VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

PMCA605L : Cyber Security

Module 4: Phishing and Identity Theft

Courtesy: Nina Godbole, Sunit Belapure & *Other Sources of Internet*

Dr. R. K. Nadesh

Phishing

- **Phishing** is a type of **cyberattack** where attackers trick individuals into revealing sensitive information.

- Such as **usernames, passwords, credit card details, or financial data**, by disguising themselves as legitimate entities.

- It is one of the most common **social engineering attacks** used by hackers.

Phishing Methods

- Dragnet (Spammed Emails)
- Rod-and-Reel (Targeted Phishing)
- Lobsterpot (Spoofed Websites)
- Gillnet (Malicious Code and Malware)

Dragnet (Spammed Emails)

- **Wide-scale phishing** method, similar to casting a net to catch as many victims as possible.
- Attackers **send mass spam emails** to thousands or millions of recipients.
- Emails appear to be from legitimate sources (e.g., banks, popular websites).
- Aimed at **tricking users into clicking on malicious links** or entering sensitive information.

Example: An email claiming you’ve won a lottery, asking for personal details to claim the prize.

Rod-and-Reel (Targeted Phishing)

- More targeted approach compared to Dragnet.
- Attackers identify specific victims (e.g., high-value targets or certain demographics).
- They craft personalized messages containing false information to manipulate victims into revealing data.
- Often involves social engineering to make the message more convincing.

Example: An email pretending to be from a company’s HR department requesting login details for a benefits portal.

Lobsterpot (Spoofed Websites)

- Focuses on **spoofed (fake) websites** that mimic legitimate ones.
- Victims are tricked into **visiting fake sites** and entering personal information (e.g., usernames, passwords, or credit card details).
- Links to these sites are often shared through phishing emails or ads.

Example: A fake banking website that looks identical to the real one but is designed to steal login credentials.

Gillnet (Malicious Code and Malware)

- **Less reliant on social engineering**; uses **malicious code or malware** instead.
- Attackers **embed malware** in emails, links, or websites to infect users' devices.
- Once installed, the malware can **steal sensitive information, record keystrokes**, or provide remote access to the attacker.

Example: An email attachment disguised as an invoice that installs spyware when opened.

Phishing Techniques

1.URL (weblink) manipulation

2.Filter Evasion

3.Website forgery

4.Flash Phishing

5.Social Phishing

6.Phone Phishing

URL (weblink) manipulation

- **URL manipulation** is a phishing technique where attackers create deceptive or misleading URLs that look legitimate but lead to malicious websites.
- The goal is to **trick users into clicking the link** and entering sensitive information like usernames, passwords, or credit card details.
- Example: Using domains like "secure-paypal.com" instead of the real "paypal.com".

Filter Evasion

- Filter evasion is a phishing technique used to **bypass email security filters** and **avoid detection by spam filters or antivirus software.**
- Attackers use various methods to disguise their phishing content, making it harder for automated systems to identify and block malicious emails or websites.
- Example : Using **image-based text** or **misspellings** (e.g., "PayPal" using Cyrillic letters) to avoid detection.

Phishing Filter

- Google uses advanced phishing filters to **protect users from phishing emails, malicious websites, and fraudulent activities**.

- These filters are integrated into Google services like **Gmail, Google Chrome, and Google Search** to detect and block phishing attempts.

- Microsoft uses advanced phishing filters to **protect users from phishing attacks, malicious websites, and fraudulent emails**. These filters are integrated into Microsoft services like **Outlook, Microsoft Edge, and Microsoft Defender** to detect and block phishing attempts in real-time.

Website Forgery

✓ Fake websites are created that **look identical** to real ones.

✓ When victims enter their login credentials, attackers steal them.

Example: A fake Google login page that captures your username and password.

Flash Phishing

- Using flash animations or interactive content to trick users into revealing personal information.

- Often used in fake surveys or online games.

Social Phishing

- Social Phishing is a technique where attackers use social engineering tactics to manipulate victims into revealing sensitive information by exploiting human trust and social interactions.

- These attacks often occur on social media platforms, messaging apps, or through impersonation of trusted contacts or organizations.

- Example : Fake Customer Support Accounts, Social Media Scams- “Win a free smartphone! Click here to participate!”

