



Ethical Hacking Essentials (EHE)

Master of Science in Cybersecurity

1



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

ETHICAL HACKING

ETHICAL HACKING

Module 05

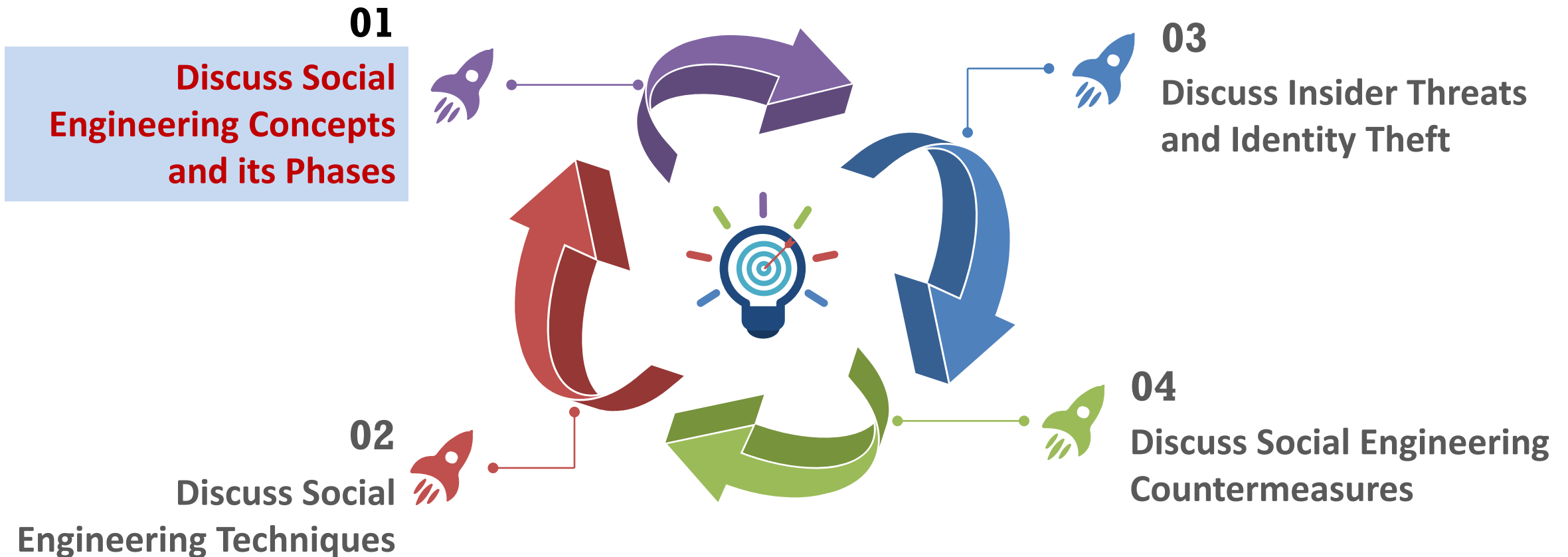
Social Engineering Techniques and Countermeasures



Module Objectives

- 1 Understanding Social Engineering Concepts
- 2 Understanding Various Social Engineering Techniques
- 3 Understanding Insider Threats
- 4 Understanding Identity Theft
- 5 Understanding Different Social Engineering Countermeasures
- 6 Understanding Different Insider Threats and Identity Theft Countermeasures

Module Flow



What is Social Engineering?



- ❑ Social engineering is the art of **convincing people** to **reveal confidential information**

- ❑ Social engineers depend on the fact that **people are unaware** of the valuable information to which they have access and are careless about protecting it

Common Targets of Social Engineering



- 1 Receptionists and Help-Desk Personnel
- 2 Technical Support Executives
- 3 System Administrators
- 4 Users and Clients
- 5 Vendors of the Target Organization
- 6 Senior Executives

