Four Weeks Industrial Training Project Report on

Social Engineering

Submitted in the partial fulfilment of the requirement for the award of degree of

Bachelor of Computer Application

in

Lamrin Tech Skills University Of Punjab

Batch

(2023-2026)

Submitted to:

Ms. Shikha Thakur

Submitted by:

Bandana BCA 5TH

Roll No:-23202002708

DEPARTMENT OF COMMERCE AND MANAGEMENT

LAMRIN TECH SKILLS UNIVERSITY OF PUNJAB

ACKNOWEDGEMANET

I express my gratitude to all those who helped us in various stages of the development of this project. First, I would like to express my sincere gratitude indebtedness to______________(Coordinator) of DAV University for allowing me to undergo the summer training of 45 days at..I am also thankful to all faculty members of Department of Computer Science and Engineering, for their true help, inspiration and for helping me for the preparation of the final report and presentation.

Last but not least, I pay my sincere thanks and gratitude to all the Staff Members of...........<institute/company name>… for their support and for making our training valuable and fruitful.

DECLARATION

I, <Student Name>, hereby declare that the work which is being presented in this project/training titled "………………………………………………….." by me, in partial fulfilment of the requirements for the award of Bachelor of Technology (B.C.A Degree in "Computer Science and Application" is an authentic record of my own work carried out under the guidance of Mr………………… …………(Name & Designation of trainer)……………..
……………………………………………………………………………………………….
.

To the best of my knowledge, the matter embodied in this report has not been submitted to any other University/ Institute for the award of any degree or diploma.

Student Name and Signature

<Roll No.>

ABOUT INSTITUTE

ThinkNEXT Technologies in Mohali offers a valuable training ground for students seeking practical experience and career development. The institute is well-regarded for its comprehensive training programs and industry certifications, making it a strong choice for internships. Let's delve into the specifics that make this institute an excellent inclusion in your report.

About ThinkNEXT Technologies:

ThinkNEXT Technologies is an established IT company operating as a Private Limited entity approved by the Ministry of Corporate Affairs, Govt. of India, with Corporate Identity Number: U72200PB2011PTC035677. The company has garnered national recognition through various awards for its work in fields like web development, digital marketing, and industrial training. ThinkNEXT has also forged strong alliances with industry giants, being certified by Google, Facebook, Microsoft, and Hubspot.

Training and Specializations:

The institute provides a diverse range of training and internship programs tailored to meet industry demands. These programs cater to students from various academic backgrounds, including engineering disciplines like Computer Science, IT, Electronics, Mechanical, Civil, and Electrical, as well as Management and other graduate programs. Training areas include popular choices like digital marketing, web design and development, data science, and mobile app development. Interns gain hands-on experience through training on live projects, ensuring they are well-prepared for real-world scenarios.

Modes of Learning:

ThinkNEXT offers flexible learning options to accommodate different needs. Students can choose between traditional classroom-based training or instructor-led live online sessions. For those needing flexibility, the institute provides customized remote internships as well as various durations ranging from 1 month to longer-term programs.

Enhancing Employability:

ThinkNEXT is dedicated to improving the employability of its students. They provide free access to valuable resources such as Spoken English, Personality Development, and Interview Preparation classes. Interns also have the opportunity to acquire internationally recognized certifications from companies like Microsoft, Apple, and Adobe. Furthermore, the institute offers placement assistance, conducting regular job interviews to help students secure positions with their numerous placement partners. ThinkNEXT also offers stipend-based and free internship options to support students financially while they gain experience.

These aspects highlight ThinkNEXT's dedication to providing a holistic and impactful internship experience, positioning it as a strong choice for career development in the region.

ABSTRACT

Social engineering is a deceptive technique used by attackers to manipulate individuals into giving up confidential information or taking actions that may harm an organization’s security. Unlike traditional hacking, which focuses on breaking into systems using software or technical tools, social engineering relies on understanding and exploiting human behaviour. Attackers use psychological tricks and emotional manipulation to gain trust, create a false sense of urgency, or simply take advantage of people’s willingness to help. This type of attack can happen through various forms of communication—such as emails, phone calls, social media messages, or even face-to-face interactions—making it one of the most versatile and dangerous methods in cybersecurity. Because social engineering does not require high-level technical knowledge to execute, it is often used by both amateur criminals and advanced threat actors to bypass security systems without ever needing to crack a password or breach a firewall.

The success of social engineering lies in its ability to disguise itself as normal behaviour. For example, an attacker may send a fake email pretending to be a manager or a bank representative, asking the recipient to share login details, download a file, or click on a malicious link. These emails are often well-crafted and designed to look genuine, which makes it difficult for the average user to identify them as threats. Sometimes, attackers create convincing stories or situations—known as pretexts—that trick people into sharing sensitive data without realizing it. Other common tactics include offering fake prizes, tech support scams, and even gaining physical access by following employees into secure buildings and pretending to be authorized visitors. In all of these cases, the attacker relies on psychological pressure, such as urgency, fear, curiosity, or trust, to get the victim to act quickly and without thinking critically.

Social engineering has become increasingly common in modern digital environments where people rely heavily on technology for communication and daily tasks. Its impact can be devastating—leading to data theft, financial loss, identity fraud, or unauthorized access to internal systems. What's particularly dangerous is that these attacks can bypass even the most advanced security software, simply by tricking a person into opening the door. Because of this, organizations now recognize that technical defenses alone are not enough. Educating users about social engineering has become just as important as installing antivirus programs or setting strong passwords. Security awareness training helps employees recognize suspicious behavior, question unusual requests, and respond appropriately to potential threats. When users are well-informed and alert, they act as a powerful line of defense against manipulation.

In conclusion, social engineering is not just a technical issue—it’s a human issue. It targets the psychology of trust and behavior, making everyone a potential victim regardless of how advanced their security systems may be. This report aims to highlight the importance of understanding how social engineering works and stresses the need for combining technological protection with human awareness. By learning to recognize and resist manipulation, individuals and organizations can take major steps toward strengthening their overall cybersecurity.

Contents

1) Understanding the Concept of Social Engineering

- **An Overview of Social Engineering:**

In today’s highly digital and interconnected world, cybersecurity has become one of the most critical aspects of personal and organizational safety. While a lot of focus is placed on securing systems through firewalls, antivirus software, and encryption, one major vulnerability often gets overlooked — human behavior. This is where Social Engineering comes into play. It is a method used by cybercriminals to manipulate individuals into giving up confidential or sensitive information. Unlike traditional hacking, which relies on technical skills and software exploits, social engineering targets the human mind. It is often easier to trick someone into revealing a password than it is to hack into a well-secured system.

Social engineering refers to the act of exploiting human behavior and emotions to gain unauthorized access to systems, networks, or confidential information. Unlike traditional hacking, which involves exploiting technical weaknesses or software flaws, social engineering relies on deception and manipulation. It is based on the idea that people are often the weakest link in any security system. By tricking someone into clicking a malicious link, sharing a password, or revealing personal information, attackers can bypass even the most secure technical defenses.

This form of attack is increasingly popular among cybercriminals because it is often simpler, cheaper, and more effective than traditional hacking methods. For example, instead of trying to break into a company’s secure database using advanced tools, an attacker might call an employee pretending to be from the IT department and ask for login credentials under the pretense of fixing a technical issue. In many cases, the victim does not even realize they’ve been manipulated until after the damage is done.

The effectiveness of social engineering lies in its ability to exploit natural human tendencies such as trust, fear, curiosity, or helpfulness. Most people are not trained to recognize deceptive behavior, especially when it appears to come from a familiar or authoritative source. As a result, social engineering attacks often go unnoticed and unreported, making them difficult to detect and prevent. Some of the most common methods include phishing emails, fake phone calls, impersonation, baiting, and pretexting — each designed to manipulate people into acting against their best interests.

Over the past decade, many major data breaches and security incidents have been traced back to social engineering. Companies have lost millions in revenue, suffered reputational damage, and exposed customer data — all because one person clicked a malicious link or shared information without verifying the request. This highlights the critical need to understand how social engineering works and how to defend against it. Awareness, education, and vigilance are essential in reducing the risk of such attacks.

What is Social Engineering?

Social engineering is a psychological manipulation technique used by cyber attackers to deceive individuals into revealing sensitive information or granting unauthorized access. Unlike traditional hacking, which targets technical vulnerabilities, social engineering focuses on exploiting human behavior — such as trust, fear, urgency, or curiosity.

At its essence, social engineering operates on the premise that it’s often easier to trick a person than to bypass a secure system. For example, an attacker may impersonate a trusted authority figure — such as an IT administrator or bank representative — to convince a user to disclose login credentials or click on a malicious link. Because the victim believes the request is legitimate, they unknowingly assist in compromising their own security.

This method is particularly effective because it bypasses technical barriers entirely. Even systems with strong defenses can be breached if a user is manipulated into opening the door. Social engineering can take many forms, including phishing emails, fake phone calls (vishing), or deceptive messages on social media — all designed to prompt impulsive or uninformed actions.

The true danger lies in its subtlety. Social engineers often conduct careful research beforehand, tailoring their attacks to be as believable and targeted as possible. As a result, even well-trained professionals can fall victim if they are caught off guard.

In today’s threat landscape, social engineering remains one of the most powerful tools in a cybercriminal’s arsenal. Combating it requires more than just technical controls — it demands awareness, training, and a culture of security-minded thinking across all levels of an organization.

How Does Social Engineering Work?

Social engineering operates on a fundamental truth in cybersecurity: the human mind is often the weakest link in any secure system. No matter how advanced firewalls, encryption protocols, or antivirus software become, they can all be bypassed if one person is convinced to hand over access. Social engineering works by exploiting this reality — using psychological manipulation, strategic deception, and personalized communication to trick individuals into giving up valuable information or unknowingly granting access to secure systems.

Rather than relying on technical skills to break into a system, social engineers carefully design scenarios that cause people to trust, panic, or act impulsively. Their methods can be subtle, convincing, and surprisingly effective — making social engineering one of the most dangerous and hard-to-detect attack strategies in the cybersecurity world today.

Below is a detailed breakdown of how a typical social engineering attack is planned and executed:

1. Reconnaissance – The Foundation of the Attack:

The first phase of a social engineering attack is reconnaissance. This involves the attacker doing a thorough investigation on the target to gather as much information as possible. Reconnaissance is like a foundation. Without it, the rest of the attack will not be successful.

During reconnaissance, attackers do not directly contact the victim. Instead, they silently collect data using publicly available sources. This phase can last from hours to weeks, depending on the attacker's goal and the complexity of the attack.

Sources of Information:

- Social Media Platforms: LinkedIn, Facebook, Instagram, and Twitter are goldmines for attackers. They can find information about a person's job, workplace, schedule, hobbies, family, and more.
- Company Websites and Newsletters: These often include employee names, designations, office addresses, recent achievements, and structural hierarchies.
- Online Forums and Public Support Requests: Sometimes people post complaints or questions online, which can reveal technical problems or company procedures.
- Leaked Databases: If the target was involved in a past data breach, attackers can reuse their old credentials.

The main objective is to understand how the target thinks and behaves. What do they care about? What are their routines? What emotions can be triggered easily? This information helps the attacker create a believable story later.

Attackers might also gather indirect information — such as what operating systems a company uses, what kinds of vendors they work with, or what tools their employees use. For example, if a company uses Microsoft Outlook for internal communications, an attacker might craft a fake Outlook-related email to blend in. The more detailed the research, the more believable the story.

2. Crafting the Scenario – Designing the Deception:

Once the attacker has enough background data, they move to the second step: crafting a believable scenario. This is the step where creativity and psychology come together.

The attacker creates a fake but convincing story tailored specifically to the target. The more personalized the story, the more effective it becomes. This stage is like writing a script for a play — every line, every role, and every event has to feel natural.

The Attacker Decides:

- Role to Play: IT support, HR manager, bank officer, team leader, a colleague, or even a customer. The role must sound logical and blend into the victim's environment.

- Narrative to Use: Examples include "There is a virus in your system," "Your salary details need urgent confirmation," or "Your account is under investigation." Sometimes attackers may even create fake emergencies, such as saying that there has been a data breach and asking the target to log in to a fake security portal.
- Emotions to Trigger: Urgency, fear, anxiety, excitement, or trust. The more emotional the target becomes, the more likely they are to react without thinking.

This phase requires the attacker to anticipate how the victim will respond. They carefully structure the conversation so that the victim has very little time or mental space to think critically.

3. Initial Contact – Opening the Door:

Now the attacker initiates direct contact. They choose a method that matches the scenario and is most likely to succeed. The attacker could reach out by email, phone, text message, social media, or even in person.

Common Communication Methods:

- Phishing: Fake emails that appear to be from trusted sources. These often contain malicious links or attachments.
- Vishing (Voice Phishing): Phone calls claiming to be from technical or financial departments. Attackers use caller ID spoofing to make the number look legitimate.
- Smishing (SMS Phishing): Urgent-looking messages sent via text. These messages often include fake tracking links or account warnings.
- Social Media Chats: Messages that appear to be from friends or coworkers. Attackers may use hacked accounts to reach others.
- Tailgating or Physical Entry: Entering secured buildings by following someone inside without authorization. Attackers may wear uniforms or carry fake IDs.

Examples of Phrases Used:

- “Hi, I’m from IT. We noticed strange activity on your account. Can I have your password to fix it?”
- “Your bank account is under threat. Please confirm your ATM PIN.”
- “This is HR. We need you to re-upload your identity documents urgently due to a system error.”

In most cases, the attacker sounds calm, professional, and friendly. They may even engage in small talk to put the victim at ease before launching the real request. This makes the attack feel more natural and trustworthy.

4. Psychological Manipulation – Exploiting Human Nature:

This is the core of social engineering. It works because it takes advantage of how humans naturally think and feel.