Phone Phishing

- Smishing (SMS Phishing)
- Vishing (Voice Phishing)

Spear Phishing

- ✓ A targeted attack aimed at specific individuals or organizations.
- ✓ Attackers customize messages based on personal details (name, job title, company) to make them more convincing.
- ✓ Often used in corporate espionage or fraud attacks.

Example: A fake email from a company’s CEO instructing an employee to transfer funds.

Whaling

- ✓ A specialized form of spear phishing targeting high-profile individuals like CEOs, executives, and senior employees.
- ✓ Attackers use fake emails or messages to impersonate executives and request sensitive data or wire transfers.

- Example: A CFO receiving an email (spoofed) from the CEO asking for an urgent wire transfer.

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

Deceptive Phishing

- **Deceptive Phishing** is the most common type of phishing attack where attackers **pretend to be a legitimate entity** to trick victims into **revealing sensitive information** such as usernames, passwords, credit card numbers, or personal details.

- These attacks usually occur through **emails, SMS, or fake websites** designed to look trustworthy.

Email (**Deceptive Phishing**)

- ✓ Attackers send fake emails that appear to be from trusted sources (banks, government agencies, or social media platforms).
- ✓ These emails contain malicious links or attachments that steal credentials.

Example: An email pretending to be from PayPal asking you to update your account information.

Malware-Based Phishing

- Emails or messages contain malicious attachments or links that download malware onto the victim's device.

- The malware may steal information, log keystrokes, or provide remote access to the attacker.

- Example: An email with a subject line, "Invoice Due - URGENT" containing a .docx or .pdf file with embedded malware.

Session Hijacking

- Session Hijacking is a cyberattack where an attacker takes over a user's active session on a website or application by stealing or manipulating session tokens.

- This allows the attacker to impersonate the user and gain unauthorized access to their account or sensitive information.

- **Example Scenario:**

✓ You connect to a public Wi-Fi at a café and log into your **email account**.

✓ An attacker on the same network uses a **packet sniffer** to capture your session cookie.

✓ Using the stolen session cookie, the attacker **impersonates you** and gains full access to your email account without needing your password.

In-Session Phishing

- **In-Session Phishing** - where attackers display **fake pop-up messages or overlays** on legitimate websites **while the user is actively logged in**.

- These deceptive prompts trick users into entering sensitive information, such as **login credentials, credit card numbers, or personal details**.

- **Example :** You are logged into your PayPal account to check recent transactions. While browsing through your payment history, a pop-up suddenly appears that looks exactly like a PayPal security alert:

"Your session has expired for security reasons. Please re-enter your password to continue."

Web Trojans

- **Web Trojans** are malicious programs or scripts that are **embedded into websites** or delivered through web applications.

- Their primary goal is to **steal sensitive information**, **hijack user sessions**, or **install additional malware** on the victim's device.

- Unlike traditional Trojans, web Trojans operate through **web browsers** and often require minimal user interaction.

Web Trojans(Example)

- You visit a **popular news website** that has been **compromised by attackers**.
- An invisible iframe is embedded on the site, loading a malicious script from a remote server.
- The script executes a **Man-in-the-Browser (MitB)** attack that:

✓ Steals your online banking credentials by injecting a fake login form.

✓ Records your keystrokes as you enter your username and password.

✓ Redirects you to the legitimate banking website after stealing your data, so you suspect nothing.

Pharming

- **Pharming** is a cyberattack where users are **redirected from legitimate websites to fraudulent sites** without their knowledge, even if they type the correct URL.

- **Pharming manipulates the underlying network infrastructure** or **DNS settings**. (DNS based pharming)

- **Host File Poisoning** - where attackers **modify the host file** on a victim's computer to **redirect them to malicious websites**, even if they type the correct URL

Host File Poisoning

Host File Overview:

- The host file is located on a user’s computer (e.g., in C:\Windows\System32\drivers\etc\hosts on Windows).
- It acts as a local DNS resolver, mapping domain names to IP addresses before querying external DNS servers.
- Example entry: 127.0.0.1 localhost or 192.168.1.10 myprinter.local.

Tabnapping (Tabjacking)

- Tabnapping, also known as Tabjacking, is a type of phishing attack where a malicious website silently changes the content of an inactive browser tab to look like a legitimate login page.