Impact of Social Engineering Attack on an Organization

1

Economic losses

2

Damage of goodwill

3

Loss of privacy

4

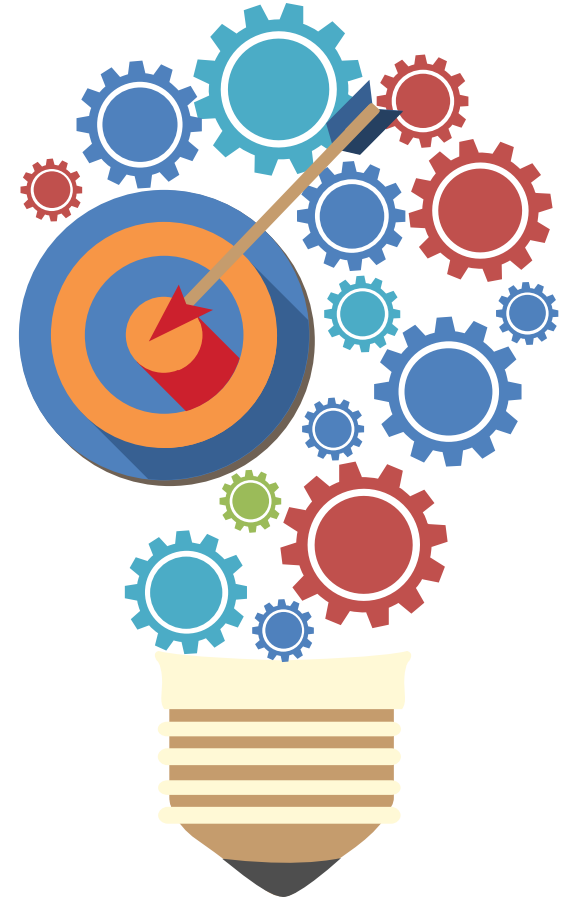
Dangers of terrorism

5

Lawsuits and arbitration

6

Temporary or permanent closure



Behaviors Vulnerable to Attacks

Authority



Intimidation



Consensus or Social Proof



Scarcity



Urgency



Familiarity or Liking

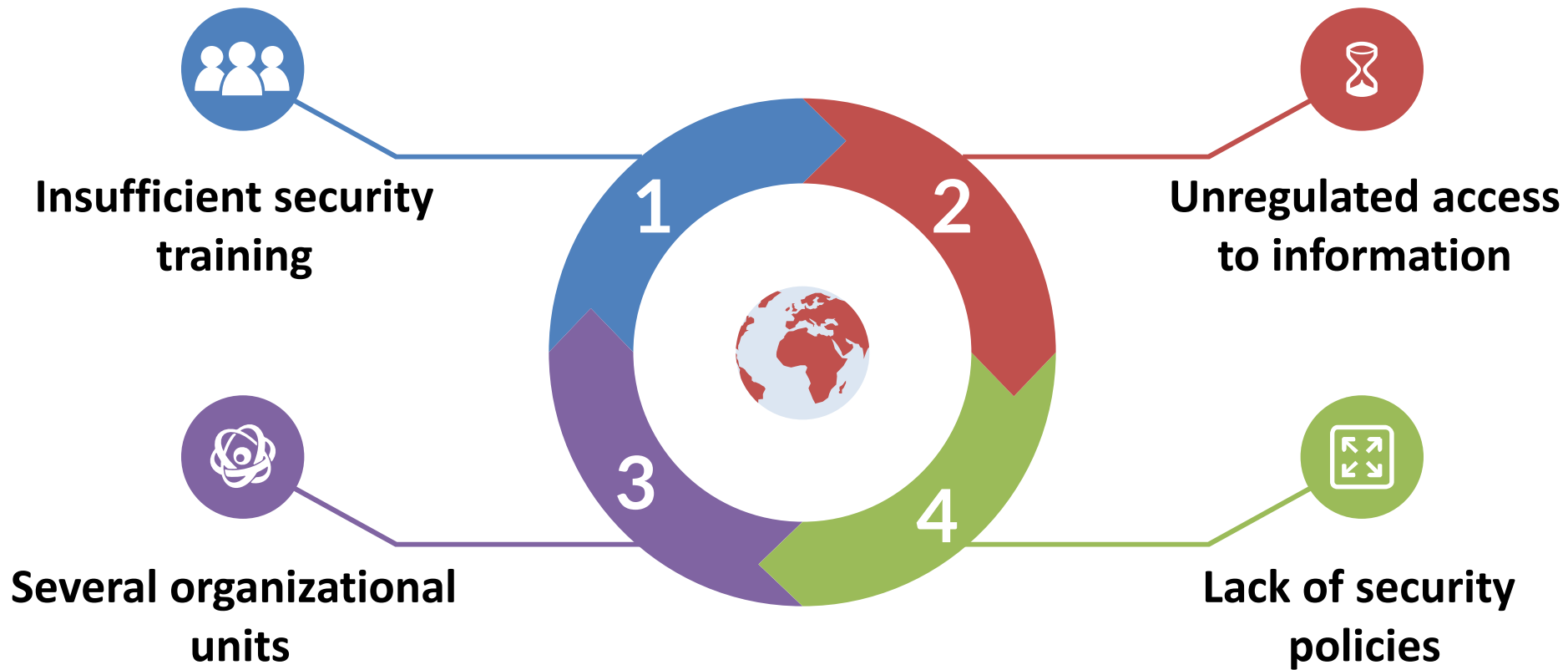


Trust



Greed

Factors that Make Companies Vulnerable to Attacks



Why is Social Engineering Effective?

- ❑ Social engineering does not deal with network security issues; instead, it deals with the **psychological manipulation** of a human being to extract desired information

01

Security policies are as strong as their weakest link, and **human behavior** is the most **susceptible factor**



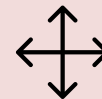
02

It is **difficult to detect** social engineering attempts



03

There is **no method that can be applied to ensure complete security** from social engineering attacks



04

There is **no specific software or hardware** to defend against a social engineering attack



Phases of a Social Engineering Attack



Research the Target Company



Dumpster diving, websites, employees, tour of the company, etc.

Select a Target



Identify frustrated employees of the target company

Develop a Relationship



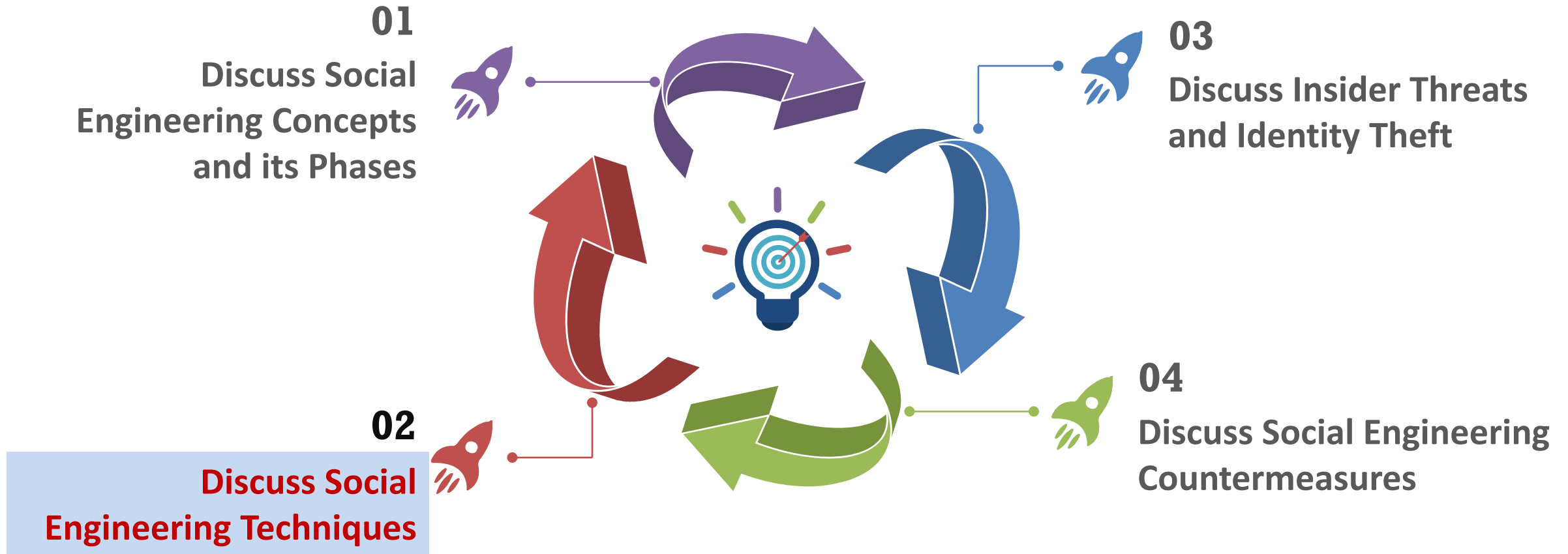
Develop a relationship with the selected employees

