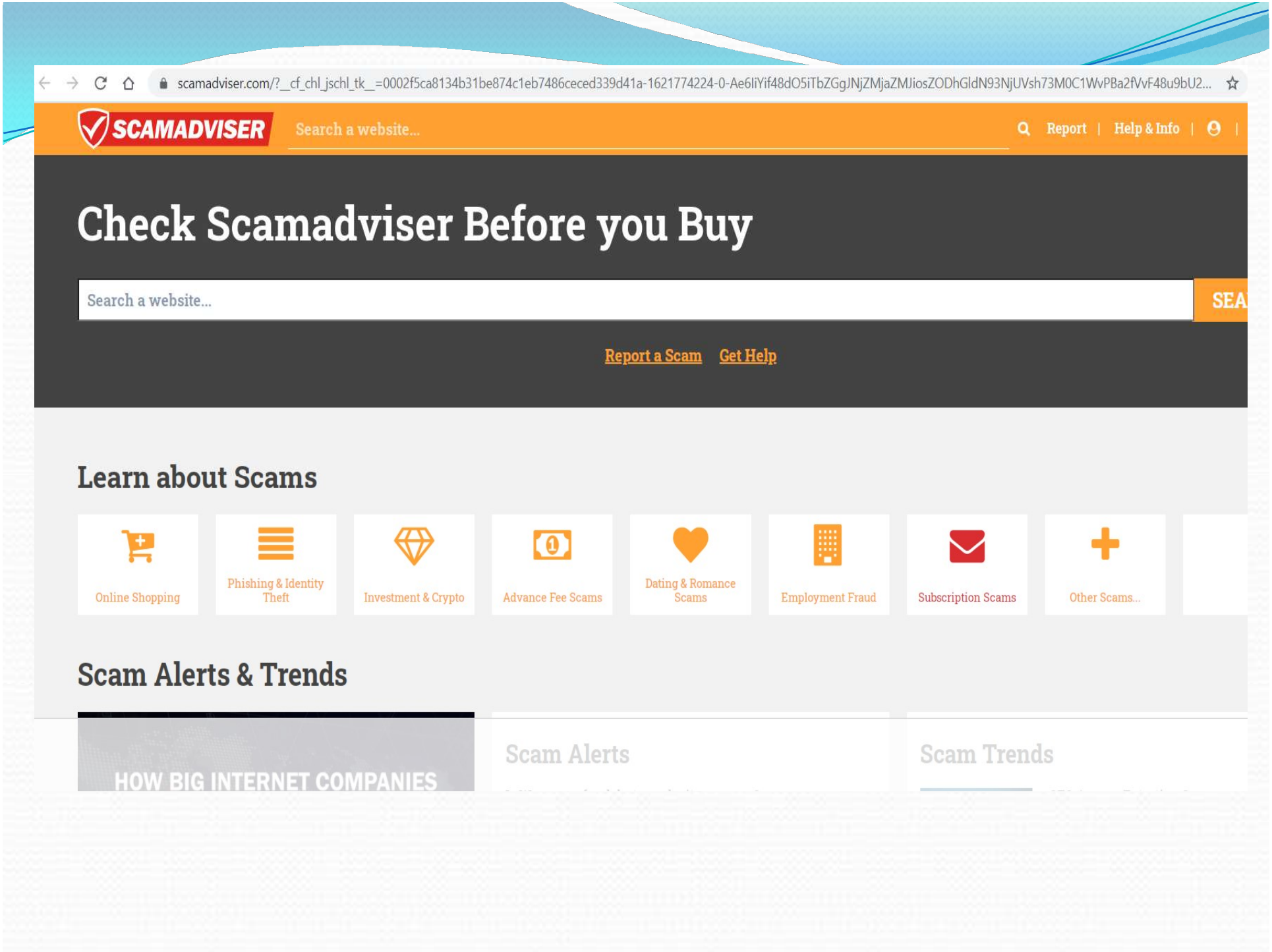

scamadviser.com/?__cf_chl_jschl_tk__=0002f5ca8134b31be874c1eb7486ceced339d41a-1621774224-0-Ae6liYif48dO5iTbZGgJNjZMjaZMJiosZODhGldN93NjUVsh73M0C1WvPBa2fVvF48u9bU2...
SCAMADVISER
Search a website...
Report | Help & Info |
Check Scamadviser Before you Buy
Search a website...
SEA
Report a Scam
Get Help
Learn about Scams
Online Shopping
Phishing & Identity Theft
Investment & Crypto
Advance Fee Scams
Dating & Romance Scams
Employment Fraud
Subscription Scams
Other Scams...
Scam Alerts & Trends
HOW BIG INTERNET COMPANIES
Scam Alerts
Scam Trends