- The attacker aims to trick users into re-entering their credentials, such as email, social media, or banking passwords, thinking their session has expired.

Tab Inactivity Detection:

- ➢ If the user switches to another tab and leaves this one inactive for a while, a script detects the inactivity.

- ➢ After a set period (e.g., 30 seconds), the script changes the content of the inactive tab to mimic a login page for a trusted website (e.g., Gmail, Facebook, or a banking portal).

System Reconfiguration Attacks

- System reconfiguration attacks involve unauthorized changes to a system's settings or configuration parameters.

- These attacks aim to disrupt normal operations, create security vulnerabilities, or provide attackers with backdoor access to sensitive information

- Example : URLs saved under favorites in the browser might be modified. www.xyzbank.com to www.xyzbanc.com

Data Theft

- Data theft is the unauthorized acquisition of sensitive or confidential information, often for malicious purposes such as identity theft, financial fraud, or corporate espionage.

- It involves stealing data from individuals, organizations, or government entities without their consent.

- Phishers get profit from selling confidential information like design documents, legal opinions and employee related records.

Phoraging (Foraging)

- **Defined as 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-Pharming-Phoraging (3Ps of CyberCrime)**

Examples:

Social Media Foraging: Collecting personal details like birthdays, locations, and family members from social media profiles to answer security questions or craft personalized phishing emails.

Corporate Reconnaissance: Gathering organizational information, including employee names, job titles, and email formats, to launch spear-phishing attacks.

Clone Phishing

- ✓ Attackers create **identical copies** of legitimate emails but replace links/attachments with **malicious versions**.

✓ The new email appears to come from a trusted sender but redirects victims to fake websites.

Example: A cloned email from Microsoft asking you to log in, but the link leads to a **fake Office 365** login page.

Social Media Phishing

- Attackers send **fake messages** on social media platforms (Facebook, Instagram, LinkedIn).

✓ They pretend to be friends, brands, or job recruiters to **steal personal data**.

Example: Fake Facebook messages asking for password resets.

Content-Injection Phishing

- Content-Injection Phishing involves inserting malicious content into legitimate websites or emails to deceive users into providing sensitive information.

- Unlike traditional phishing, this technique leverages trusted platforms, making the attack more convincing and harder to detect.

Examples:

Website Compromise: A banking website is compromised to display a fake login form, capturing customer credentials.

Man-in-the-Middle Phishing

- **Where attackers intercept and manipulate communication between two parties without their knowledge.**
- The attacker secretly relays and possibly alters the communication, tricking users into revealing sensitive information like login credentials, financial data or personal details.

Example

Email Manipulation: Intercepting and altering email communication between a buyer and seller to change payment details, leading to financial fraud.

SSL Certificate Phishing

- SSL Certificate Phishing is a type of phishing attack where cybercriminals use fraudulent or misleading SSL certificates to make malicious websites appear secure and legitimate.

- These fake certificates trick users into trusting the site, as they see the secure padlock symbol and HTTPS in the browser's address bar.

Examples:

- **Typosquatting with SSL:** A fake website like amaz0n.com has a valid SSL certificate, tricking users into entering their Amazon login details.

Search Engine Phishing

- Search Engine Phishing, also known as SEO Poisoning, involves manipulating search engine results to promote malicious websites.

- These fake sites appear legitimate and rank highly in search results, tricking users into visiting them and entering sensitive information.

Search Engine Phishing

- **Creating Fake Websites:** Attackers create websites that closely resemble legitimate sites, such as online banking, e-commerce, or social media platforms.

- **SEO Manipulation:** They use Search Engine Optimization (SEO) techniques, including popular keywords, backlinks, and meta tags, to rank these fake sites higher in search engine results.

- **User Deception:** When users search for common services (e.g., customer support, software downloads, or banking), they are directed to the malicious sites, believing them to be authentic due to their high ranking.

- **Data Theft or Malware Distribution:** The fake websites prompt users to enter sensitive information (e.g., login credentials, credit card details) or trick them into downloading malware.

- **Exploitation:** The stolen data is used for identity theft, financial fraud, or sold on the dark web.