Exploit the Relationship



Collect sensitive account and financial information, as well as current technologies

Module Flow



Types of Social Engineering



Human-based Social Engineering

- ❑ “Sensitive information is gathered **by interaction**”.
- ❑ Techniques:
 - Impersonation
 - Vishing
 - Eavesdropping
 - Shoulder Surfing
 - Dumpster Diving
 - Reverse Social Engineering
 - Piggybacking
 - Tailgating



Computer-based Social Engineering

- ❑ “Sensitive information is gathered with the **help of computers**”.
- ❑ Techniques:
 - Phishing
 - Pop-up Window Attacks
 - Spam Mail
 - Instant Chat Messenger
 - Scareware



Mobile-based Social Engineering

- ❑ “Sensitive information is gathered with the **help of mobile apps**”.
- ❑ Techniques:
 - Publishing Malicious Apps
 - Using Fake Security Apps
 - Repackaging Legitimate Apps
 - SMiShing (SMS Phishing)

Human-based Social Engineering

Impersonation



- ❑ The attacker **pretends to be someone legitimate or an authorized person**
- ❑ Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc. to reveal **sensitive information**

Impersonation Examples



Posing as a Legitimate End User

The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"



Posing as an Important User

The attacker poses as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Human-based Social Engineering (Cont'd)

Impersonation (Vishing)

- ❑ An impersonation technique in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.



Vishing Example

Abusing the Over-Helpfulness of Help Desks

- ❑ The attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Human-based Social Engineering (Cont'd)



Eavesdropping

- **Unauthorized listening of conversations**, or reading of messages
- Interception of audio, video, or written communication



Shoulder Surfing

- Direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.



Dumpster Diving

- Looking for **treasure in someone else's trash**



Human-based Social Engineering (Cont'd)



Reverse Social Engineering

- ☐ The attacker presents him/herself as an **authority** and the target seeks his or her advice before or after offering the information that the attacker needs

Piggybacking

- ☐ An authorized person intentionally or unintentionally allows an **unauthorized person** to pass through a secure door e.g., “I forgot my ID badge at home. Please help me”

Tailgating

- ☐ The attacker, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door that requires key access

Computer-based Social Engineering



Pop-Up Windows

Windows that suddenly pop up while surfing the Internet and ask for **user information** to login or sign-in



Hoax Letters

Emails that issue **warnings** to the user about new viruses, Trojans, or worms that may harm the user's system



Chain Letters

Emails that offer **free gifts** such as money and software on condition that the user **forwards the mail to a specified number of people**

Computer-based Social Engineering (Cont'd)



Instant Chat Messenger

Gathering **personal information by chatting** with a selected user online to get information such as birth dates and maiden names



Spam Email

Irrelevant, unwanted, and unsolicited emails that attempt to collect **financial information, social security numbers, and network information**



Scareware

Malware that tricks computer users into **visiting malware infested websites**, or downloading/buying potentially malicious software



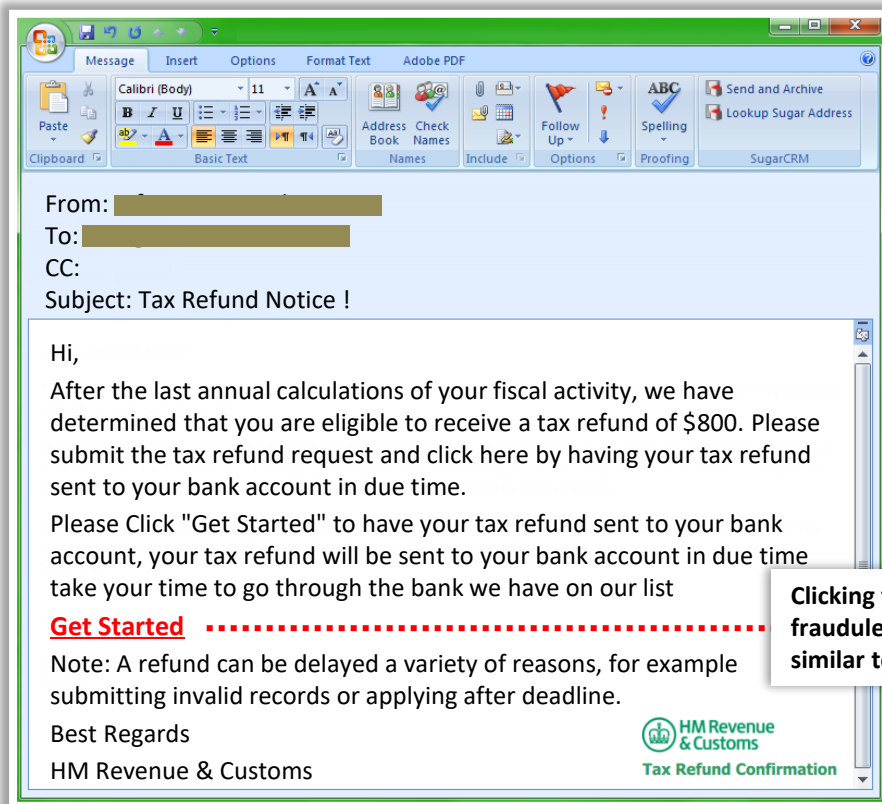
Computer-based Social Engineering: Phishing