Key Emotional Triggers Used:

- **Authority:** People tend to obey figures of authority. Attackers may pose as bosses, police officers, IT heads, or bank managers to pressure the victim into compliance.
- **Urgency or Fear:** Creating a sense of crisis causes people to act before thinking. Attackers might say "your account will be locked in 5 minutes unless…" or "you've been exposed to a virus; click here immediately."
- **Curiosity:** People are naturally curious. A vague subject line like "Confidential Info – Don't Share" or "URGENT: Salary Update" can easily get someone to open a malicious link.
- **Helpfulness or Empathy:** Employees often want to be helpful. Social engineers may exploit this by pretending to be a new employee who is "locked out" or an elderly person needing assistance.

Attackers are highly skilled at emotional manipulation. They may mimic a tone of concern, urgency, friendliness, or professionalism depending on what works best. This manipulation bypasses logical reasoning and creates a direct path to the victim's instinctive response.

5. Execution – Gaining Access or Information:

When the victim is convinced, the attacker proceeds to carry out the main part of the attack. This might include:

- Stealing login credentials
- Convincing the user to download malicious software
- Getting the victim to transfer money or reveal sensitive data
- Accessing restricted areas physically or digitally

In some cases, attackers may use fake websites that look nearly identical to real ones. Victims unknowingly enter their usernames and passwords into these websites, thinking they are legitimate.

Some attacks are simple, like getting someone to reset their password. Others are complex and may involve multiple people, fake forms, and even staged video calls with deepfake technology.

What makes this step so dangerous is that the victim usually performs the action themselves, believing they are doing the right thing. This means there are no warning alerts or system flags to stop the action.

6. Post-Attack Phase – Covering Tracks or Maintaining Access:

After the attacker succeeds, they may try to hide their tracks or stay connected to the system for future attacks.

Post-Attack Activities Include:

- Deleting emails or messages that were part of the attack
- Changing credentials to lock out the real user
- Installing hidden malware or backdoors
- Continuing communication as a trusted person for further manipulation

A clever attacker does not stop at one success. They know that maintaining access allows them to gather more information or launch deeper attacks later. Sometimes, they use the victim's own email or device to reach others within the same organization, causing widespread damage.

Why Social Engineering is So Dangerous?

What makes social engineering such a terrifying method is not just its success rate, but also how simple and hard to detect it is. It doesn't require fancy hacking tools. All it needs is patience and a deep understanding of human psychology.

Key Reasons for Its Danger:

- **Targets Human Emotions:** Social engineering manipulates basic human instincts like fear, curiosity, urgency, or trust. Unlike machines, people are emotional — making them easier to deceive than hacking a system.
- **Bypasses Security Systems:** Even the best antivirus or firewall can't stop a user from willingly sharing sensitive information. Attackers exploit people, not software, making this tactic very hard to block.
- **Hard to Detect:** Social engineering often uses legitimate-looking messages or interactions that don't leave any malware or logs behind. As a result, it becomes nearly invisible to standard security tools.
- **High Success Rate:** Most users are unaware of these manipulation tactics and fall into the trap without realizing it. Even professionals can get tricked if the attacker plays the role well.
- **Scalable & Flexible:** These attacks can be done one-on-one (like spear phishing) or in mass (bulk phishing). The same method can be customized for small or large groups with ease.
- **Low Cost, High Impact:** A hacker doesn't need expensive tools — just a fake email, phone call, or message is enough. It's a cheap and efficient way to cause big damage.
- **Abuses Trust:** By pretending to be a boss, IT support, or a friend, attackers take advantage of the natural trust we place in people we know or recognize.

- **One Breach, Many Losses:** A single mistake — like clicking a bad link — can lead to larger attacks, including data leaks, ransomware, or full network access.

  Social engineering does not depend on the victim being careless or unintelligent. Even highly trained professionals can fall for it because it is designed to work on basic human instincts. The most advanced firewalls or antivirus software cannot stop a user from willingly handing over their password.

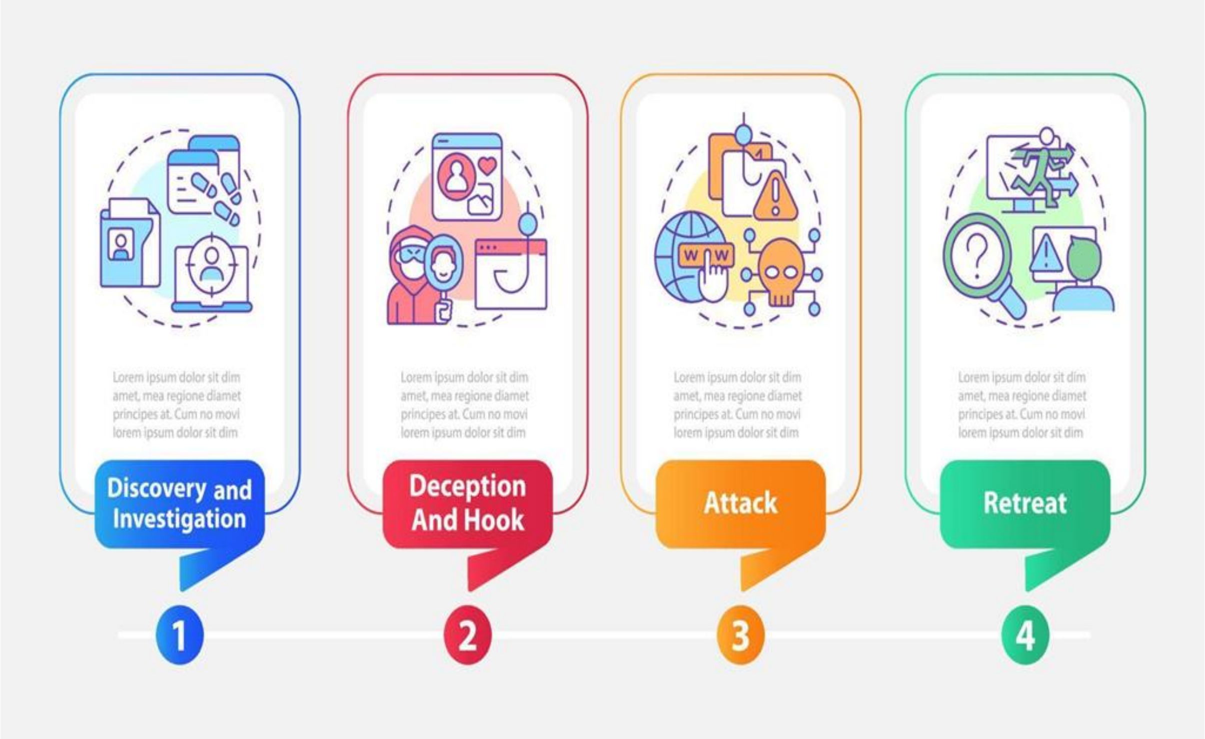

Discovery and Investigation
Deception And Hook
Attack
Retreat
1
2
3
4
Lorem ipsum dolor sit dim amet, mea regione diamet principes at. Cum no movi lorem ipsum dolor sit dim

FIG 1.1

2) SOCIAL ENGINEERING ATTACK

What is a social engineering attack?

A social engineering attack is a type of cyber attack where the hacker doesn't break into systems using advanced technology — instead, they trick people into giving away sensitive information or access.

Instead of "hacking a computer," the attacker hacks human behavior — by lying, pretending, or manipulating emotions like fear, curiosity, urgency, or trust.

Think of it like this:

🔒 "Why pick a lock when you can just ask someone to open the door for you?"

That's exactly how social engineering works — attackers pretend to be someone trustworthy like a bank officer, company employee, or friend, and trick the victim into clicking a link, sharing a password, or transferring money.

Why is it so dangerous?

- It targets people, not machines.
- It can bypass even the strongest security systems if a person makes one wrong move.
- It's often difficult to detect until the damage is already done.

➢ How does Social Engineering Attack works?

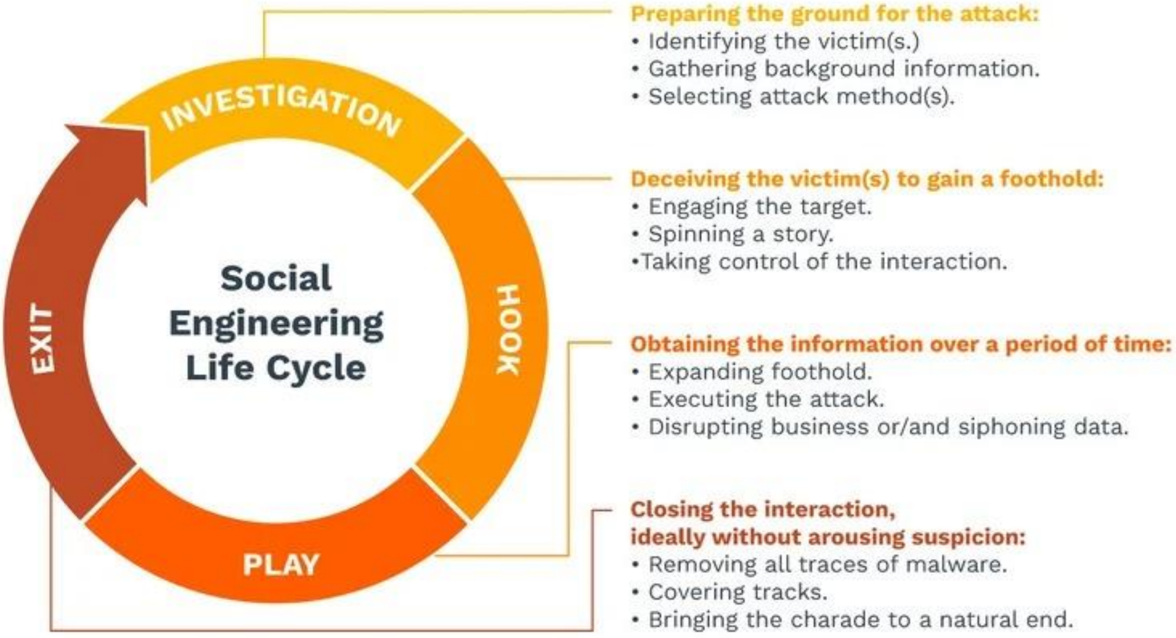

Social Engineering Life Cycle
INVESTIGATION
HOOK
PLAY
EXIT
Preparing the ground for the attack:
• Identifying the victim(s.)
• Gathering background information.
• Selecting attack method(s).
Deceiving the victim(s) to gain a foothold:
• Engaging the target.
• Spinning a story.
•Taking control of the interaction.
Obtaining the information over a period of time:
• Expanding foothold.
• Executing the attack.
• Disrupting business or/and siphoning data.
Closing the interaction,
ideally without arousing suspicion:
• Removing all traces of malware.
• Covering tracks.
• Bringing the charade to a natural end.

FIG 2.1

STAGES OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks are psychological manipulations used to deceive individuals into revealing confidential information or performing harmful actions. These attacks follow a structured process with specific stages, each designed to gradually lower the victim's defenses and increase the success of the final attack. Below are the five comprehensive stages of a social engineering attack, explained in detail:

1. Reconnaissance (Information Gathering):

This is the most critical and time-consuming phase of the attack. The attacker spends time silently gathering all possible information about the target — whether an individual, a group, or an entire organization. The attacker does not directly interact with the target at this point, which makes this phase difficult to detect.

Key Activities:

- **Social Media Scanning:** Analyzing LinkedIn, Facebook, Instagram, or Twitter profiles to extract names, interests, vacations, birthdays, job positions, and more.
- **Google Dorking:** Using advanced search operators to find hidden documents or files on company websites.
- **Corporate Website Analysis:** Checking the team section, organizational structure, email formats, ongoing projects, or open job listings.
- **Third-Party Breaches:** Searching the dark web or leaked databases to find if the target's credentials were exposed in previous data breaches.

Example:

An attacker finds out from an employee's LinkedIn that they recently joined the IT department. Using that, the attacker might craft a scenario posing as an onboarding specialist or vendor.

Objective: Collect maximum background information to make the next steps seem natural, real, and trustworthy.

2. Engagement (Interaction & Trust Building):

Once enough information has been gathered, the attacker begins actively engaging with the target, often through digital or verbal communication. This phase is designed to appear harmless and friendly to build trust, reduce suspicion, and increase the chances of cooperation.

Techniques Used:

- **Pretexting:** Creating a believable backstory to justify why the attacker is reaching out. E.g., pretending to be from the HR department requesting document verification.
- **Impersonation:** Mimicking a trusted person's identity — like a CEO, coworker, client, or technical support executive.
- **Phishing & Vishing:** Sending emails, messages, or making calls that look urgent, official, or beneficial.

Realistic Scenario:

An attacker sends a WhatsApp message pretending to be the company's IT team, saying:

"Due to a security update, we need you to verify your login. Please click the link below within 30 minutes to avoid account lockout."

Objective: Establish a sense of legitimacy and comfort, tricking the victim into responding or cooperating.

3. Exploitation (Manipulating Human Behaviour):

Now that trust has been established, the attacker uses psychological tactics to manipulate the victim into taking action that serves the attacker's purpose. This is where human emotions like fear, urgency, greed, or helpfulness are heavily exploited.

Manipulation Tactics:

- **Urgency:** "You must act now, or you'll lose access!"
- **Authority:** "I'm from the head office. You need to follow this protocol."
- **Curiosity or Greed:** Offering fake rewards, gift cards, or prizes in exchange for clicks or personal information.

Actions Triggered:

- Victim enters login credentials on a fake website.
- Victim installs malicious software thinking it's an update.
- Victim shares confidential files, passwords, or OTPs.
- Victim unknowingly gives remote access to attacker via tools like AnyDesk or TeamViewer.
- **Objective:** Trigger the victim to perform an action that gives control, access, or information to the attacker.