Common Techniques

- **Keyword Stuffing:** Using trending or commonly searched keywords to rank higher in search results.

- **Typosquatting and Homograph Attacks:** Registering domain names similar to legitimate sites (e.g., g00gle.com) to deceive users.

- **Poisoned Ads:** Creating fake advertisements that appear at the top of search results, leading to phishing sites.

- **Malicious Redirects**: Using compromised legitimate sites to redirect users to phishing pages.

Examples

- **Fake Customer Support Sites**: Phishing sites disguised as customer support for popular brands rank highly in search results, leading users to call fake support numbers and share personal details.

- **Fake Software Downloads**: Malicious websites offer fake versions of popular software, tricking users into downloading malware.

- **SEO-Boosted Scam Sites**: Scammers optimize fake online shopping sites with holiday sale keywords to capture payment information.

Distributed Phishing Attack (DPA)

- A Distributed Phishing Attack (DPA) involves launching **coordinated phishing campaigns from multiple sources or domains** to evade detection and maximize impact.

- By distributing the attack across different servers, email accounts, or websites, attackers make it more challenging for security systems to block or trace the origin of the phishing attempts.

- **Multiple Attack Vectors:** Attackers use a network of compromised servers, email accounts, or domains to send phishing emails or host phishing websites.

Example

- **Multi-Domain Phishing Campaigns:** A phishing attack that uses dozens of look-alike domains (e.g., paypall-support.com, pay-pal-login.com) to trick users into entering credentials.

Distributed Phishing Attack (DPA)

- **Multiple Attack Vectors:** Attackers use a network of compromised servers, email accounts, or domains to send phishing emails or host phishing websites.
- **Load Distribution**: By distributing the attack traffic, they avoid triggering security filters that detect large volumes of phishing messages from a single source.
- **Domain Rotation:** Phishing websites rotate across different domains or IP addresses to avoid being blacklisted.
- **Phishing Payloads**: The distributed nature allows attackers to host phishing pages, malicious downloads, or credential harvesters on multiple servers.
- **Data Collection and Exfiltration**: Stolen information is collected across multiple endpoints and exfiltrated to the attackers' central servers.

Distributed Phishing Attack (DPA)

- Domain Shadowing: Using compromised domains to create subdomains for phishing websites.
- Fast Flux DNS: Frequently changing IP addresses linked to phishing domains to evade detection.
- Botnets: Utilizing botnets to send phishing emails from multiple compromised devices worldwide.
- Malicious URL Shorteners: Distributing phishing links using multiple shortened URLs that redirect to phishing sites.
- Social Media Phishing: Using distributed social media accounts to share phishing links and malware.

Phishing Toolkits

- Phishing toolkits are pre-packaged software bundles designed to help cybercriminals create and deploy phishing attacks with minimal effort.

- These kits provide templates, scripts, and tools needed to build convincing phishing websites, craft deceptive emails, and harvest credentials or other sensitive information.

Phishing Toolkits

- ✓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.

Examples of Phishing Toolkits

- **Shadow Phisher**: Known for its realistic templates of social media and banking websites.
- **Hidden Cobra Phishing Kit:** Associated with advanced persistent threat (APT) groups, offering sophisticated anti-detection features.
- **WebPhish:** A beginner-friendly toolkit with easy-to-use templates and automated email dispatch.
- **Modlishka**: An advanced reverse proxy toolkit that supports real-time man-in-the-middle phishing attacks.
- **BlackEye and Zphisher:** Popular open-source phishing frameworks used to clone websites and capture credentials.

COVID-19 Scams: During the pandemic, phishing toolkits were used to create fake COVID-19 relief portals and vaccine registration sites.

Spy Phishing

- Spy Phishing is a type of phishing attack designed to secretly monitor and capture sensitive information without the victim's knowledge.

- Unlike traditional phishing, which relies on tricking users into entering credentials, spy phishing covertly records data such as keystrokes, screenshots, or browser activity.

- This information is then sent to the attacker, enabling them to steal personal details, financial information, or corporate secrets.

Spy Phishing

- **Infection Vector:** Attackers deliver spyware through phishing emails, malicious links, or infected attachments. Social engineering techniques are often used to lure victims into clicking on these links.