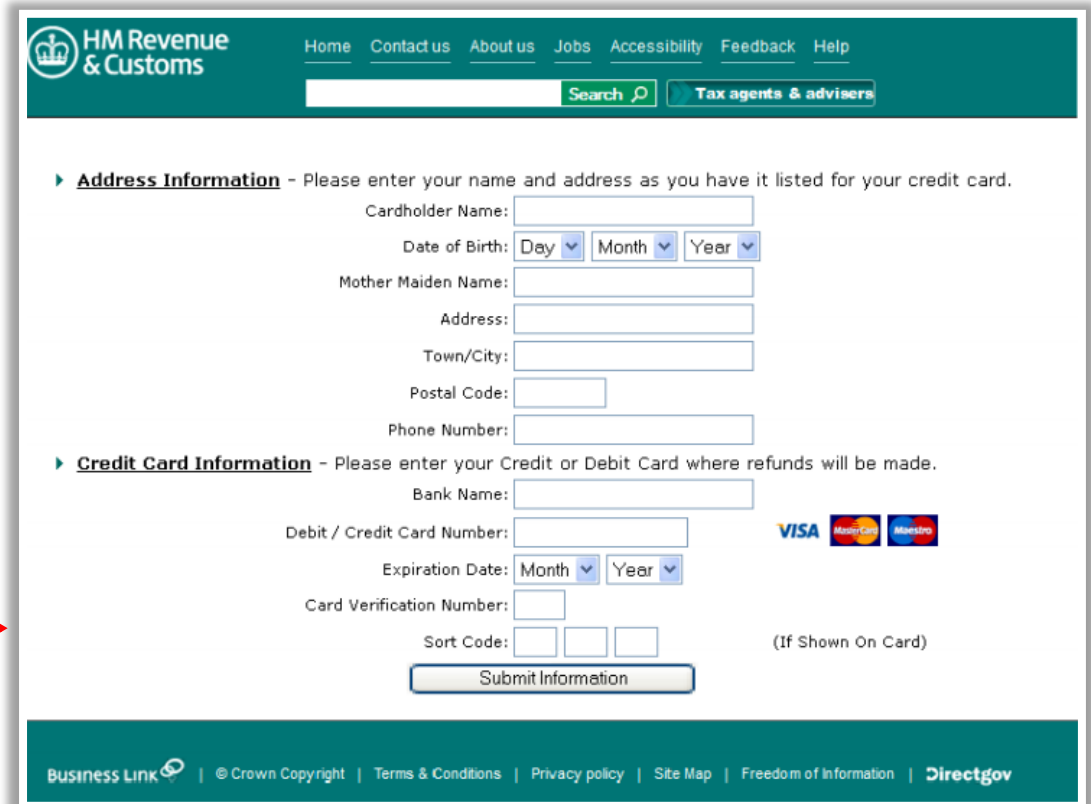
Phishing is the practice of **sending an illegitimate email** claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**



Phishing emails or pop-ups **redirect users to fake webpages** that mimic trustworthy sites, which ask them to submit their personal information



Clicking the link directs you to a fraudulent web page that looks similar to a genuine HMRC page



<http://www.hmrc.gov.uk>

Computer-based Social Engineering: Phishing (Cont'd)



Examples of Phishing Emails

From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: User
Subject: Important changes to your account

Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@tntech.edu,

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account , To confirm this verification

Log into [Online Banking](#) and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to \$1000 weekly also, to view details of the job and apply please visit website

<https://tinyurl.com/y3o3xzst>

Job Placement & Student Services
Cookeville, TN 38505 USA

From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: <joebstudent@students.tntech.edu>
Subject: The Security of Your Account



The Security of Your Account

Dear joebstudent@students.tntech.edu ,
We regret to inform you of this bad news

We have put your account in the list of limited accounts because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

[Confirm](#)

Questions? Take a look at our FAQs or contact Customer Support.

<https://its.tntech.edu>

Computer-based Social Engineering: Phishing (Cont'd)

Types of Phishing

-  **Spear Phishing**
A **targeted phishing attack** aimed at **specific individuals** within an organization
-  **Whaling**
An attacker **targets high profile executives** like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information
-  **Pharming**
The attacker **redirects web traffic** to a fraudulent website by installing a malicious program on a personal computer or server
-  **Spimming**
A **variant of spam** that **exploits Instant Messaging platforms** to flood spam across the networks

Phishing Tools



ShellPhish

A phishing tool used to **phish user credentials from various social networking platforms** such as Instagram, Facebook, Twitter, LinkedIn, etc.

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/shellphish
# ./shellphish.sh

[ASCII Art]

..... Phishing Tool coded by: @linux_

:: Disclaimer: Developers assume no liability
:: responsible for any misuse or damage cau

[01] Instagram    [09] Origin      [17]
[02] Facebook     [10] Steam        [18]
[03] Snapchat     [11] Yahoo         [19]
[04] Twitter      [12] LinkedIn     [99]
[05] Github       [13] Protonmail
[06] Google       [14] Wordpress
[07] Spotify      [15] Microsoft
[08] Netflix      [16] InstaFollowers

[*] Choose an option: 1
```

<https://github.com>

```
Parrot Terminal
File Edit View Search Terminal Help

[*] IP Found!
[*] Victim IP: 66
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google
[*] Reverse DNS: 52
[*] IP Continent: North America (NA)
[*] IP Country: United States
[*] City Location: Unknown
[*] ISP: Google
[*] AS Number:
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: @gmail.com
[*] Password:
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```