4. Execution (Attack Launch / Objective Fulfilled):

In this stage, the attacker successfully launches the attack or achieves their goal, using the access, information, or control gained from the victim in the previous step. Depending on the nature of the attack, the consequences can vary from mild data leaks to major financial or reputational damage.

Common Goals Achieved:

- Unauthorized access to business-critical systems
- Theft of personal or corporate data
- Installation of malware, ransomware, or keyloggers
- Fund transfers or financial frauds
- Identity theft and misuse

Example:

A victim unknowingly provides their Office365 credentials through a phishing email. The attacker now accesses sensitive company emails, downloads data, or sends malicious emails to other employees from the same account.

Objective: Complete the purpose of the attack — be it data theft, sabotage, blackmail, or financial gain.

5. Exit Strategy (Covering Tracks):

A professional attacker knows how to exit the system cleanly, minimizing the chances of being detected. They erase evidence, cover logs, and may even leave hidden backdoors to maintain future access.

Activities Performed:

- Deleting sent phishing emails or messages
- Clearing system logs and browser histories
- Changing passwords or security settings
- Installing silent spyware for future surveillance
- Logging out or closing fake sessions

Long-term Impact: Sometimes, attackers remain undetected for weeks or months — silently watching or stealing — because they cleaned up their tracks effectively after the initial breach.

Objective: Avoid detection, erase footprints, and possibly ensure future access to the compromised environment.

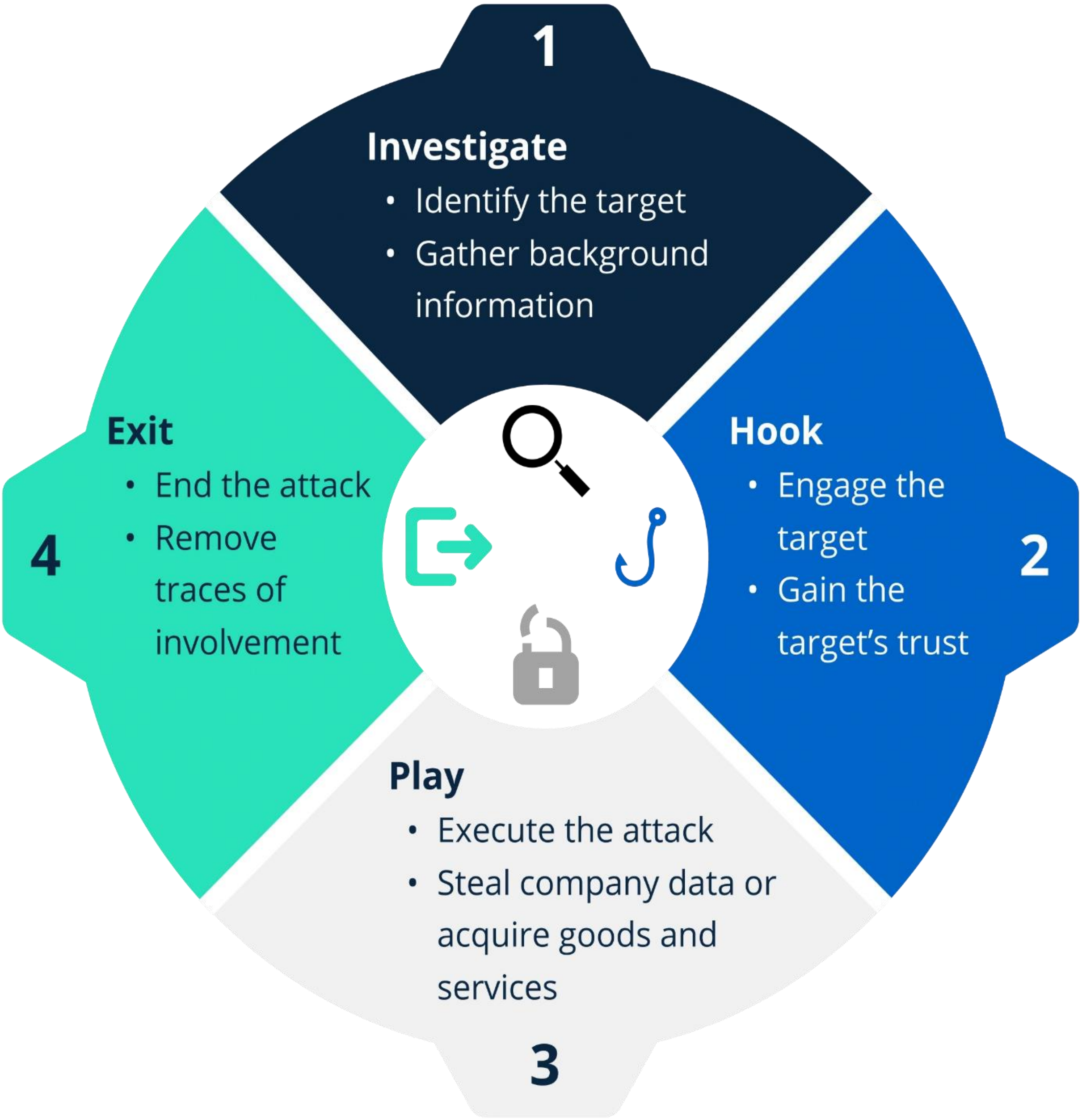

1
Investigate
• Identify the target
• Gather background information
2
Hook
• Engage the target
• Gain the target's trust
3
Play
• Execute the attack
• Steal company data or acquire goods and services
4
Exit
• End the attack
• Remove traces of involvement

FIG 2.2

TYPES OF ATTACKS

Social engineering attacks come in various forms, each exploiting human behavior and trust to gain unauthorized access to sensitive data, systems, or physical spaces. These attacks are often subtle and manipulative, making them highly effective and dangerous. Below are the most common and significant types of social engineering attacks:

1. Phishing

Definition:

Phishing is a cyber-attack where fake emails, messages, or websites are used to trick users into revealing sensitive information like passwords, bank details, or personal data.

How it Works:

The attacker sends an email or message pretending to be from a trusted source (like a bank or service provider). It often contains a link to a fake login page that records your credentials.

Example:

A user receives an email from “PayPal” saying their account is suspended. The email provides a link to log in and fix the issue, but it leads to a fake site that steals the login details.

2. Spear Phishing

Definition:

Spear phishing is a targeted phishing attack aimed at a specific individual or organization using personal or contextual information.

How it Works:

The attacker researches the target (via social media or company websites) and crafts a personalized email that seems trustworthy and relevant, increasing the chance of success.

Example:

An attacker emails a company’s finance manager pretending to be the CEO, asking for an urgent wire transfer to a client — using real names and references.

3. Vishing (Voice Phishing)

Definition:

Vishing is a type of social engineering attack conducted over phone calls to trick victims into giving up confidential details.

How it Works:

Attackers impersonate banks, government officials, or tech support. They use fear or urgency to pressure victims into revealing information like PINs or OTPs.

Example:

A caller claims to be from your bank and says your account has been compromised. You’re asked to confirm your card number and OTP to “secure” it.

4. Smishing (SMS Phishing)

Definition:

Smishing involves sending deceptive SMS messages to trick users into clicking malicious links or sharing sensitive information.

How it Works:

The message may contain fake alerts, offers, or delivery notifications. Clicking the link often installs malware or leads to phishing websites.

Example:

You receive a text saying, “Your income tax refund is ready. Click here to claim.” The link takes you to a fake government page asking for your PAN and bank details.

5. Pretexting

Definition:

Pretexting involves creating a false scenario or role to trick someone into revealing information or performing actions.

How it Works:

Attackers often pose as authority figures like HR staff, police, or IT technicians. They build trust using believable stories and then ask for access or data.

Example:

An attacker calls an employee pretending to be from the HR department and asks for personal details to “update records.”

6. Baiting

Definition:

Baiting uses false promises to lure victims into a trap that infects their system with malware or steals data.

How it Works:

The attacker places something attractive (free music, USB drives, or software) where users will find it and use it.

Example:

A pen drive labeled “Bonus Salaries 2025” is left near office desks. An employee plugs it in, activating spyware.

7. Scareware

Definition:

Scareware tricks users into thinking their device is infected and urges them to install harmful software disguised as antivirus tools.

How it Works:

Pop-up messages or fake scans claim the system is infected and prompt the user to click or download malicious software.

Example:

A user browsing the web sees a warning: “Virus Detected! Download antivirus now!” The tool they download is actually malware.

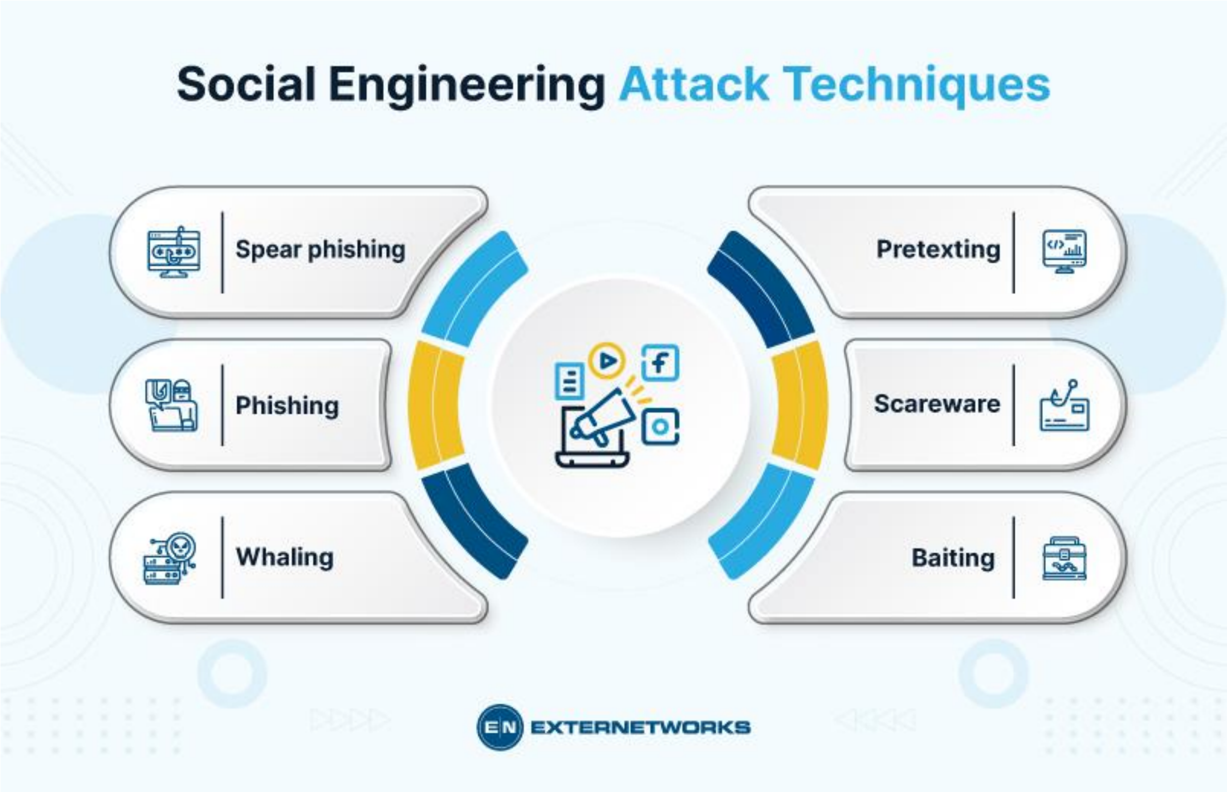


FIG 2.3

3) PHISHING

➢ What is Phishing?

Phishing is a common type of cyber-attack that targets individuals through email, text messages, phone calls, and other forms of communication. A phishing attack aims to trick the recipient into falling for the attacker's desired action, such as revealing financial information, system login credentials, or other sensitive information. Fundamentally, these threats exploit human psychology rather than technical vulnerabilities.

As a popular form of social engineering, phishing uses psychological manipulation and deception whereby threat actors masquerade as reputable entities to mislead users into performing specific actions. These actions often involve clicking links to fake websites, downloading and installing malicious files, and divulging private information, like bank account numbers or credit card information.

Since the mid-1990s, the term "phishing" has been used to identify hackers who use fraudulent emails to "fish for" information from unsuspecting users. However, phishing attacks have become increasingly sophisticated and are now broken down into different types, including email phishing, spear phishing, smishing, vishing, and whaling. Each type is characterized by specific channels and methods of execution—email, text, voice, social media, etc.—all with a similar underlying intention of exploiting human trust and decision-making processes.

HOW PHISHING WORKS?

A phishing campaign always starts with a malicious message disguised to look like it's from a legitimate sender, usually a company. The more aspects of the message that mimic the real company, the more likely an attacker will be successful.

While their goals may vary, attackers aim to steal personal information or credentials. An attack is facilitated by injecting a sense of urgency into the message by, for example, threatening account suspension, money loss, or loss of one's job. Users tricked into an attacker's demands typically don't take the time to consider if the demands seem reasonable or if the source is legitimate.

"Cyber criminals know that humans can be easily exploited, either through negligence, compromised identity—or in some instances—malicious intent,". "Individuals play a central role in an organization's security posture, with 74% of breaches still centering on the human element. While fostering a security culture is important, training alone is not a silver bullet. Knowing what to do and doing it are two different things."

It only takes one person to fall for a phishing attack to incite a severe data breach. That's why it's one of the most critical and challenging threats to mitigate, as it requires human defenses.