Table 5.2 Anti-Phishing plug-ins

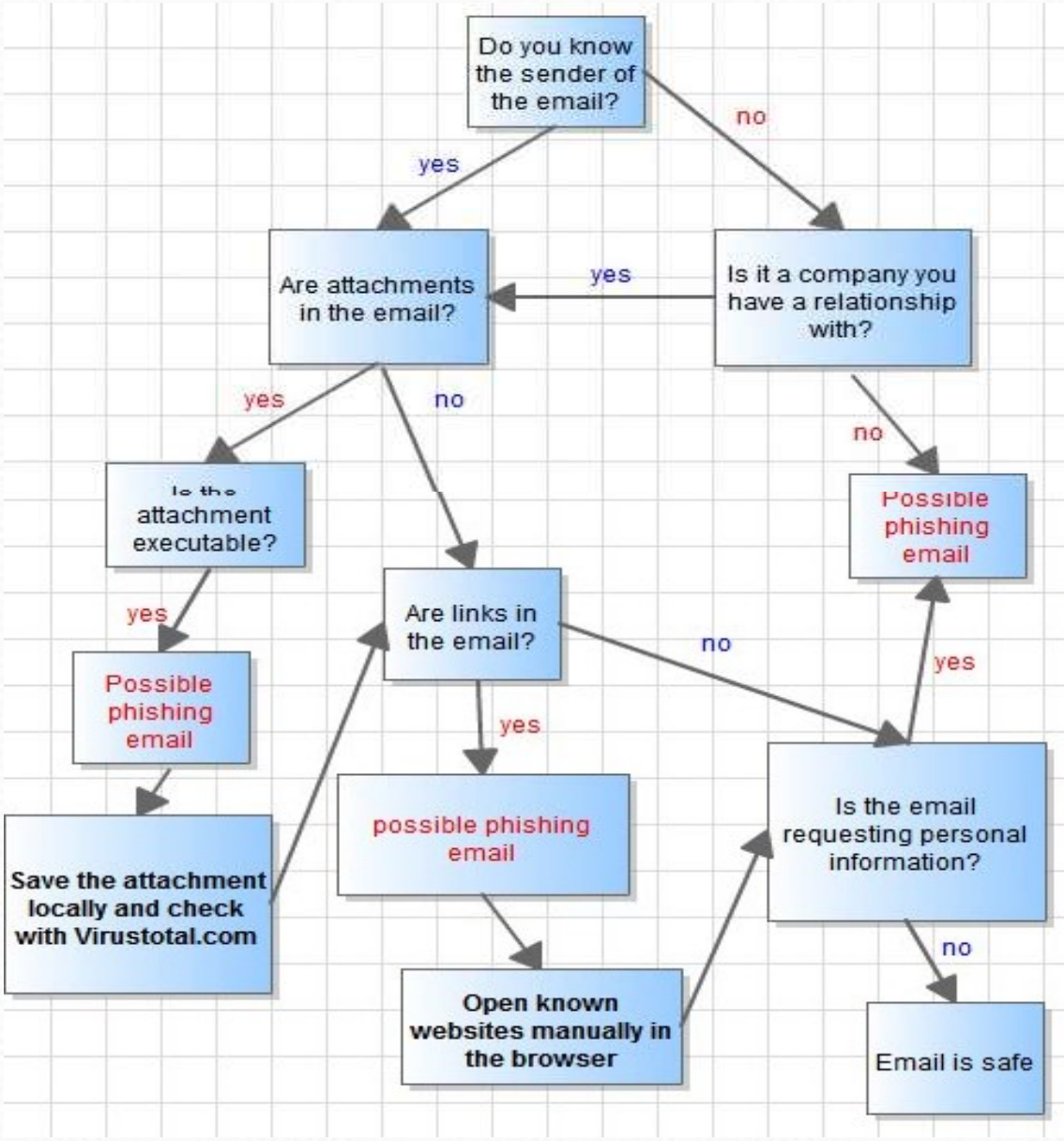
- Windows Defender Browser Protection
- (https://browserprotection.microsoft.com/learn.html)
- Avira Browser Safety (https://www.avira.com/en/avira-browser-safety)
- BitDefender TrafficLight
- (https://www.bitdefender.com/solutions/trafficlight.html)
- Avast Online Security (https://www.avast.com/avast-online-security)
- McAfee SECURE Safe Browsing (https://www.mcafeesecure.com/safe-browsing)
- Panda Sage Web (https://www.pandasecurity.com/en-us/homeusers/solutions/vpn/)
- PhishingFree (https://phishingfree.com/index.html)
- Dr.Web Link Checker (https://free.drweb.com/linkchecker/?lng=en)