BLACKKEYE

<https://github.com>



PhishX

<https://github.com>



Modlishka

<https://github.com>



Trape

<https://github.com>

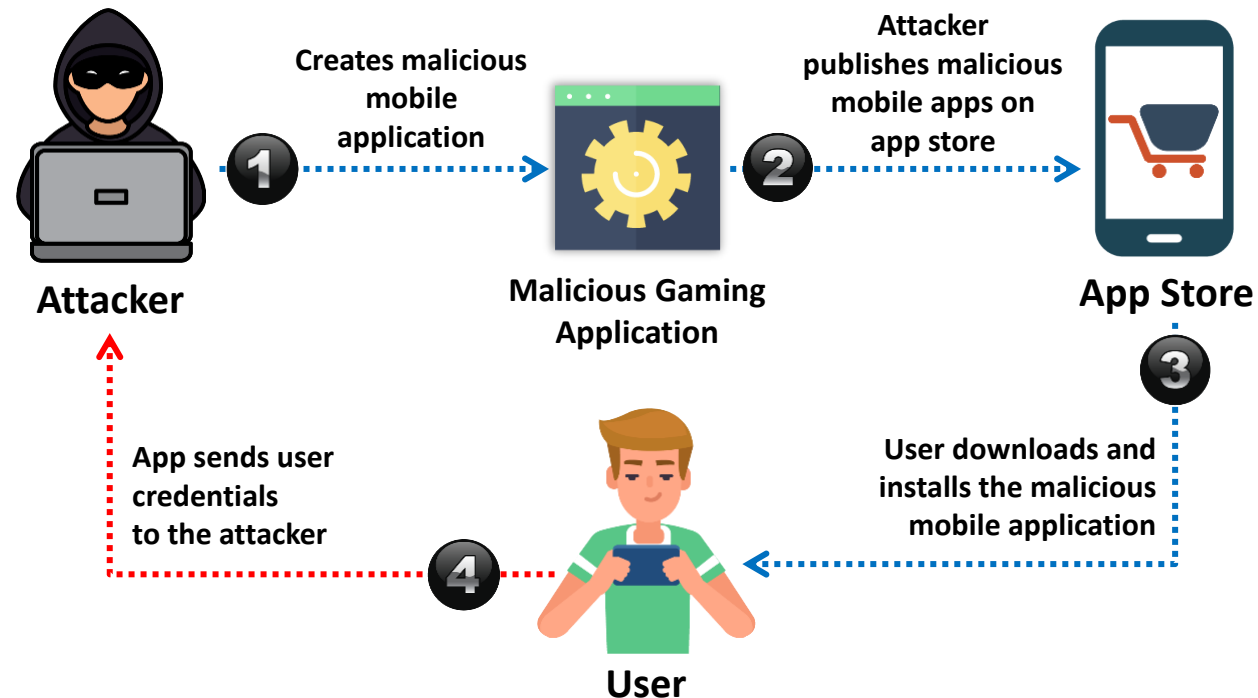


Evilginx

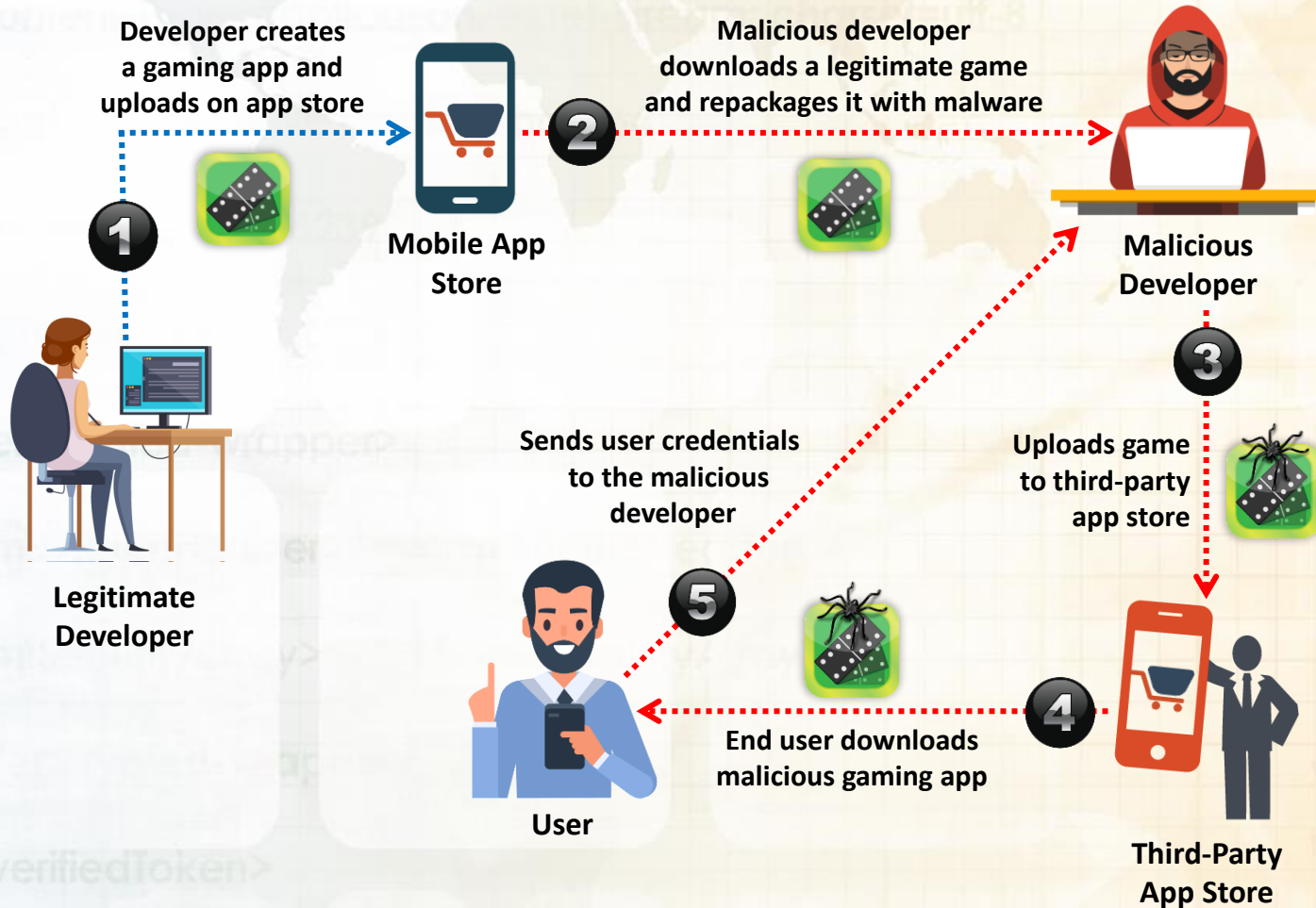
<https://github.com>

Mobile-based Social Engineering: Publishing Malicious Apps

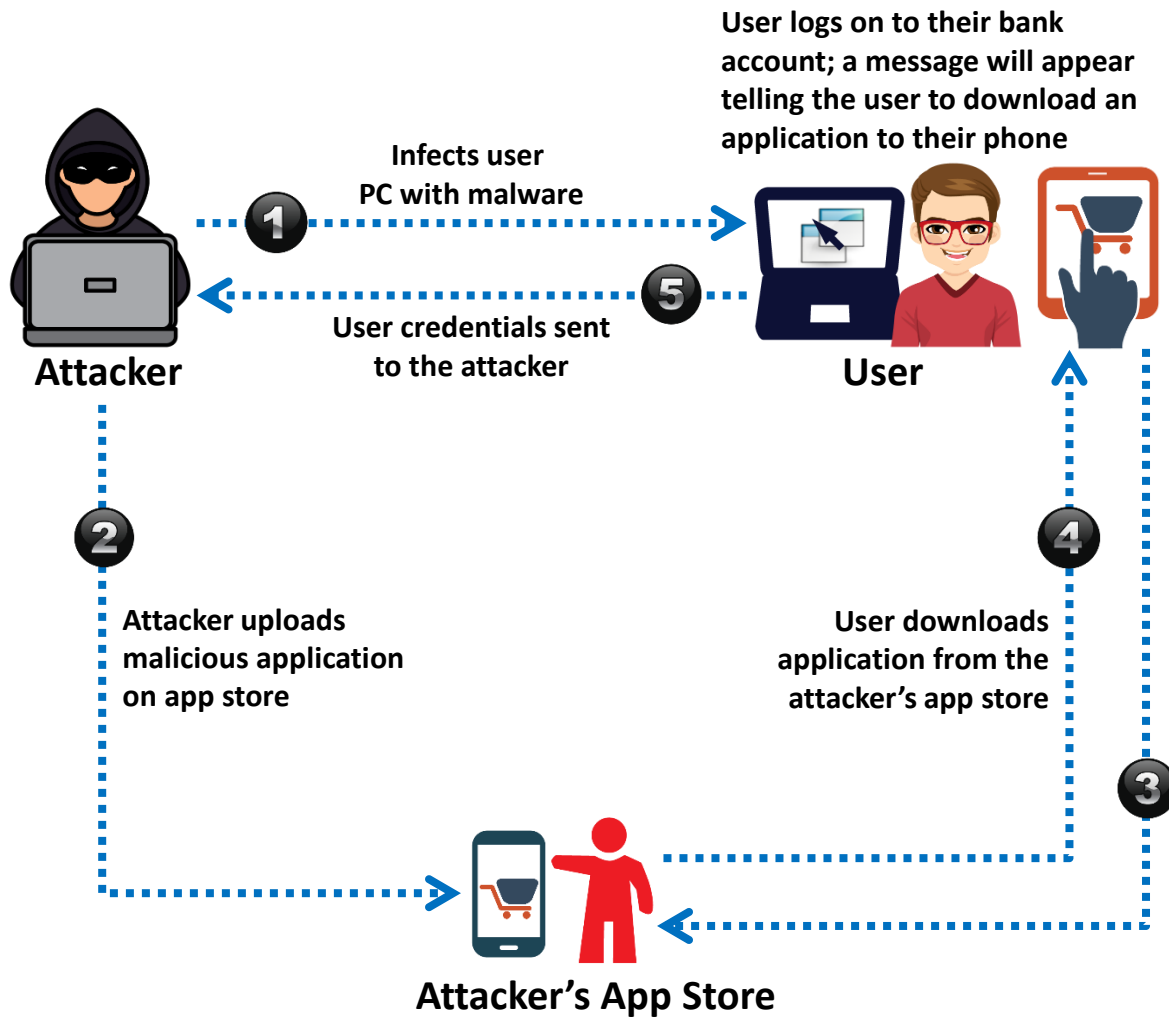
- ❑ Attackers create **malicious apps** with attractive features and **similar names** to popular apps, and publish them in major **app stores**