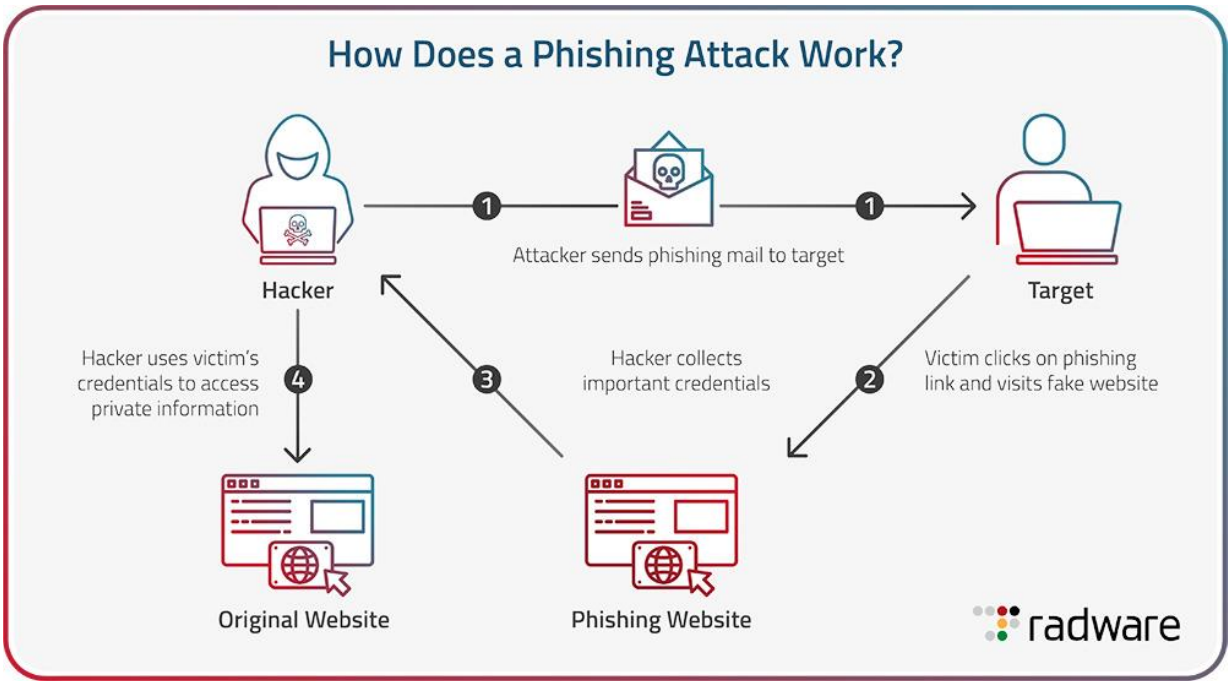
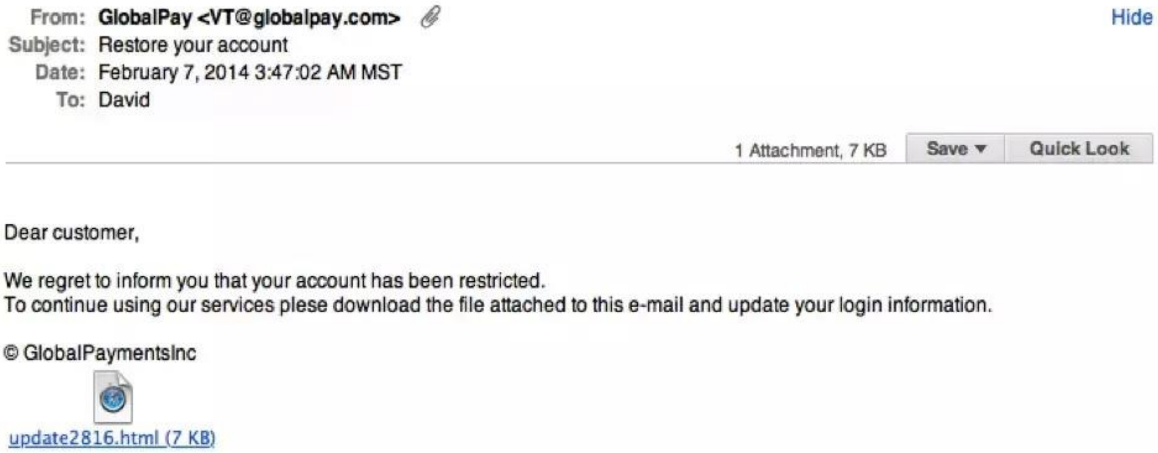

How Does a Phishing Attack Work?
Hacker
1
1
Attacker sends phishing mail to target
Target
Hacker uses victim's credentials to access private information
4
3
Hacker collects important credentials
2
Victim clicks on phishing link and visits fake website
Original Website
Phishing Website
radware

FIG 3.1

PHISHING EXAMPLES:

Attackers prey on fear by creating a sense of urgency, often using strategies that tell users their account has been restricted or will be suspended if they don't respond to the email. Because phishing attacks are typically sent to as many people as possible, the messaging is usually thin and generic. The following illustrates a common phishing email example.



From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

1 Attachment, 7 KB

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

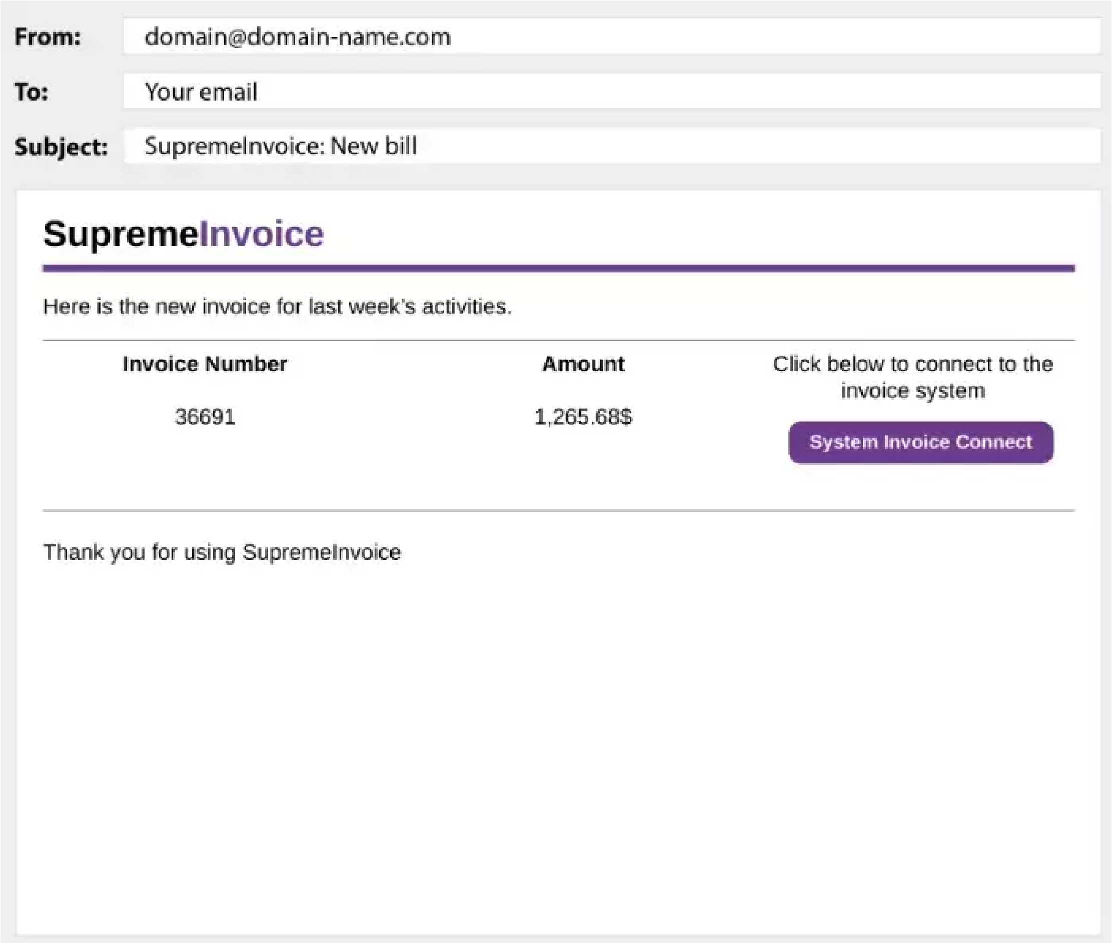
update2816.html (7 KB)

FIG 3.2

In the above message, the user's name is not mentioned, and the sense of urgency tricks users into opening the attachment.

The attachment could be a web page, a shell script (e.g., PowerShell), or a Microsoft Office document with a malicious macro. The macro and scripts can be used to download malware or trick users into divulging their account credentials. In some email phishing tactics, attackers register domains similar to their official counterparts or occasionally use generic email providers such as Gmail. The messages might contain the official company logo, but the sender's address would not include the official company domain.

How an attacker carries out a phishing campaign depends on their goals. Attackers may attach fake invoices to trick an organization's accounts payable department into sending money.



From:	domain@domain-name.com
To:	Your email
Subject:	SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	

Thank you for using SupremeInvoice

FIG 3.3

The button in this example opens a web page with a fraudulent Google authentication form. The page attempts to scam targeted victims into entering their Google credentials so that attackers can steal accounts. These social engineering tactics are designed to bypass technical security measures by manipulating the people who have legitimate access to systems and data.

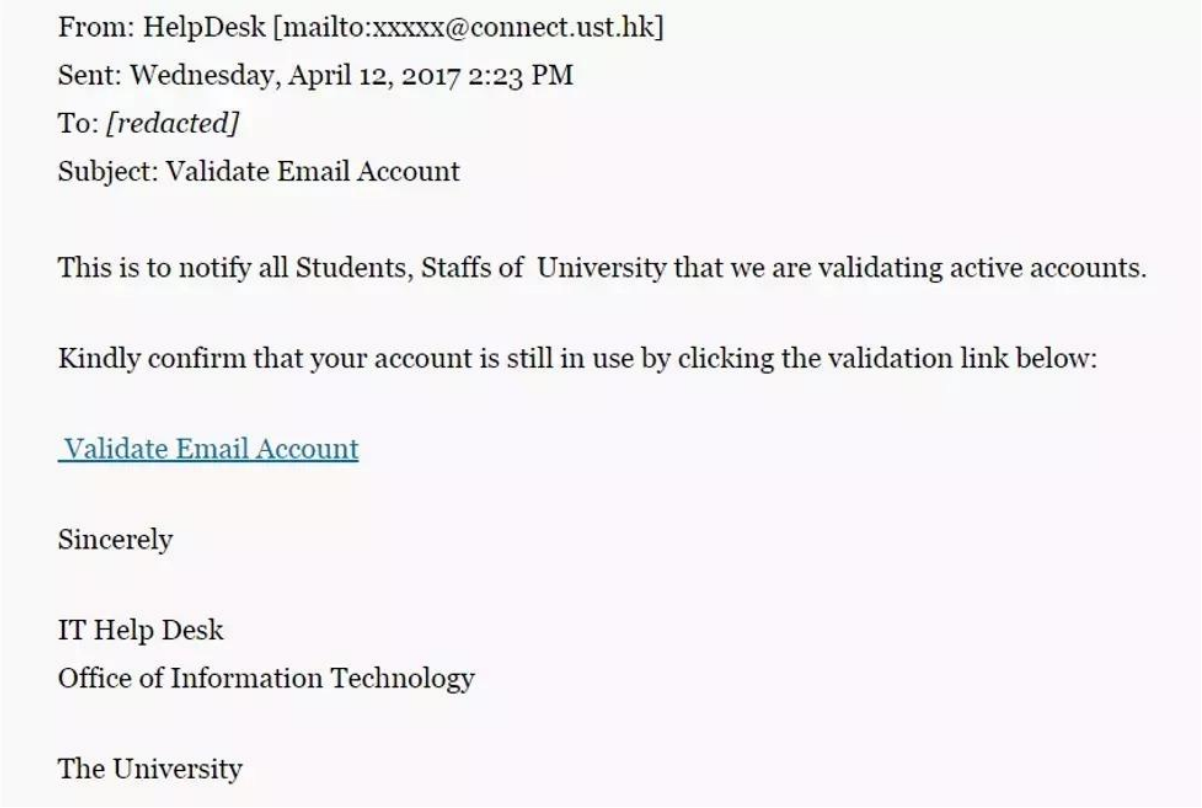
PHISHING TECHNIQUES:

Cyber criminals use three primary phishing techniques to steal information: malicious web links, malicious attachments, and fraudulent data-entry forms. These techniques are designed to exploit human psychology and behavior, making them particularly effective in bypassing traditional security measures.

➢ Malicious Web Links:

Phishing links take users to impostor websites or sites infected with malicious software, known as malware. Malicious links can be disguised as trusted links and are embedded in logos and other images in an email.

Here is an example of an email received by users at Cornell University, displaying "Help Desk" as the sender's name. However, the email did not originate from the university's help desk but from the @connect.ust.hk domain. The link embedded in the email points to a page that mirrors the Office 365 login page, attempting to steal user credentials.



From: HelpDesk [mailto:xxxxx@connect.ust.hk]
Sent: Wednesday, April 12, 2017 2:23 PM
To: *[redacted]*
Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

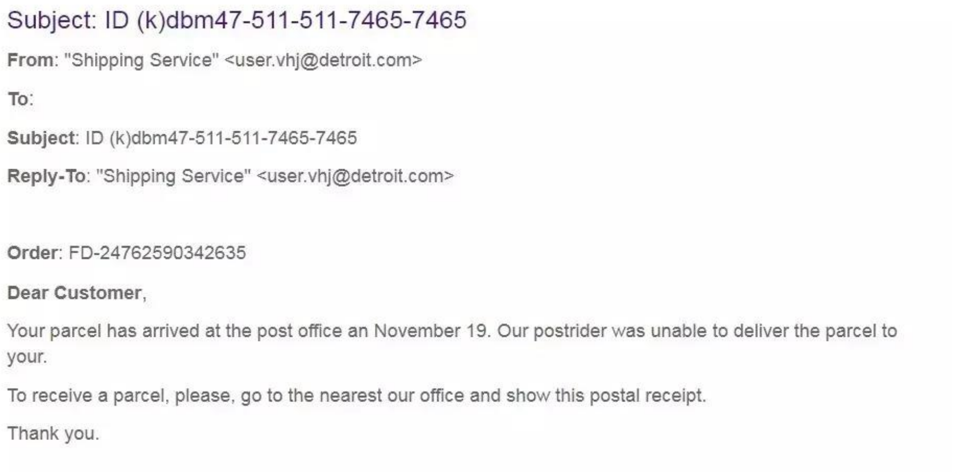
IT Help Desk
Office of Information Technology

The University

FIG 3.4

➢ Malicious Attachments:

While these may look like legitimate file attachments, they are actually infected with malware that can compromise computers and their files.