- **Silent Installation:** The spyware is installed silently in the background without the victim’s knowledge. It often disguises itself as legitimate software or hides in system processes.

- **Data Monitoring and Collection:** The spyware begins monitoring user activity, such as keystrokes, screenshots, clipboard data, or browser history.

- **Data Exfiltration:** Collected data is periodically sent to the attacker’s server for analysis and exploitation.

- **Continuous Surveillance:** Advanced spy phishing campaigns may allow attackers to remotely control the victim's device, activate webcams or microphones, or track real-time activity.

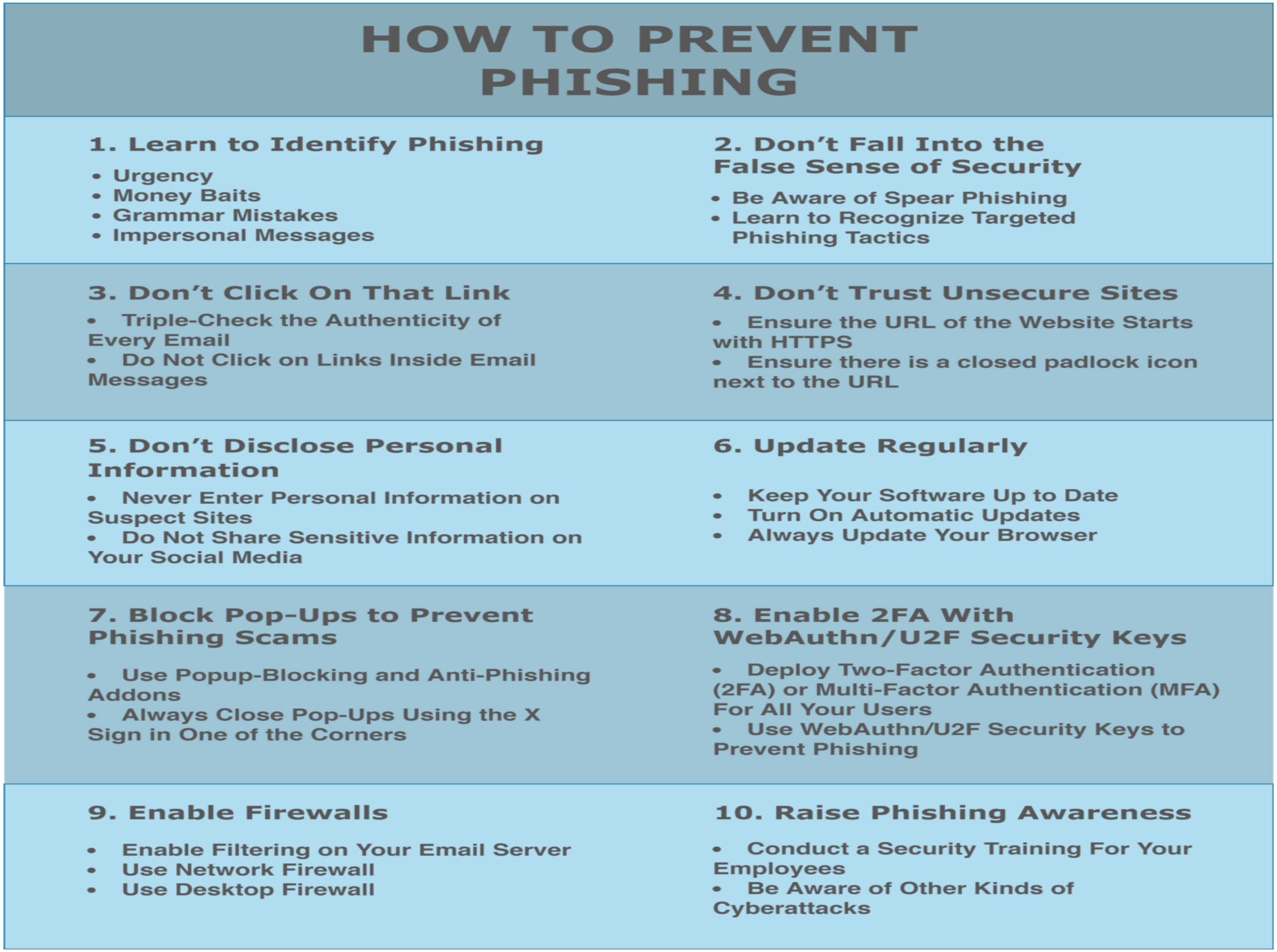
Spy Phishing

- **Fake Software Updates:** A phishing email tricks the user into installing a fake browser update that contains spyware.
- **Malicious Attachments:** An infected PDF or Word document installs keylogging malware when opened.
- **Social Media Links:** A shortened URL shared on social media leads to a compromised website that silently installs spyware.
- **BrowserExtensions:** Malicious browser extensions secretly monitor browsing activity and steal cookies.

How to avoid being a victim of a Phishing Attack?

- Keep Antivirus up to date
- Don’t click on hyperlinks in email
- Take advantage of anti-spam software
- Verify https(SSL)
- Use anti-spyware software
- Get Educated
- Use Microsoft Baseline Security Analyzer(MBSA)
- Firewall
- Use Backup System Images
- Do not enter sensitive or financial information into pop-up windows
- Secure the host file
- Protect against DNS Pharming attacks

Phishing Countermeasures



HOW TO PREVENT PHISHING

1. Learn to Identify Phishing

- Urgency
- Money Baits
- Grammar Mistakes
- Impersonal Messages

2. Don’t Fall Into the False Sense of Security

- Be Aware of Spear Phishing
- Learn to Recognize Targeted Phishing Tactics

3. Don’t Click On That Link

- Triple-Check the Authenticity of Every Email
- Do Not Click on Links Inside Email Messages

4. Don’t Trust Unsecure Sites

- Ensure the URL of the Website Starts with HTTPS
- Ensure there is a closed padlock icon next to the URL

5. Don’t Disclose Personal Information

- Never Enter Personal Information on Suspect Sites
- Do Not Share Sensitive Information on Your Social Media

6. Update Regularly

- Keep Your Software Up to Date
- Turn On Automatic Updates
- Always Update Your Browser