- ❑ **Users download these apps** unknowingly and are infected by malware that sends **credentials to attackers**



Mobile-based Social Engineering: Repackaging Legitimate Apps



Mobile-based Social Engineering: Fake Security Applications



Mobile-based Social Engineering: SMiShing (SMS Phishing)

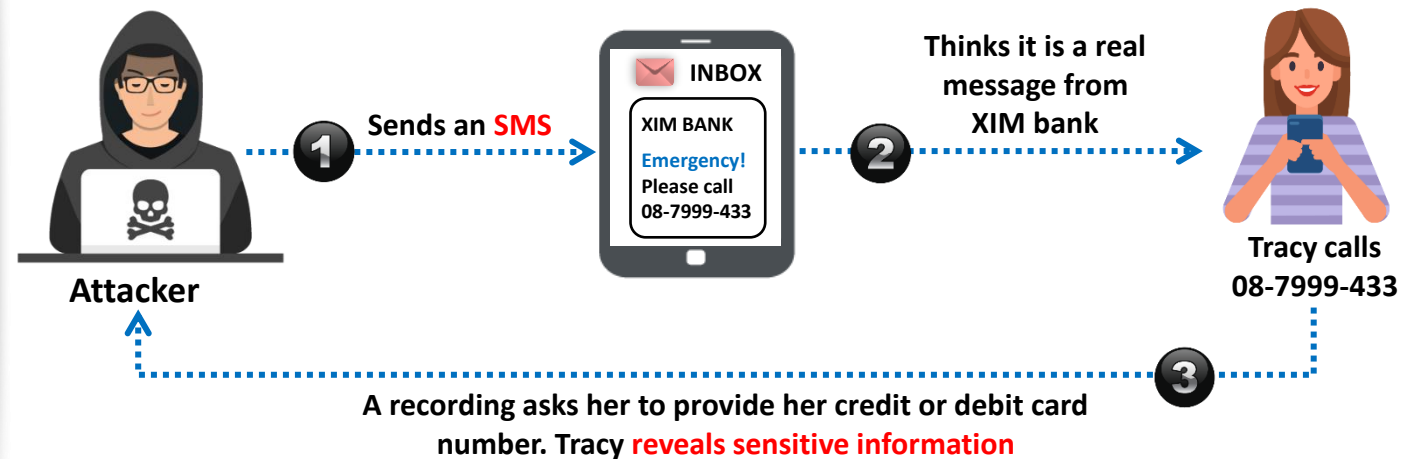


SMiShing (SMS phishing) is the act of using **SMS text messaging system** of cellular phones or other mobile devices to **lure users into instant action**, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number