Phishing Countermeasures

- SPS Algorithm to Thwart Phishing Attack
- Sanitizing Proxy Systems
- The key idea of SPS is that Web phishing attack can be immunized by removing part of the content that traps novice users into entering their personal information.
- Also, since SPS sanitizes all HTTP responses from suspicious URLs with warning messages, novice users will realize that they are browsing phishing sites.
- The SPS filtering algorithm is very simple and can be described in roughly 20 steps, and can also be built in any proxy system, such as a server solution, a personal firewall or a browser plug-in.
- By using SPS with a transparent proxy server, novice users will be protected from almost all Web phishing attacks even if novice users misbehave

Phishing Countermeasures

- SPS Algorithm to Thwart Phishing Attack



Phishing Countermeasures

- SPS Algorithm to Thwart Phishing Attack
- A phishing attack is composed of two phases: attraction and acquisition.
- Attraction: Email spoofing attracts users using a 'spoofed' email, as if it were sent by a legitimate corporation.
- To acquire the users' personal information, the spoofed email leads users to execute the attached crime-ware, such as a keylogger or a redirector, or to access a 'spoofed' Web site, the so-called "phishing site".
- Acquisition: The acquisition method using a phishing site is defined as Web spoofing which can be categorized by techniques of stealing personal information downloading crime-ware, cross site scripting (XSS), and deceit.
- Downloading and XSS cases employ technical subterfuges. On the other hand, in the deceit case only social engineering, that is, the misbehaviour of users is employed.

Identity Theft

- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Theft Resource Center (ITRC), with the objective to extend the support to the society to spread awareness about this fraud.
- Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below :
- 1. Credit card fraud (26%):
- 2. Bank fraud (17%): Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft.
- 3. Employment fraud (12%): In this fraud, the attacker borrows the victim's valid SSN to obtain a job.

Identity Theft

- 4. Government fraud (9%): This type of fraud includes SSN, driver license and income tax fraud.
- 5. Loan fraud (5%): It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.
- It is important to note the various usage of ID theft information.
- 1. 66% of victims' personal information is used to open a new credit account in their name.
- 2. 28% of victims' personal information is used to purchase cell phone service.
- 3. 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief

Box 5.14 Identity Theft Resource Centre (ITRC)

- The ITRC Is A Non-Profit Organization Established To Empower And Guide Consumers, Victims, Business And Government To Minimize Risk And Mitigate The Impact Of Identity Compromise And Crime.
- The ITRC was established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cyber security, scams/fraud and privacy issues.
- The ITRC conducts training and presentations on best practices and risk reduction for both businesses and consumers as it fundamentally believes that both consumers and businesses are victims of identity theft and fraud.
- For more information visit https://www.idtheftcenter.org/

Table 5.3 Identity Theft Myths and Facts

- 1: there is no way to protect yourself from ID theft
- 2: Identity theft is just a financial crime.
- 3: Its my bank's fault I become victim of ID theft
- 4: its safe to give my personal information if my caller ID confirms that its my bank.
- 5: checking your credit report periodically and using credit card monitoring service is all you need to protect yourself from ID theft.
- 6: My personal information (address, telephone number, email, etc.) is not valuable to a thief.
- 7: shredding my Email and other personal documents will keep me safe.
- Myth 8: I don't use internet, so I am safe.
- Myth 9: Social networking is safe.
- Myth 10: it is not safe to shop or bank online.