7. Block Pop-Ups to Prevent Phishing Scams

- Use Popup-Blocking and Anti-Phishing Addons
- Always Close Pop-Ups Using the X Sign in One of the Corners

8. Enable 2FA With WebAuthn/U2F Security Keys

- Deploy Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) For All Your Users
- Use WebAuthn/U2F Security Keys to Prevent Phishing

9. Enable Firewalls

- Enable Filtering on Your Email Server
- Use Network Firewall
- Use Desktop Firewall

10. Raise Phishing Awareness

- Conduct a Security Training For Your Employees
- Be Aware of Other Kinds of Cyberattacks

Sanitizing Proxy System (SPS)

- The **Sanitizing Proxy System (SPS)** is a security mechanism designed to thwart phishing attacks by filtering and sanitizing web content before it reaches the user.

- Its primary objective is to detect and neutralize phishing attempts while maintaining a seamless browsing experience.

- SPS acts as an intermediary between the user and the internet, inspecting and sanitizing all incoming web traffic to prevent phishing attempts.

- It intercepts requests, analyzes the content for malicious elements, and delivers a "clean" version of the webpage to the user.

Sanitizing Proxy System (SPS)

- **Content Analysis Engine** (Analyzes web content (HTML, scripts, links) for malicious code and phishing indicators.)
- **Sanitization Module** (Removes or neutralizes malicious scripts, links, and embedded content)
- **Behavioral Analysis** (Monitors the behavior of web elements to detect phishing tactics like fake login prompts and credential harvesting.)
- **Feedback and Learning Loop** (Continuously improves the detection engine by learning from new phishing patterns and user interactions.)

How SPS Thwarts Phishing Attacks?

- URL Validation: Identifies and blocks deceptive URLs and fake login pages.
- Content Sanitization: Removes malicious scripts designed to steal user credentials.
- Form Protection: Prevents unauthorized data collection by sanitizing form submissions.
- User Alerting: Warns users about suspicious sites or potential phishing attempts.

Examples of Software with SPS-like Capabilities

- Zscaler Internet Access – Secure web gateway with advanced phishing protection.
- Cisco Umbrella – Cloud-delivered security service with URL filtering and phishing defense.
- Symantec Web Security Service – Provides web content sanitization and anti-phishing protection.