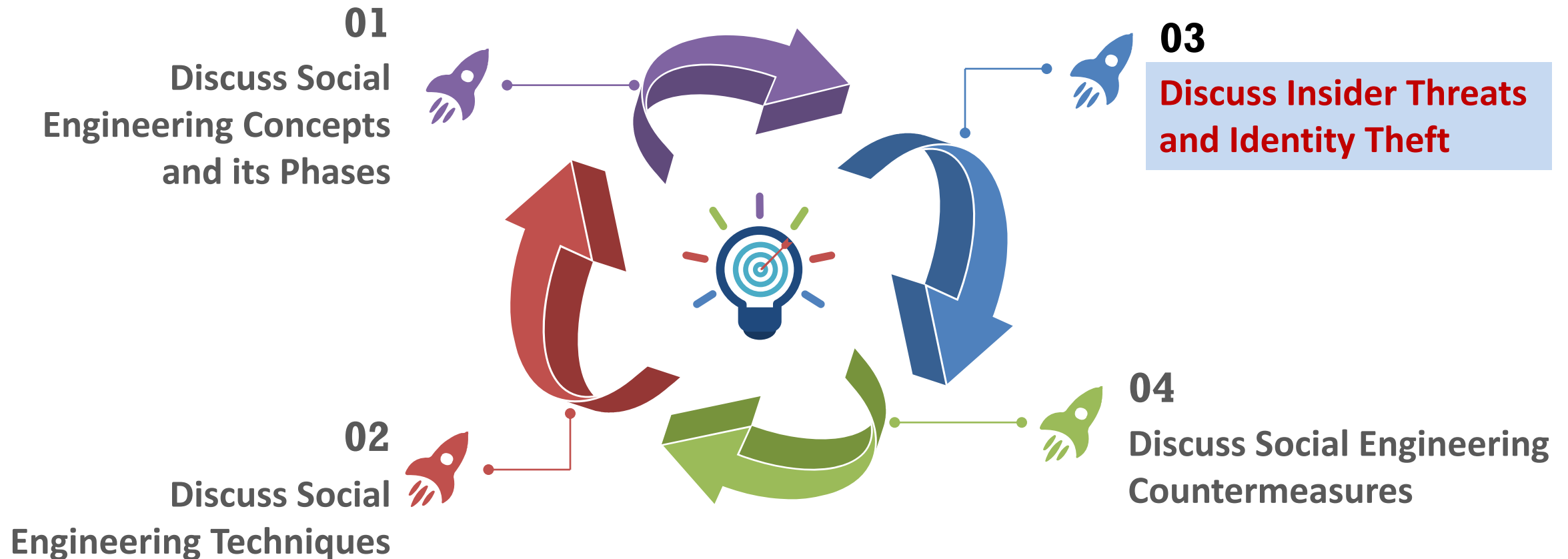


SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them **to divulge their personal information and account details**

SMiShing Example



Module Flow

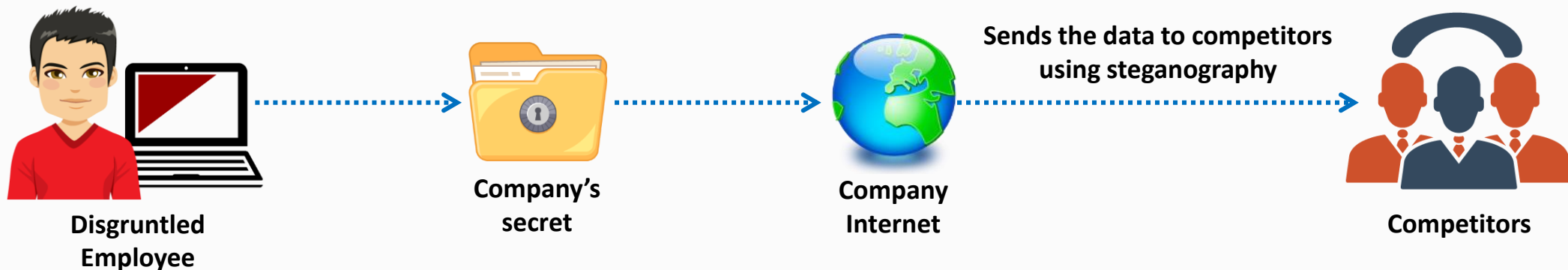


Insider Threats/Insider Attacks

- ❑ An insider is any **employee** (trusted person or people) who have **access to critical assets** of an organization
- ❑ An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- ❑ Such attacks are generally performed by a privileged user, **disgruntled employee**, **terminated employee**, accident-prone employee, **third party**, undertrained staff, etc.



Example of Insider Attack: Disgruntled Employee



Reasons for Insider Attacks



Financial gain



Steal confidential data



Revenge



Become future competitor



Perform competitor's bidding



Public announcement



Types of Insider Threats



Malicious Insider

A **disgruntled or terminated employee** who steals data or destroys the company's networks intentionally by **introducing malware** into the corporate network



Negligent Insider

Insiders who are **uneducated on potential security threats** or who simply bypass general security procedures to meet workplace efficiency



Professional Insider

Harmful insiders who use their technical knowledge to **identify weaknesses and vulnerabilities** in the company's network and **sell confidential information to competitors** or black-market bidders



Compromised Insider

An insider with **access to critical assets** of an organization who is **compromised by an outside threat actor**



Why are Insider Attacks Effective?



Insider attacks are easy **to launch**



Preventing insider attacks **is difficult**; an inside attacker can easily succeed



Differentiating **harmful actions** from the employee's regular work is very difficult



If malicious activity is detected, the employee may **refuse to accept** responsibility and claim it was a mistake



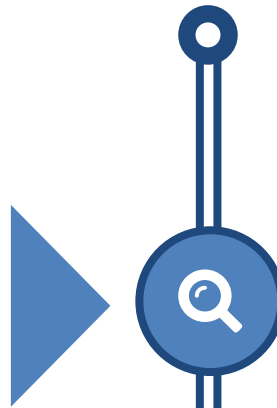
Employees can easily **cover their tracks**



Can go **undetected** for years and remediation is very expensive

Identity Theft

Identity theft is a crime in which **an imposter steals your personally identifiable information** such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes



Attackers can use identity theft to **impersonate employees of a target** organization and physically access facilities

Identity Theft (Cont'd)

The attacker steals people's identity for fraudulent purposes such as:



To open new credit card accounts in the **name of the user** without paying the bills



To open a **new phone** or wireless account in the user's name



To use the victims' information to obtain **utility services** such as electricity, heating, or cable TV