Subject: ID (k)dbm47-511-511-7465-7465

From: "Shipping Service" <user.vhj@detroit.com>

To:

Subject: ID (k)dbm47-511-511-7465-7465

Reply-To: "Shipping Service" <user.vhj@detroit.com>

Order: FD-24762590342635

Dear Customer,

Your parcel has arrived at the post office an November 19. Our postrider was unable to deliver the parcel to your.

To receive a parcel, please, go to the nearest our office and show this postal receipt.

Thank you.

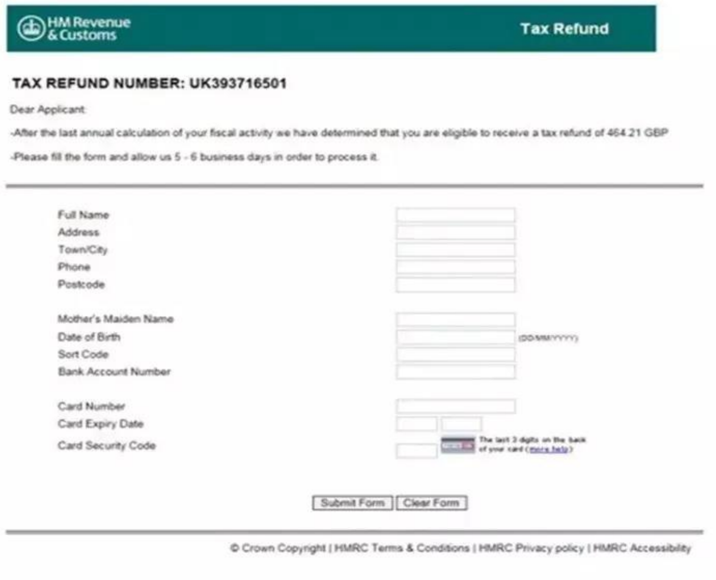
FIG 3.5

Here's an example of a phishing email shared by international shipper FedEx on its website. This email encouraged recipients to print a copy of an attached postal receipt and take it to a FedEx location to get a parcel that could not be delivered. Unfortunately, the attachment contained a virus that infected the recipients' computers.

- **Fraudulent Data Entry Forms:**

These techniques use fake forms that prompt users to fill in sensitive information—such as user IDs, passwords, credit card data, and phone numbers. Cyber criminals use the submitted information for various fraudulent activities, including identity theft.

Here's an example of a fake landing page coping the gov.uk website. After clicking a link in a phishing email, users lead to this fraud page that appears to be part of the HMRC tax collection agency.Users are told the're eligible for a refund but must completed form first.



HM Revenue & Customs — Tax Refund

TAX REFUND NUMBER: UK393716501

Dear Applicant:

-After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 464.21 GBP

-Please fill the form and allow us 5 - 6 business days in order to process it.

Full Name
Address
Town/City
Phone
Postcode

Mother's Maiden Name
Date of Birth (DD/MM/YYYY)
Sort Code
Bank Account Number

Card Number
Card Expiry Date
Card Security Code — The last 3 digits on the back of your card (more help)

Submit Form
Clear Form
© Crown Copyright | HMRC Terms & Conditions | HMRC Privacy policy | HMRC Accessibility

FIG 3.6

TYPES OF PHISHING ATTACKS:

Phishing has evolved into more than simple credential and data theft. An attacker's process depends on the following phishing types:

- **Email phishing:** The general term for any malicious email message meant to trick users into divulging private information. Attackers generally aim to steal account credentials, personally identifiable information (PII), and corporate trade secrets. However, attackers targeting a specific business might have other motives.
- **Spear phishing:** These email messages are sent to specific people within an organization, usually high-privilege account holders, to trick them into divulging sensitive data, sending the attacker money, or downloading malware. This hyper-targeted approach exploits the human tendency to trust communications that appear personalized and relevant.
- **Link manipulation:** Messages contain a link to a malicious site that looks like the official business but takes recipients to an attacker-controlled server where they are persuaded to authenticate into a spoofed login page that sends credentials to an attacker.
- **Content injection:** An attacker who has injected malicious content into an official site tricks users into accessing the site to show them a malicious popup or redirect them to a phishing website.
- **Malware:** A clicked link or opened attachment might download malware onto devices. Ransomware, rootkits, or keyloggers are common malware attachments that steal data and extort payments from targeted victims.
- **Smishing:** Using SMS messages, attackers send a text message to a targeted victim with a malicious link that promises discounts, rewards, or free prizes. This technique exploits the increasing reliance on mobile devices and the quick, often less cautious way people interact with text messages.
- **Vishing:** Attackers use voice-changing software to leave a message telling targeted victims they must call a number where they can be scammed. Attackers also use voice changers when speaking to targeted victims to deceive them.
- **"Evil Twin" Wi-Fi:** Spoofing free Wi-Fi, attackers trick users into connecting to a malicious hotspot to perform man-in-the-middle exploits.
- **Pharming:** Pharming is a two-phase attack used to steal account credentials. The first phase installs malware on a targeted victim and redirects them to a browser and a spoofed website, where they are tricked into divulging credentials. DNS poisoning is also used to redirect users to spoofed domains.
- **Angler phishing:** Attackers reply to social media posts as an official organization to trick users into divulging account credentials and personal information.
- **Watering hole:** An attacker identifies a site numerous targeted users use, exploits a vulnerability, and uses it to trick users into downloading malware. With malware installed on targeted user machines, an attacker can redirect users to spoofed websites or deliver a payload to the local network to steal data.

REAL-WORLD PHISHING EXAMPLES:

- **Twitter Bitcoin Scam (2020):**

In July 2020, hackers gained access to Twitter’s internal tools by spear-phishing employees through phone calls and fake login portals. They compromised high-profile accounts including Elon Musk, Barack Obama, Bill Gates, and Apple, tweeting messages promoting a Bitcoin scam.

Method Used: Spear phishing + social engineering + insider trickery.

Loss: Over $100,000 in Bitcoin stolen within hours

Impact: Global news, exposed how powerful phishing + social engineering can be

- **Sony Pictures Phishing Attack (2014):**

Attackers used fake Apple ID verification emails to trick Sony employees into giving up login credentials. This resulted in one of the most destructive cyberattacks in corporate history.

Data Stolen: Confidential emails, upcoming movie scripts, personal data of employees

Technique Used: Credential harvesting via phishing email

Impact: Estimated $100 million in losses, reputation damage, and global media exposure

- **Anthem Healthcare Phishing Attack (2015):**

Anthem Inc., one of the largest healthcare providers in the U.S., was targeted through a phishing email that allowed attackers access to their database of over 80 million records.

Data Stolen: Names, birthdays, medical IDs, Social Security numbers

Method Used: Spear phishing email opened by a system administrator

Damage: One of the largest healthcare breaches in history

- **US Democratic National Committee (DNC) Hack (2016):**

A phishing email sent to John Podesta, campaign chairman of Hillary Clinton, tricked him into revealing his Gmail password. The attackers then leaked thousands of sensitive emails during the U.S. election campaign.

Technique: Fake Google warning email with a malicious link

Effect: Major political impact and international attention

Lesson: Even senior political figures can fall for phishing attacks

- **AirAsia Employee Credential Leak (2022):**

Cybercriminals used a phishing campaign posing as official HR communication to trick AirAsia employees into giving up their credentials.

Target: Internal HR system login

Result: Employee details and internal documents were leaked on the dark web

Outcome: AirAsia acknowledged the breach and increased awareness training

- **Colonial Pipeline Attack (2021):**

While this attack is known for its ransomware component, initial access was gained via a compromised VPN account — likely due to phishing or password reuse.

Impact: Fuel shortages across the U.S. East Coast

Ransom Paid: $4.4 million in Bitcoin

Takeaway: Phishing can be the entry point to massive infrastructure damage

- **EA Games Hack (2021):**

Phishers targeted Electronic Arts (EA) employees by pretending to be from IT support. They tricked employees into providing login tokens, which were used to gain access to internal Slack channels and source code repositories.

Method Used: Voice phishing + social engineering

Stolen: Source code for FIFA 21 and Frostbite engine

Lesson: Even tech-savvy companies are vulnerable to targeted phishing

- **LinkedIn Job Offer Phishing Scam (2022):**

Attackers sent fake job offer emails on LinkedIn, luring professionals into downloading infected documents disguised as job descriptions.

Method: Phishing via LinkedIn + malicious file

Target: Job seekers, HR managers

Damage: Malware installed, credentials stolen

Takeaway: Spear phishing can exploit hopes and emotions, not just fear

- **Amazon Delivery Scam (2023):**

Cybercriminals sent fake Amazon delivery failure emails with links to "reschedule" a package. Clicking the link led to a fake Amazon login page, harvesting passwords and card details.

Method: Clone phishing + urgency trick

Target: Mobile and email users globally

Takeaway: Phishing often mimics services people use every day

PHISHING PREVENTION:

Preventing phishing attacks requires a combination of user training to recognize the warning signs and robust cybersecurity systems to stop payloads. Email filters are helpful with phishing, but human prevention is still critical.

"Nine times out of 10, attackers and scammers will try to manipulate our emotions. And one of the most common emotional tools that we see in phishing attacks is fear." This psychological manipulation is precisely why technical solutions alone cannot fully address the phishing threat landscape.

A few ways your organization can **prevent** being a **victim of phishing:**

- **Train users to detect a phishing email:** a sense of urgency and requests for personal data, including passwords, embedded links, and attachments, are all warning signs. "Attackers will urge victims to take immediate action, so they don't have time to think, increasing the success rate of their attack,". Users must be able to identify these warning signs to defend against phishing.
- **Avoid clicking links:** instead of clicking a link and authenticating into a web page directly from an embedded link, type the official domain into a browser and authenticate directly from the manually typed site.
- **Use anti-phishing email security:** artificial intelligence scans incoming messages, detects suspicious messages, and quarantines them without allowing phishing messages to reach the recipient's inbox. Advanced email security solutions detect and block an average of 66 million business email compromise (BEC) attacks per month.
- **Change passwords regularly:** users should be forced to change their passwords every 30-45 days to reduce an attacker's window of opportunity. Based on Proofpoint's 2024 State of Phish report, reusing or sharing passwords ranks highest as the most risky behavior.
- **Update software and firmware:** software and firmware developers release updates to remediate bugs and security issues. Always install these updates to ensure known vulnerabilities are no longer in your infrastructure. This practice helps close potential entry points that phishing campaigns often exploit.
- **Install firewalls:** firewalls control inbound and outbound traffic. Malware installed from phishing silently eavesdrops and sends private data to an attacker, but a firewall blocks malicious outgoing requests and logs them for further review.
- **Avoid clicking on popups:** attackers change the location of the X button on a popup window to trick users into opening a malicious site or downloading malware. Popup

blockers stop many popups, but false negatives are still possible. Teaching users to recognize these manipulation tactics is essential to building security awareness.

- **Be cautious about disclosing credit card data:** unless you know the site is entirely trustworthy, never give credit card data to a website you don't recognize. Any site promising gifts or money should be used with caution. This vigilance should extend to QR codes and other emerging phishing vectors

Technology is pivotal in preventing phishing attacks, but awareness is equally vital. "Since people are the primary target of these evolving phishing attacks, you want to empower them with the right knowledge and tools to protect themselves and your organization," Pan highlights.

PHISHING PROTECTION:

Phishing protection is the security measures organizations can take to mitigate phishing attacks on their employees and systems. Security awareness training and education through real-world examples and exercises help users identify phishing. Organizations often work with experts who send simulated phishing emails to employees and track who opened the email and clicked the link.

Some email gateway solutions can catch and classify phishing emails based on the known bad reputation of the embedded URLs. However, these solutions are not always reliable in detecting well-crafted phishing messages from compromised legitimate websites.

The most effective systems identify suspicious emails based on unusual traffic patterns, rewrite the embedded URL, and monitor the URL for in-page exploits and downloads. Monitoring tools quarantine suspicious email messages so administrators can research ongoing phishing attacks. If a high number of phishing emails are detected, administrators can alert employees and reduce the chance of a successful targeted phishing campaign.

Another critical line of defense is user-based awareness training on the latest phishing and social engineering techniques to reduce the risk of breaches and generate a culture of cybersecurity.