Top Anti-Phishing Plugins for Browsers

- Netcraft Extension
- Avast Online Security
- Bitdefender TrafficLight
- PhishGuard
- Trend Micro Toolbar

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.

Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual, either on its own or when combined with other information.

- It is highly sensitive and requires protection to prevent identity theft, fraud, and privacy breaches.

Types of PII

- **Sensitive PII:** Information that, if compromised, could cause harm or fraud, such as SSNs, financial details, or biometric data.

- **Non-sensitive PII:** Publicly available information, like names or email addresses, that, on their own, pose minimal risk.

Personally Identifiable Information (PII)

1. Full name

2. National identification number

(e.g., **Social Security Number (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

Search Information

- **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

Classification of Information (Media and Asset Protection)

- Non-Classified Information

❖ Public Information

❖ Personal Information

❖ Private Information

❖ Routine Business Information

❖ Confidential Business Information

- Classified Information

✓ Confidential – Protection - (Information about strength if armed forces, technical info about weapon)

✓ Secret- Substantial Protection - (National Security Policy, Intelligence Operations)

✓ Top Secret – Highest Degree of Protection - (Vital Defense plans)

Types of Identity Theft

1. **F**inancial identity theft
2. **C**riminal identity theft
3. **I**dentity cloning
4. **B**usiness identity theft
5. **M**edical identity theft
6. **S**ynthetic identity theft
7. Child identity theft

Financial Identity Theft

- When someone steals your personal information (like credit card numbers, bank account details, or Social Security Number) to make unauthorized purchases, open new accounts, or obtain loans.

- To gain financial benefits, such as buying goods, withdrawing money, or getting credit.

Examples:

✓ Unauthorized credit card charges.

✓ Taking out loans or mortgages in your name.

Criminal identity theft

- Occurs when someone uses your identity during an arrest or investigation, leading to criminal records under your name.
- To avoid legal consequences or fines by impersonating another person.

Examples:

✓ A criminal provides your name and details during a police arrest.

✓ Using your identity to get a driver’s license, which is then used in criminal activity.

Identity Cloning

- When someone completely assumes another person’s identity to live as them, using their name, Social Security Number, and other personal details.

Examples:

✓ Applying for jobs or renting a house using your identity.

✓ Accessing healthcare or government benefits in your name

Business Identity Theft

- Involves stealing a business's identity to obtain credit, loans, or purchase goods and services, leaving the business liable for debts.
- To commit fraud, evade taxes, or acquire goods without payment.

Examples:

✓ Opening lines of credit using a business’s name and tax information.

✓ Filing false tax returns to get refunds.

Medical Identity Theft

- When someone uses your identity to obtain medical care, prescription drugs, or health insurance benefits.
- To receive medical treatment, surgeries, or medications fraudulently.

Examples:

- Using stolen health insurance information for medical procedures.
- Altering medical records, which can lead to dangerous health consequences.

Synthetic Identity Theft

- Involves creating a new, fake identity by combining real and fake information (e.g., using a real Social Security Number but a fake name).

- To open bank accounts, apply for loans, or obtain credit cards using a fabricated identity.

Examples:

- Using synthetic identities to apply for government benefits.

Child Identity Theft

- Involves stealing a child's Social Security Number or personal details to create fraudulent accounts or take out loans.

- **Examples**:

➢ Opening credit cards, loans, or utility accounts using a child’s identity.

Techniques of ID Theft

1. Human-Based Methods
2. Computer-Based Technique

Human-Based Methods

- Direct access to information (Degree of Trust)
- Dumpster Diving
- Theft of a wallet
- Mail Theft and re-routing
- Shoulder Surfing
- Skimming
- Dishonest Employees
- Fake Telephone calls

Computer-Based Technique

- Backup Theft
- Hacking
- Phishing
- Pharming
- Geotagging
- Redirectors
- Hardware

Identity Theft Countermeasure

- Strengthen Online Security
- Protect Personal Information
- Secure Financial Transactions
- Prevent Medical & Business Identity Theft
- Respond Quickly to Identity Theft
- Awareness and proactive security practices

Summary

- Phishing
- Types of Phishing
- Toolkit
- Identity Theft
- Countermeasures