Personally Identifiable Information (PII)

- The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:
- 1. Full name;
- 2. national identification number (e.g., SSN);
- 3. telephone number and mobile phone number;
- 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/birth day;
- 8. birthplace;
- 9. face and fingerprints.

Personally Identifiable Information (PII)

- The fraudster may search for following about an individual, which is less often used to distinguish individual identity; however these can be categorized as potentially PII because they can be combined with other personal information to identify an individual.
  - First or last name;
  - Age;
  - Country, state or city of residence;
  - Gender;
  - Name of the school/college/workplace;
  - Job position, grades and/or salary;
  - Criminal record.
- The information can be further classified as (a) non-classified and (b) classified.

Personally Identifiable Information (PII)

- **1 . Non-classified information**
- Public information: Information that is a matter of public record or knowledge.
- Personal information: Information belongs to an individual but he/she may share this information with others for personal or business reasons (e.g., addresses, telephone numbers and E-Mail addresses).
- Routine business information: Business information that do not require any special protection and may be routinely shared with anyone inside or outside of the business.
- Private information: Information that can be private if associated with an individual and individual can object in case of disclosure (e.g. SSN, credit card numbers and other financial information).
- Confidential business information: Information which, if disclosed, may harm the business e.g., sales and marketing plans, new product plans and notes associated with patentable inventions).

Personally Identifiable Information (PII)

- **2 . Classified information**
- Confidential: Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
- Secret: Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
- Top secret: Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems)
- ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

Types of Identity Theft

- 1. Financial identity theft: Financial ID theft includes bank fraud, credit card fraud, tax refund fraud, mail fraud and several more.
- The process of recovering from the crime is often expensive, time-consuming and psychologically painful.
- This type of fraud often destroys a victim's credit and it may take weeks, months or even years to repair.
- 2. Criminal identity theft: It involves taking, over someone else's identity to commit a crime such as enter into a country, get special permits, hide one's own identity or commit acts of terrorism.
- These criminal activities can include Computer and cybercrimes, Organized crime, Drug trafficking, Alien smuggling, Money laundering.
- The victims of this crime are left with the burden to clear their own name in the eyes of the criminal justice system.
- It is very crucial and important to contact local police department immediately in case of becoming a victim of criminal ID theft.
- This should be the first step in building a case and clearing your name.

Types of Identity Theft

- 3. Identity cloning: Identity cloning may be the scariest variation of all ID theft.
- Identity clones compromise the victim's life by actually living and working as the victim.
- In short cloning is the act of a fraudster living a natural and usual life similar, to a victims life, may be at a different location.
- 4. Business identity theft: "Bust-out" is one of the schemes fraudsters use to steal business identity. A fraudster rents a space in the same building as victim's office.
- Then he applies for corporate credit cards using victim's firm name.
- The application passes a credit check because the company name and address match, but the cards are delivered to the fraudster's mailbox.
- He sells them on the street and vanishes before the victim discovers the firm's credit is wrecked.
- The consequences of business ID theft may call for a disaster to the business, such as call out from market and damage to the reputation, and hence it is extremely important to employ countermeasures for such type attacks.

Types of Identity Theft

- 5. Medical identity theft: India is known to have become famous for "medical tourism."
- Thousands of tourists, every year visit India with dual purpose - touring the country plus getting their medical problems attended to because India has made name for good quality and yet reasonable priced in medical services.
- In the process thousands of medical records of foreigners as well as locals who avail medical facility get created thousands of electronic records area available online. This has created a boom for cybercriminals.
- 6. Synthetic identity theft: This is an advanced form of ID theft in the ID theft world. The fraudster will take parts of personal information from many victims and combine them.
- The new identity is not any specific person, but all the victims can be affected when it is used.
- 7. Child identity theft: Parents might sometimes steal their children's identity to open credit card accounts, utility accounts, bank accounts and even to take out loans or secure because their own credit history is insufficient or too damaged to open such accounts.