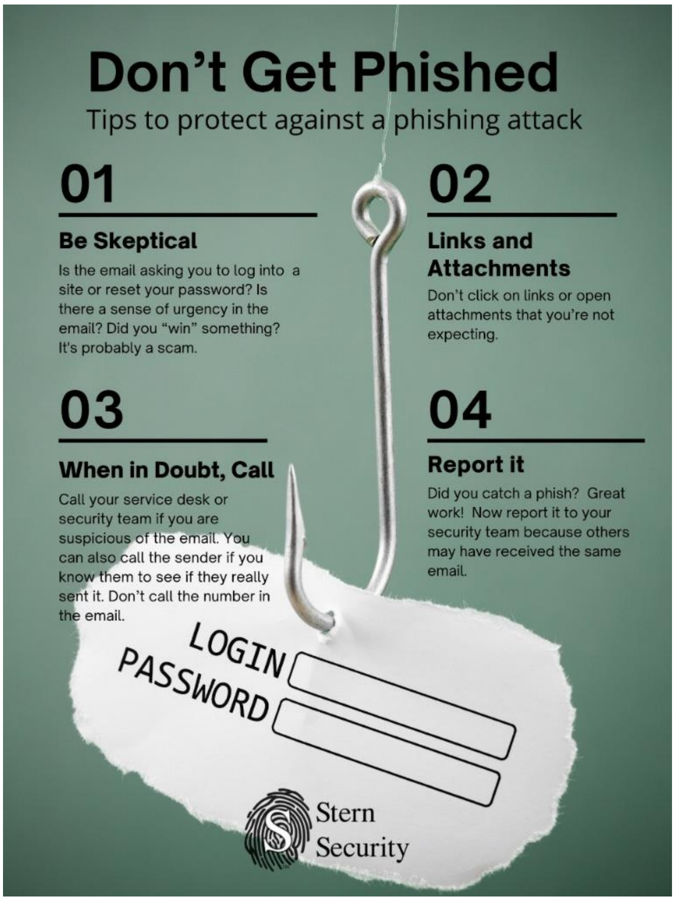
➢ PROTECT YOURSELF:

- **Be cautious of unsolicited emails and messages:** Don't click on links or open attachments from unknown senders.
- **Verify website legitimacy:** Carefully examine URLs for misspellings or unusual characters before entering any information.
- **Use strong passwords and multi-factor authentication:** This adds an extra layer of security beyond just a password.
- **Use security software:** Install reputable antivirus and anti-phishing software.
- **Be aware of social engineering tactics:** Understand how attackers manipulate users to gain their trust.
- **Report suspicious messages:** Report phishing attempts to your email provider or relevant authorities.

- **Double-check everything:** Before providing any information, verify the sender and the legitimacy of the request.
- **Be wary of urgent or alarming messages:** Phishing attempts often create a sense of urgency or fear to pressure users into acting quickly.

➢ PHISHING PROTECTION FOR ORGANIZATIONS:

- **Employee training:**Educate employees about phishing techniques and best practices for recognizing and reporting attacks.
- **Simulated phishing attacks:**Conduct regular simulated phishing campaigns to test employee awareness and identify areas for improvement.
- **Email filtering and security solutions:**Implement robust email filtering and security solutions to detect and block phishing emails.
- **Multi-factor authentication:**Enforce MFA for all critical systems and applications to add an extra layer of security.
- **Endpoint protection:**Install security software on all devices to detect and prevent malware infections.
- **Data backup and recovery:**Implement regular data backups to minimize the impact of successful attacks.



Don’t Get Phished

Tips to protect against a phishing attack

01

Be Skeptical

Is the email asking you to log into a site or reset your password? Is there a sense of urgency in the email? Did you “win” something? It's probably a scam.

02

Links and Attachments

Don’t click on links or open attachments that you’re not expecting.

03

When in Doubt, Call

Call your service desk or security team if you are suspicious of the email. You can also call the sender if you know them to see if they really sent it. Don’t call the number in the email.

04

Report it

Did you catch a phish? Great work! Now report it to your security team because others may have received the same email.

FIG 3.7

What to Do If You’ve Fallen Victim?

Once an attacker has accessed your information to an attacker, they will likely disclose it to other scammers. You may receive vishing and smishing messages, new phishing emails, and voice calls. Always be alert for suspicious messages asking for your information or financial details.

If you respond to a phishing email, “you’ll need to act quickly to mitigate the damage,” emphasizes Cybersecurity Analyst Dave Cook. In this post, he outlines steps to take if you’ve responded to a phishing email (condensed below):

- **Change passwords:** Immediately update passwords and ensure they are complex and unique.
- **Report incident:** Promptly inform the IT department or email provider about the phishing email.
- **Enable MFA:** Implement multifactor authentication for an extra layer of security.
- **Monitor accounts:** Scan devices for malware and check for any suspicious activity.
- **Contact affected organization:** Alert the company impersonated in the phishing attempt.
- **Educate yourself:** Learn about phishing tactics and how to identify suspicious emails.

At the company-wide level, Cook suggests that organizations “establish clear guidelines so that users know exactly what to do if they fall prey to a phishing scam. These guidelines should include changing passwords, notifying IT, enabling 2FA, checking for malware, and remaining vigilant in the future.”

The Federal Trade Commission has a website dedicated to identity theft to help you mitigate damages and monitor your credit score. To detect and remove the malware, ensure your antivirus software is up-to-date and has the latest patches installed.

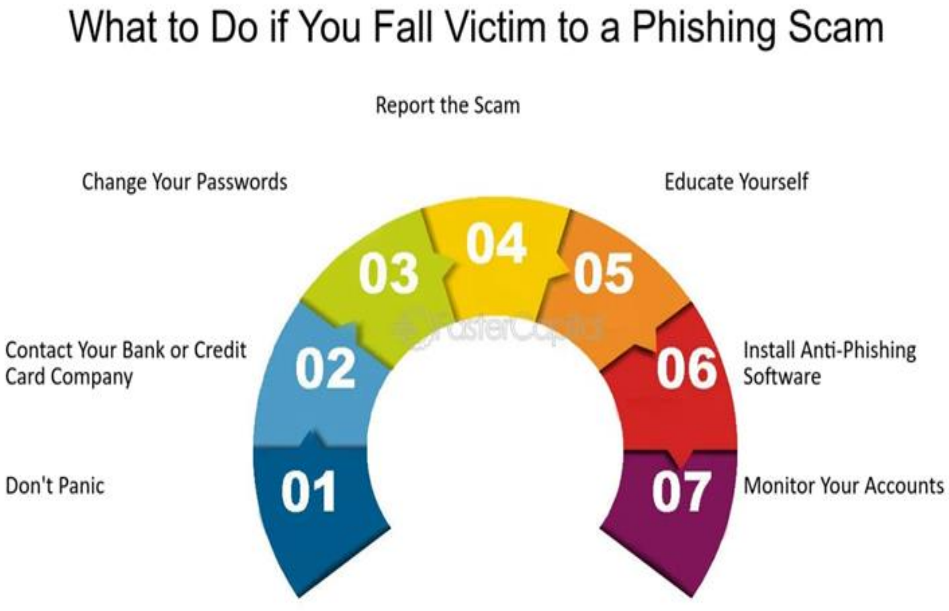

What to Do if You Fall Victim to a Phishing Scam
Report the Scam
Change Your Passwords
Educate Yourself
Contact Your Bank or Credit Card Company
Install Anti-Phishing Software
Don't Panic
Monitor Your Accounts
01
02
03
04
05
06
07

FIG 3.8

4) PHISHING TOOLS

What is a Phishing Tool?

A phishing tool is a software or script used to create fake login pages or emails that look like real ones. These tools are often used to trick people into entering sensitive information like usernames, passwords, or bank details. In cybersecurity, phishing tools are used legally for training and testing purposes to help people understand how such attacks happen and how to protect against them.

❖ ZPHISHER TOOL

What is Zphisher?

Zphisher is a powerful and easy-to-use phishing automation tool written in Bash shell script, designed for penetration testing, ethical hacking, and cybersecurity awareness training. It simulates real-world phishing attacks by replicating popular website login pages and capturing credentials in a controlled lab environment.

This tool is especially popular among students, ethical hackers, and cybersecurity trainers because it:

- Doesn't require deep coding knowledge
- Runs entirely on Kali Linux, Parrot OS, or Termux
- Uses tunneling services like Ngrok and Cloudflare to make phishing pages accessible over the internet

Use Case: Zphisher is ideal for ethical demonstrations of phishing attacks — such as in workshops, cyber awareness campaigns, or lab assignments in college.

How Zphisher Works?

Zphisher follows a simple yet realistic phishing workflow:

1. User selects a fake login page (e.g., Facebook, Instagram, Gmail, etc.)
2. Zphisher clones that page and hosts it locally using PHP
3. It then uses tunneling tools to create a publicly accessible link
4. When a victim visits that link and submits credentials, those details are:
    - Logged in the terminal
    - Stored in a text file for later analysis

This helps simulate how a real-world attacker could trick users into revealing sensitive information — without actually harming anyone.

➢ Features of Zphisher :

Here are the key features of Zphisher that make it a widely used phishing toolkits

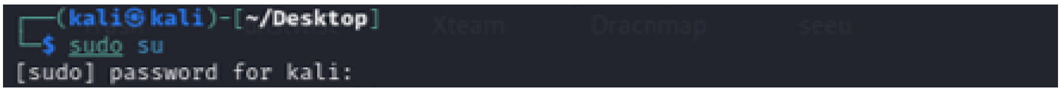
Features and description:

- **40+ Website Templates:** Facebook, Instagram, Twitter, GitHub, Netflix, etc
- **Tunneling Options**: Supports Ngrok, Cloudflared, Localhos
- t**URL Masking:** Masks long URLs to appear more legitimate
- **Auto-updates:** Automatically fetches latest login pages
- **Beginner-friendly:** Simple CLI interface — just follow the prompts
- **Lightweight:** No heavy dependencies; works on most Linux systems
- **Credential Logging:** Stores captured data in readable log files

➢ Installation and Setup in Kali Linux:

#STEP 1: i. Login to kali:

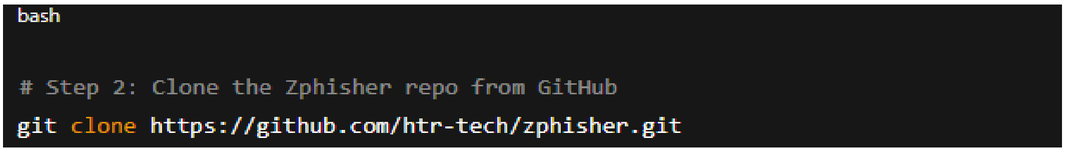
ii.Login to super user by sudo su command:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
```

FIG 4.1

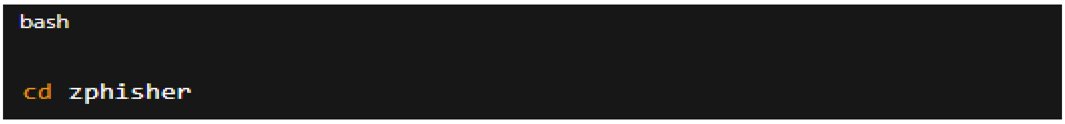
#STEP 2: Clone Zphisher Repository:



```
bash

# Step 2: Clone the Zphisher repo from GitHub
git clone https://github.com/htr-tech/zphisher.git
```

FIG 4.2

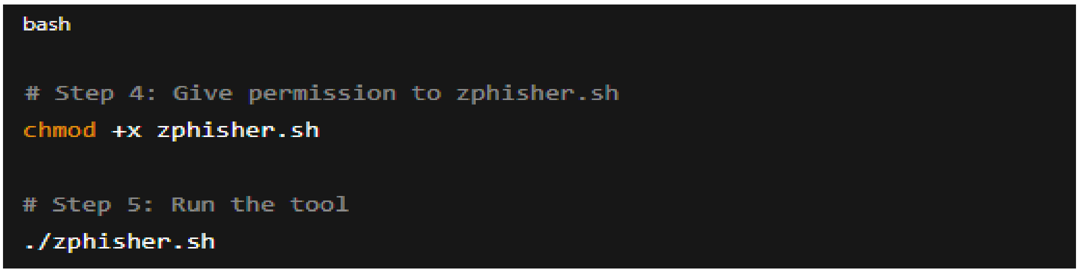
#STEP 3: Navigate to Directory:



```
bash

cd zphisher
```

FIG 4.3

#STEP 4: Give Permissions and Run:

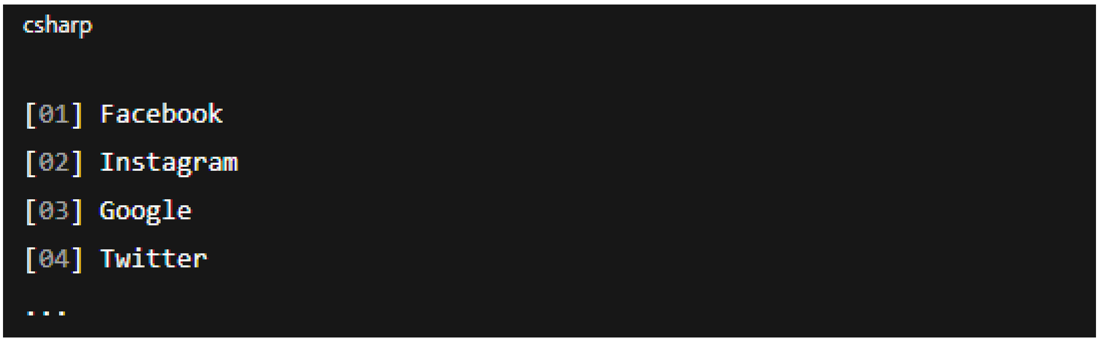


```
bash

# Step 4: Give permission to zphisher.sh
chmod +x zphisher.sh

# Step 5: Run the tool
./zphisher.sh
```

FIG 4.4

➢ Choose a Phishing Template:

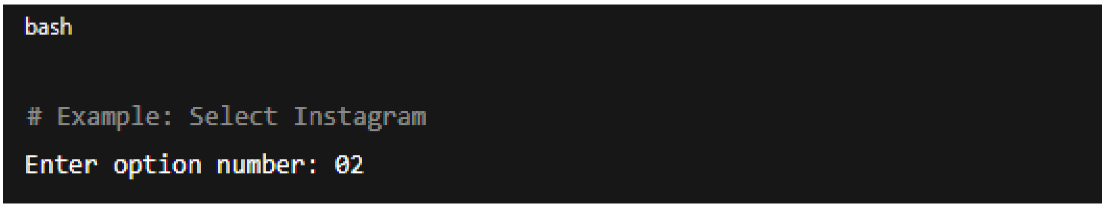
You'll see options like:



```
csharp

[01] Facebook
[02] Instagram
[03] Google
[04] Twitter
...
```

FIG 4.5

Example Selection:

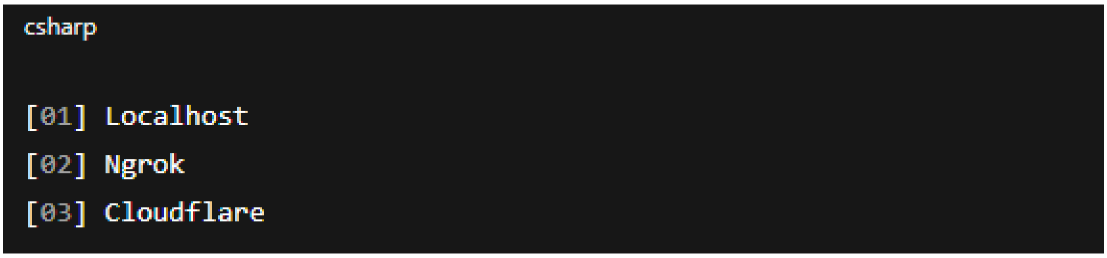


```
bash

# Example: Select Instagram
Enter option number: 02
```

FIG 4.6

➢ Select Tunneling Service:

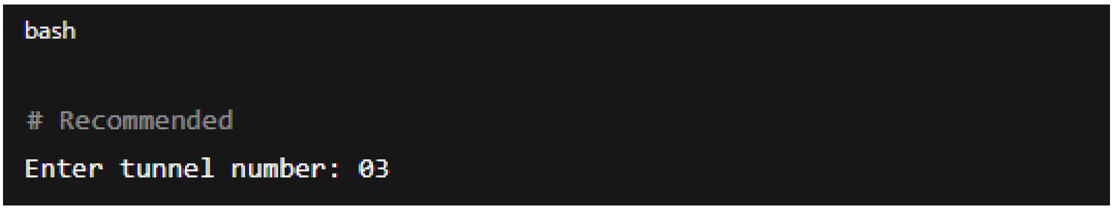
Zphisher will ask:



```
csharp

[01] Localhost
[02] Ngrok
[03] Cloudflare
```

FIG 4.7

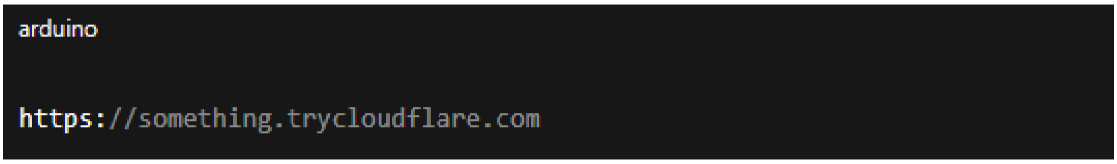
Choose Cloudflare:



```
bash

# Recommended
Enter tunnel number: 03
```

FIG 4.8

It now generates a public Cloudflare URL, e.g.:



```arduino
https://something.trycloudflare.com
```

FIG 4.9

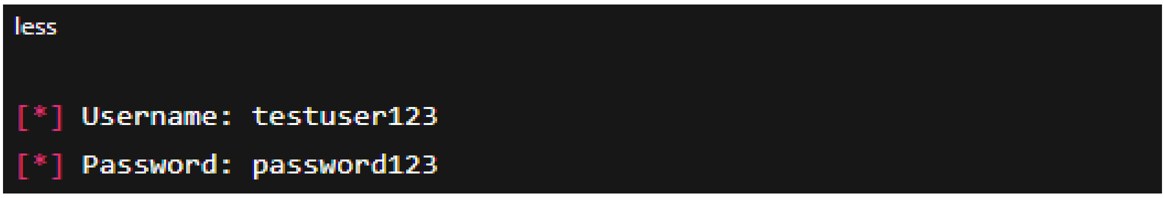
- **Victim Interaction:**

You copy the Cloudflare link and open it in a browser (locally or on another machine).

Instagram Login Page (Phishing):

Looks exactly like the real Instagram login.

When credentials are entered → you see them in terminal:



```less
[*] Username: testuser123
[*] Password: password123
```

FIG 4.10

This part:

- Launches a Cloudflare tunnel
- Binds it to localhost where your fake page is running

- **How to Defend Against Phishing Attacks ?**

To protect yourself and others from phishing attacks like the ones demonstrated with Zphisher, follow these best practices:

- **Enable MFA:**Even if someone steals your password, they can’t log in without your second factor (like a phone OTP)
- **Check URLs:** Always verify if the URL is real (e.g., instagram.com not 1nstagram.net)
- **User Awareness:**Training people to spot fake emails and pages is the most powerful defense
- **Use Password Managers:**They autofill only on real domains, preventing fake login submissions
- **Anti-Phishing Tools:**Use browser plugins or endpoint tools that block known phishing URLs

❖ NEXPHISHER TOOL

➢ What is NexPhisher?

Nexphisher is a fully automated phishing toolkit designed to generate fake login pages for a variety of popular websites. It is particularly known for its simplicity, minimal setup, and compatibility with Android devices via the Termux app. Nexphisher enables even beginners with basic command-line knowledge to launch phishing attacks by providing them with pre-built templates and built-in tunneling services such as Ngrok, Cloudflare Tunnel, and Localhost.run.

The tool's main purpose is to replicate real login pages of well-known platforms like Instagram, Gmail, Snapchat, Netflix, and many others. Once a fake page is created, the attacker shares the link with the target through email, SMS, or social media. When the victim enters their login details, those credentials are instantly sent to the attacker in real time.

Although Nexphisher is marketed as a tool for ethical hacking and awareness training, it is frequently misused to gain unauthorized access to users' accounts. Its versatility, combined with its mobile accessibility and automation features, has made it one of the most widely used phishing tools by both amateur and professional attackers.

➢ How Nexphisher Works?

- Nexphisher automatically clones login pages of popular websites like Instagram, Snapchat, Netflix, and Google.
- The attacker installs the tool in Termux and selects the target website for which a phishing page is to be generated.
- The tool then uses a tunneling service (like Ngrok or Cloudflare) to host the page online and generate a public link.
- This link is sent to the target through social engineering—via email, DMs, or other means.
- When the victim opens the link and enters their login credentials, the information is displayed live in the attacker's terminal.
- At the same time, the tool captures additional information such as the victim's IP address, browser, device details, and whether a VPN is being used.

➢ Features of Nexphisher:

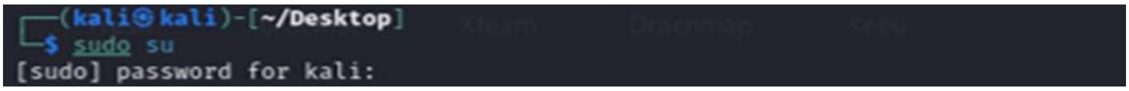
- Nexphisher includes over 30 pre-built phishing templates including Instagram, PayPal, Twitter, ProtonMail, Spotify, and more.
- It supports multiple tunneling methods like Ngrok, Localhost.run, and Cloudflare.
- Real-time credential capturing allows attackers to monitor victim activity instantly.
- It is lightweight and runs smoothly on Termux without needing root access.
- It can detect the user agent, IP address, geographic location, and VPN usage.

- Fully automated and user-friendly, with no need for programming knowledge.
- The tool is actively maintained and updated through GitHub repositories.

➢ Installation & Setup in Kali Linux:

#STEP 1: i. Login to kali:

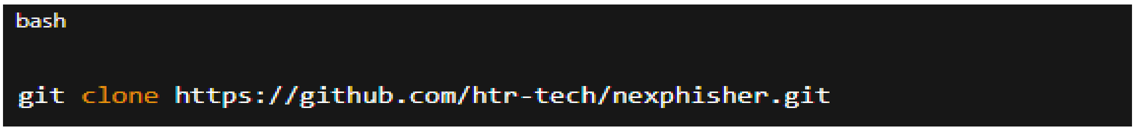
ii.Login to super user by sudo su command:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
```

FIG 4.11

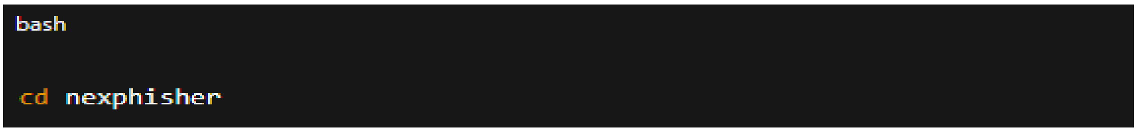
#STEP 2: Clone the Tool:



```
bash

git clone https://github.com/htr-tech/nexphisher.git
```

FIG 4.12

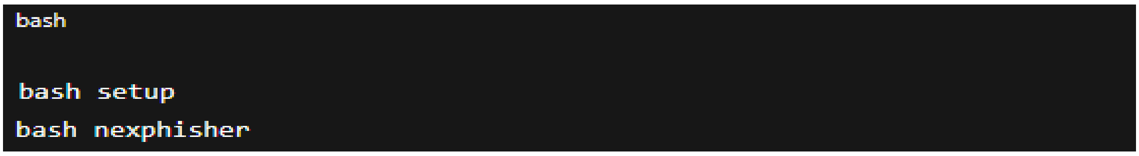
#STEP 3: Enter Directory:



```
bash

cd nexphisher
```

FIG 4.13

#STEP 4: Setup and Run:

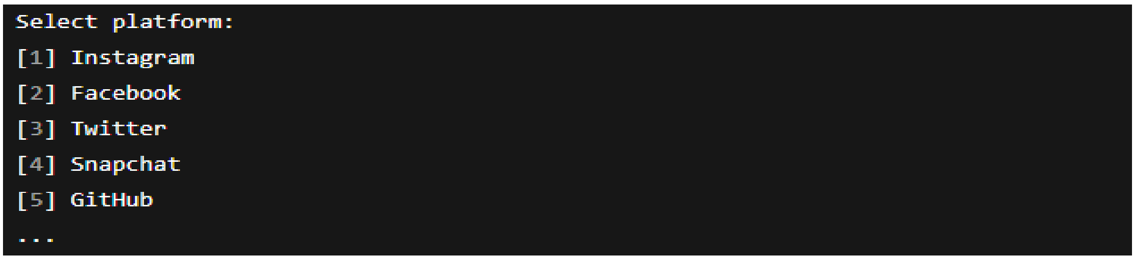


```
bash

bash setup
bash nexphisher
```

FIG 4.14

➢ Choose a Phishing Template:

The interface provides this list:

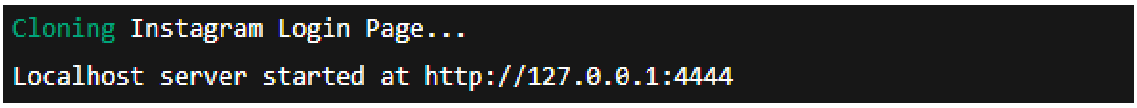


```
Select platform:
[1] Instagram
[2] Facebook
[3] Twitter
[4] Snapchat
[5] GitHub
...
```

FIG 4.15

Example Selection:

Choose option 1 for Instagram.

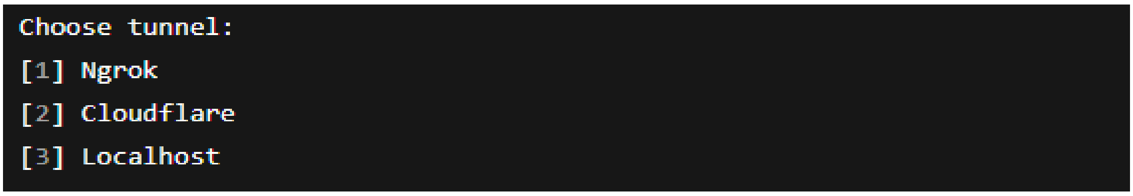


```
Cloning Instagram Login Page...
Localhost server started at http://127.0.0.1:4444
```

FIG 4.16

➢ Select Tunneling Service:

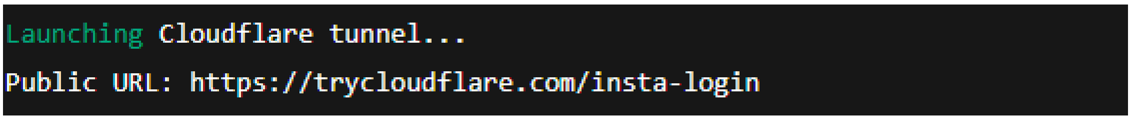
NexPhisher prompts:



```
Choose tunnel:
[1] Ngrok
[2] Cloudflare
[3] Localhost
```

FIG 4.17

Choose Cloudflare:



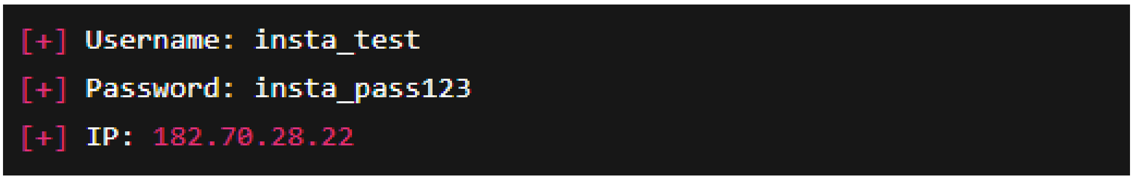
```
Launching Cloudflare tunnel...
Public URL: https://trycloudflare.com/insta-login
```

FIG 4.18

➢ Victim Interaction:

You send the Cloudflare link to the victim. The Instagram login looks real.