Box 5.15 Chinese Ghost Net

- GhostNet is the name given to a large-scale cyber espionage operation discovered in March 2009.
- The operation's command and control infrastructure was based mainly in the People's Republic of China and had infiltrated high-value political, economic and media locations in 103 countries.
- At least 1,295 computer systems were compromised, including systems belonging to embassies, foreign ministries, government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City.
- The Trojan was primarily delivered through carefully social engineered e-mails and upon installation it connected back to a control server to receive commands. The infected computer would then execute commands specified by the control server.
- Although the activity was mostly based in China, the Chinese government denied all involvement in this operation and conclusive links between the Chinese government and GhostNet were not discovered.

Table 5.4 Business Identity Theft - Countermeasures

- Secure your business premises with locks and alarms
- Put your business records under lock and key
- Shred, shred and shred carefully
- Be cautious on the phone
- Limit access to your IT systems
- Protect the IT systems from hackers
- Create awareness that internet is a dangerous place
- Avoid broadcasting information
- Create and enforce an organization-wide information security policy
- Disconnect the access of Ex-employees immediately

Techniques of ID Theft

- **1. Human-based methods:** These methods are techniques used by an attacker without and/or minimal use of technology.
- Direct access to information: People who have earned a certain degree of trust (house cleaners, babysitters, nurses, friends or roommates) can obtain legitimate access to a business or to a residence to steal the required personal information.
- Dumpster diving
- Theft of a purse or wallet: Wallet often contains bank credit cards, debit cards, driving license, medical insurance identity card and what not. Pickpockets work on the street as well as in public, transport and exercise rooms to steal the wallets and in turn sell the personal information.
- Mail theft and rerouting: It is easy to steal the postal mails from mailboxes, which has poor security mechanism and all the documents available to the fraudster are free of charge.

Techniques of ID Theft

- **1. Human-based methods:**
- Shoulder surfing: People who loiter around in the public facilities such as in the cybercafes, near ATMs and telephone booths can keep an eye to grab the personal details.
- Dishonest or mistreated employees: Just as it is possible to imitate a bank ATM, it is also possible to install miniaturized equipment on a valid ATM.
- This equipment (a copier) captures the card information, using which, duplicate card can be made and personal identification number (PIN) can be obtained by stealing the camera films.
- Telemarketing and fake telephone calls: An employee or partner with access to the personal files, salary information, insurance files or bank information can gather all sorts of confidential information and can use it to provide sufficient damage.

Techniques of ID Theft

- **2. Computer-based technique:** These techniques are attempts made by the attacker to exploit the vulnerabilities within existing processes and/or systems.
- Backup theft: This is the most common method. In addition to stealing equipment from private buildings, attackers also strike public facilities such as transport areas, hotels and recreation centers. They carefully analyze stolen equipment or backups to recover the data.
- Hacking, unauthorized access to systems and database theft: Besides stealing the equipment and/or hardware, criminals attempt to compromise information systems with various tools, techniques and methods, to gain unauthorized access, to download the required information.

Techniques of ID Theft

- **2. Computer-based technique:**
- Phishing:
- Pharming:
- Redirection: These are malicious programs that redirect users' network traffic to locations they did not intend to visit.
- Hardware: Using Keylogger types of devices.

ID Theft Countermeasures

- 1. Monitor your credit closely: The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you.
- Watch for suspicious signs such as accounts you did not open.
- You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security.
- 2. Keep records of your financial data and transactions: Review your statements regularly for any activity or charges you did not make.
- 3. Install security software: Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions.
- 4. Use an updated Web browser: Use an updated web browser to make sure you're taking advantage of its current safety features.

ID Theft Countermeasures

- 5. Store sensitive data securely: Just as you keep sensitive paper documents under lock and key, secure sensitive online information.
- This can be done through file encryption software.
- 6. Be wary of E-Mail attachments and links in both E-Mail and instant messages: Use caution even when the message appears to come from a safe sender, as identity information in messages can easily be spoofed.
- 7. Stay alert to the latest scams: Awareness and caution are effective methods to counter fraud.
- Create awareness among your friends and family members by sharing security tips you learn with them.

How to protect your online Identity?

- Use Strong Passwords
- Look for Encryption
- Install Security Suites
- Turn on Web Browser Blacklisting
- Avoid Phishing Scams
- Get Private Data Protection
- Password-Protect Your Wireless Router
- Hide Your Personal Information
- Enable Cookies on Your Web Browser Only When Required
- Protect Your Credit Card Information