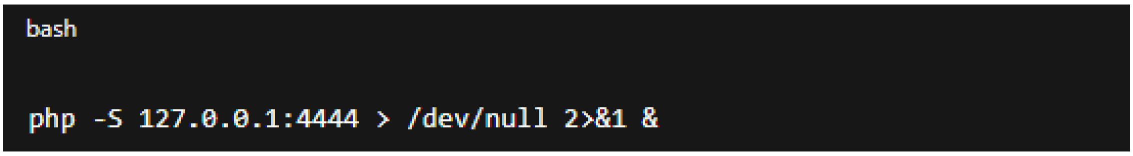
When credentials are submitted:



```
[+] Username: insta_test
[+] Password: insta_pass123
[+] IP: 182.70.28.22
```

FIG 4.19

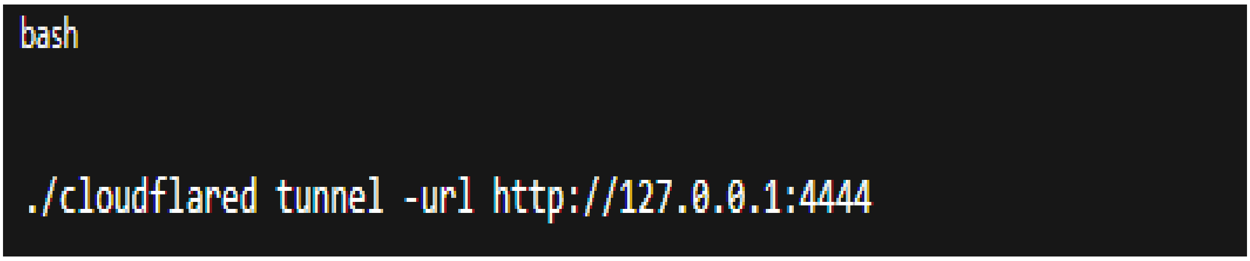
➢ Code Explanation (Bash):



```bash
php -S 127.0.0.1:4444 > /dev/null 2>&1 &
```

FIG 4.20

- Hosts the phishing page locally using PHP.



```
bash

./cloudflared tunnel -url http://127.0.0.1:4444
```

FIG 4.21

Launches public tunnel via Cloudflare.

➢ How to Defend Against Becoming a Victim?

- The most important defense is cyber awareness. People should be educated about how phishing pages appear and how to identify fake websites.
- Always log in through official apps or manually typed URLs—never click on suspicious links.
- Avoid opening unknown or suspicious messages, especially those that contain login links or ask for credentials.
- Enable Two-Factor Authentication (2FA) on all accounts to add a layer of security.
- Use browser security plugins that can detect and block phishing attempts.
- Regularly update your device and browser software to stay protected from known vulnerabilities.
- Use email spam filters to catch potential phishing emails.
- Always log out of accounts when using public or shared devices.32A

❖ Slash TOOL

➢ What is Slash Tool?

Slash is an **OSINT (Open-Source Intelligence) and Reconnaissance tool**.
It is used to **collect publicly available information** from the internet about:

- **Usernames**
- **Emails**
- **Phone numbers**
- **Domains**
- **Social Media Accounts**

It automatically checks many websites and online platforms to see where that username, email, or phone number exists.

🔍 What Slash Tool Can Do

Slash helps you:

✔ Check if a username exists on multiple websites

Example: Instagram, GitHub, Facebook, Twitter, etc.

✔ Find information about an email address

Such as validity, leaks, or online accounts.

✔ Get info about a phone number

For country, carrier, format, etc.

✔ Gather details about a domain

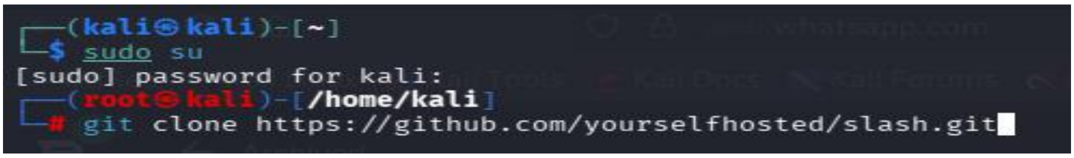
Like WHOIS, DNS records, and website info.

🛠 Why Slash Is Used

- For cyber security reconnaissance
- For OSINT investigations
- For bug bounty initial research
- For gathering digital footprint
- For quick and automated information-gathering

➢ Installation & Setup:

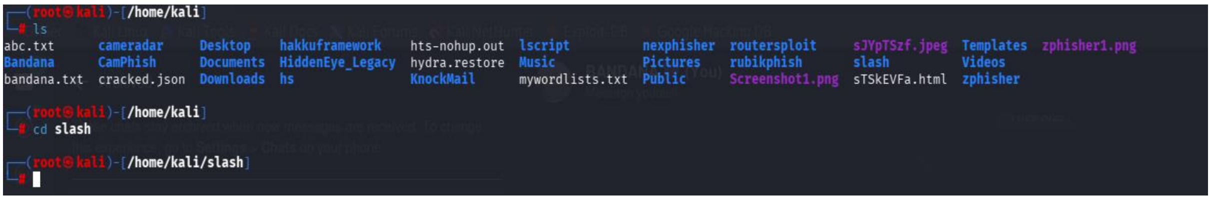
#STEP 1: Clone a Tool (Infer Example) :



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/yourselfhosted/slash.git
```

FIG 4.22

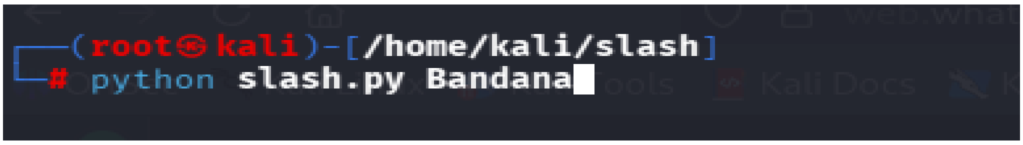
#STEP 2:Go to Slash Directroy :



```
┌──(root㉿kali)-[/home/kali]
└─# ls
abc.txt     cameradar     Desktop    hakkuframework    hts-nohup.out  lscript          nexphisher  routersploit     sJYpTSzf.jpeg  Templates  zphisher1.png
Bandana     CamPhish      Documents  HiddenEye_Legacy  hydra.restore  Music            Pictures    rubikphish       slash          Videos
bandana.txt cracked.json  Downloads  hs                KnockMail      mywordlists.txt  Public      Screenshot1.png  sTSkEVFa.html  zphisher

┌──(root㉿kali)-[/home/kali]
└─# cd slash

┌──(root㉿kali)-[/home/kali/slash]
└─#
```

FIG 4.23

#STEP 3: Setup and Run:

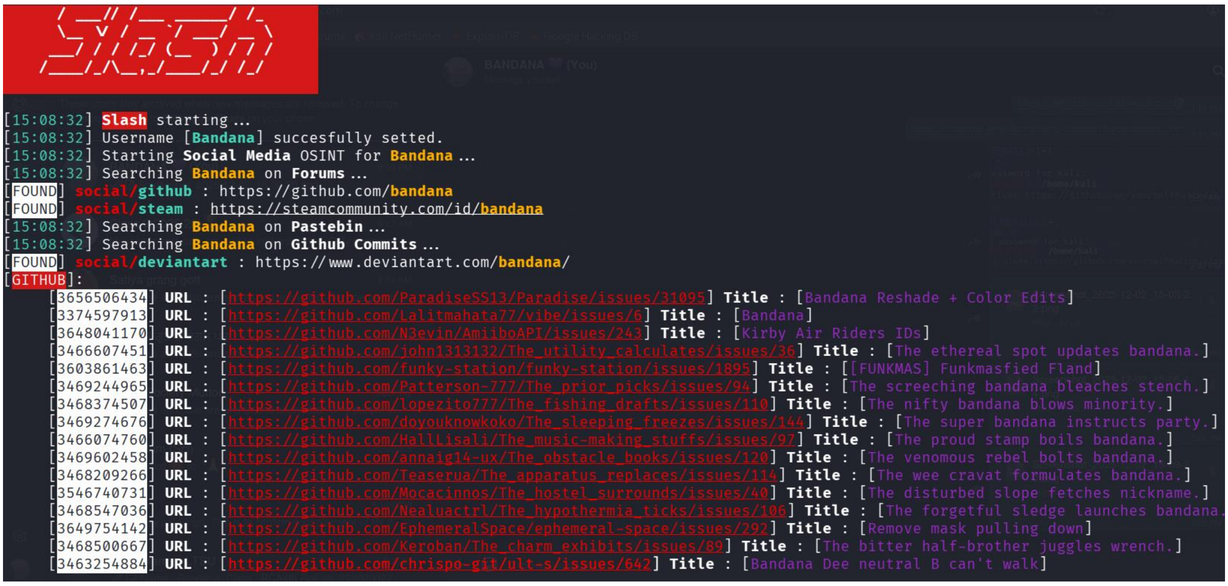


```
┌──(root㉿kali)-[/home/kali/slash]
└─# python slash.py Bandana
```

FIG 4.24

➢ Running Process :

The interface provides this list:



```
[15:08:32] Slash starting ...
[15:08:32] Username [Bandana] succesfully setted.
[15:08:32] Starting Social Media OSINT for Bandana ...
[15:08:32] Searching Bandana on Forums ...
[FOUND] social/github : https://github.com/bandana
[FOUND] social/steam : https://steamcommunity.com/id/bandana
[15:08:32] Searching Bandana on Pastebin ...
[15:08:32] Searching Bandana on Github Commits ...
[FOUND] social/deviantart : https://www.deviantart.com/bandana/
[GITHUB]:
     [3656506434] URL : [https://github.com/ParadiseSS13/Paradise/issues/31095] Title : [Bandana Reshade + Color Edits]
     [3374597913] URL : [https://github.com/Lalitmahata77/vibe/issues/6] Title : [Bandana]
     [3648041170] URL : [https://github.com/N3evin/AmiiboAPI/issues/243] Title : [Kirby Air Riders IDs]
     [3466607451] URL : [https://github.com/john1313132/The_utility_calculates/issues/36] Title : [The ethereal spot updates bandana.]
     [3603861463] URL : [https://github.com/funky-station/funky-station/issues/1895] Title : [[FUNKMAS] Funkmasfied Fland]
     [3469244965] URL : [https://github.com/Patterson-777/The_prior_picks/issues/94] Title : [The screeching bandana bleaches stench.]
     [3468374507] URL : [https://github.com/lopezito777/The_fishing_drafts/issues/110] Title : [The nifty bandana blows minority.]
     [3469274676] URL : [https://github.com/doyouknowkoko/The_sleeping_freezes/issues/144] Title : [The super bandana instructs party.]
     [3466074760] URL : [https://github.com/HallLisali/The_music-making_stuffs/issues/97] Title : [The proud stamp boils bandana.]
     [3469602458] URL : [https://github.com/annaig14-ux/The_obstacle_books/issues/120] Title : [The venomous rebel bolts bandana.]
     [3468209266] URL : [https://github.com/Teaserua/The_apparatus_replaces/issues/114] Title : [The wee cravat formulates bandana.]
     [3546740731] URL : [https://github.com/Mocacinnos/The_hostel_surrounds/issues/40] Title : [The disturbed slope fetches nickname.]
     [3468547036] URL : [https://github.com/Nealuactrl/The_hypothermia_ticks/issues/106] Title : [The forgetful sledge launches bandana.
     [3649754142] URL : [https://github.com/EphemeralSpace/ephemeral-space/issues/292] Title : [Remove mask pulling down]
     [3468500667] URL : [https://github.com/Keroban/The_charm_exhibits/issues/89] Title : [The bitter half-brother juggles wrench.]
     [3463254884] URL : [https://github.com/chrispo-git/ult-s/issues/642] Title : [Bandana Dee neutral B can't walk]
```

FIG 4.25

CONCLUSION

Social engineering is not just a cyberattack; it is a psychological strategy that targets the most vulnerable component of any security system – the human mind. Unlike traditional hacking techniques that depend on breaking technical barriers, social engineering manipulates emotions such as trust, fear, curiosity, and urgency to gain access to confidential data. This makes it one of the most powerful, effective, and dangerous forms of cybercrime, as even the strongest technical security can fail when human awareness is weak.

In this report, we examined social engineering in detail, beginning with what it is, how it works, and why it poses such a serious threat to individuals and organizations worldwide. We analyzed the stages of social engineering attacks, which include research, building trust, exploitation, and execution. Furthermore, we explored various types of attacks such as phishing, spear phishing, vishing, and smishing, which clearly demonstrate how attackers use different communication channels to trick victims.

A major section of this report focused on phishing, the most common and successful social engineering attack. We discussed what phishing is, how it works, various techniques used by attackers, real-world phishing examples, and the devastating consequences of falling victim to such attacks. Additionally, we examined preventive measures and steps to take if someone becomes a victim, highlighting the importance of vigilance in reducing risks.

To provide practical insights, we also studied commonly used phishing tools, such as Zphisher, Nexphisher, and Slash -based tools. These tools allow attackers to create fake login pages, clone websites, and steal sensitive data with ease, proving how quickly and easily phishing attacks can be executed today and slash tool used for information gathering . This section demonstrated that cybercriminals no longer need advanced programming knowledge to launch sophisticated attacks, which further emphasizes the importance of awareness and prevention.

The biggest lesson from this study is that no cybersecurity solution is perfect if the human factor is ignored. Firewalls, antivirus software, and advanced encryption can provide strong technical protection, but they cannot prevent a user from unknowingly sharing personal information or clicking on a malicious link. This is why awareness, education, and alertness remain the most effective defenses against social engineering attacks. Every user must think twice before trusting online sources, sharing confidential data, or responding to suspicious messages.

In conclusion, social engineering will continue to evolve with new tools and advanced psychological tricks, making it an ever-present threat in the digital world. To fight this, our defenses must also evolve. A strong combination of advanced security technologies and well-informed, cautious users is the key to cybersecurity success. Remember, in the fight against cybercrime, human awareness is both the first line of defense and the last hope of protection. Staying alert, adopting safe practices, and educating others can help create a safer digital environment for everyone.