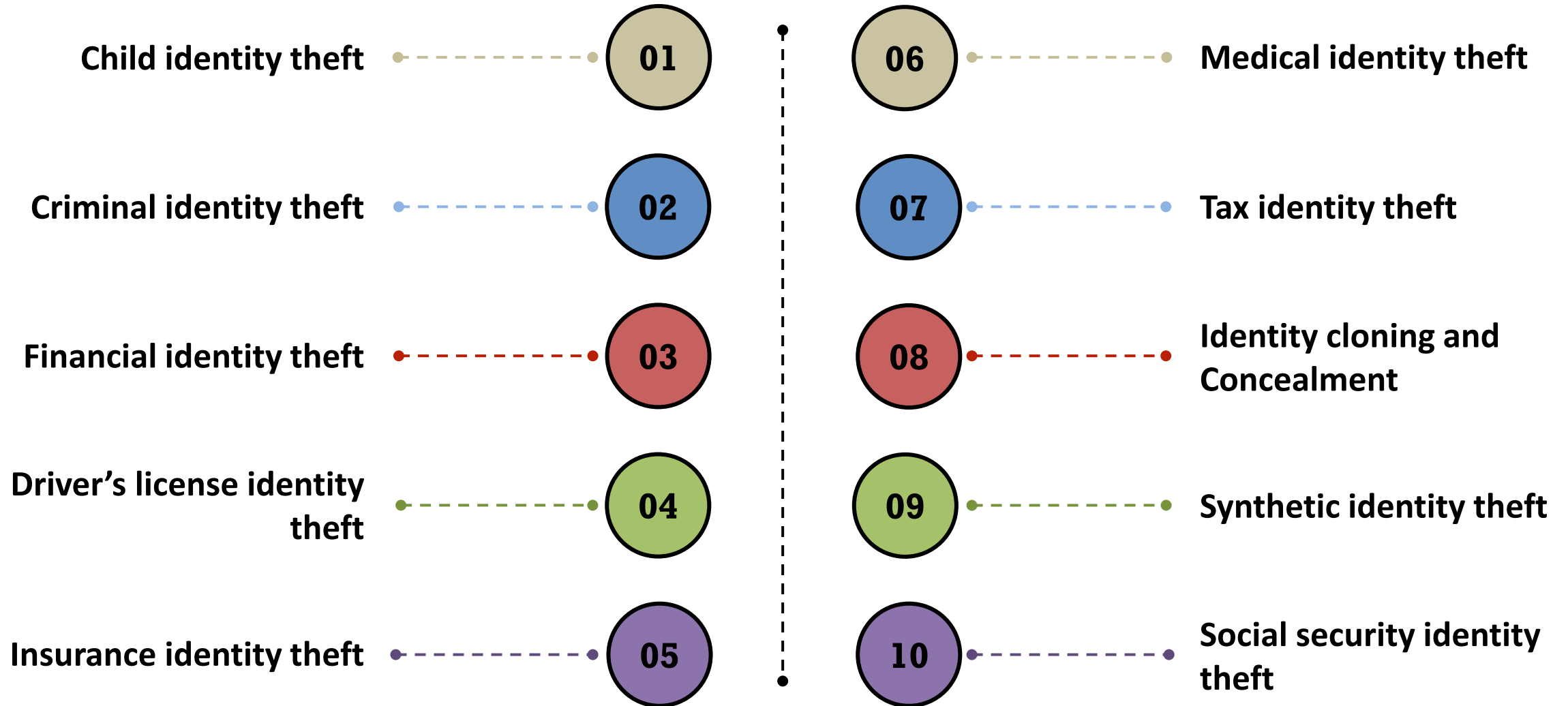
To open bank accounts with the intention of **writing bogus** checks using the victim's information



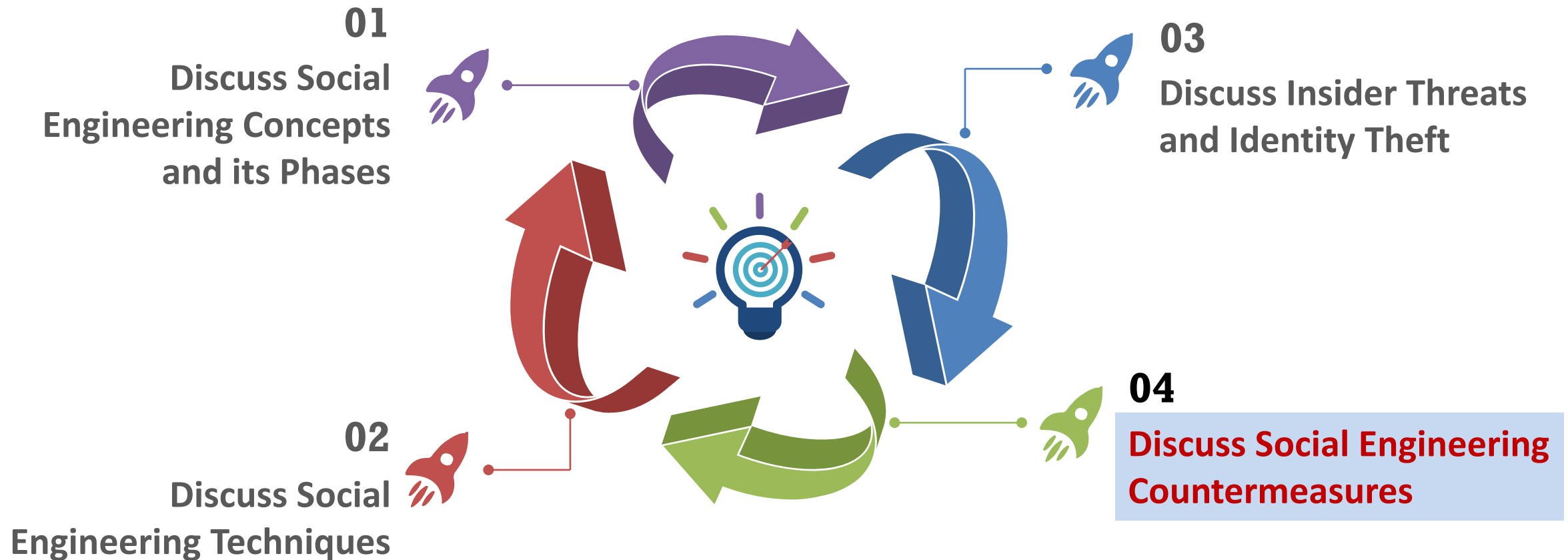
To clone an ATM or debit card to make **electronic withdrawals** from the victim's accounts



Types of Identity Theft



Module Flow



Social Engineering Countermeasures



Password Policies

- ✓ Periodic password changes
- ✓ Avoiding guessable passwords
- ✓ Account blocking after failed attempts
- ✓ Increasing length and complexity of passwords
- ✓ Improving secrecy of passwords



Physical Security Policies

- ✓ Identification of employees by issuing ID cards, uniforms, etc.
- ✓ Escorting visitors
- ✓ Restricting access to work areas
- ✓ Proper shredding of useless documents
- ✓ Employing security personnel



Defense Strategy

- ✓ Social engineering campaign
- ✓ Gap analysis
- ✓ Remediation strategies



Insider Threats Countermeasures



Identity Theft Countermeasures



Secure or shred all documents containing your **private information**



Ensure your name is not present in **marketers' hit lists**



Review your **credit card statement** regularly and store it securely, out of reach of others



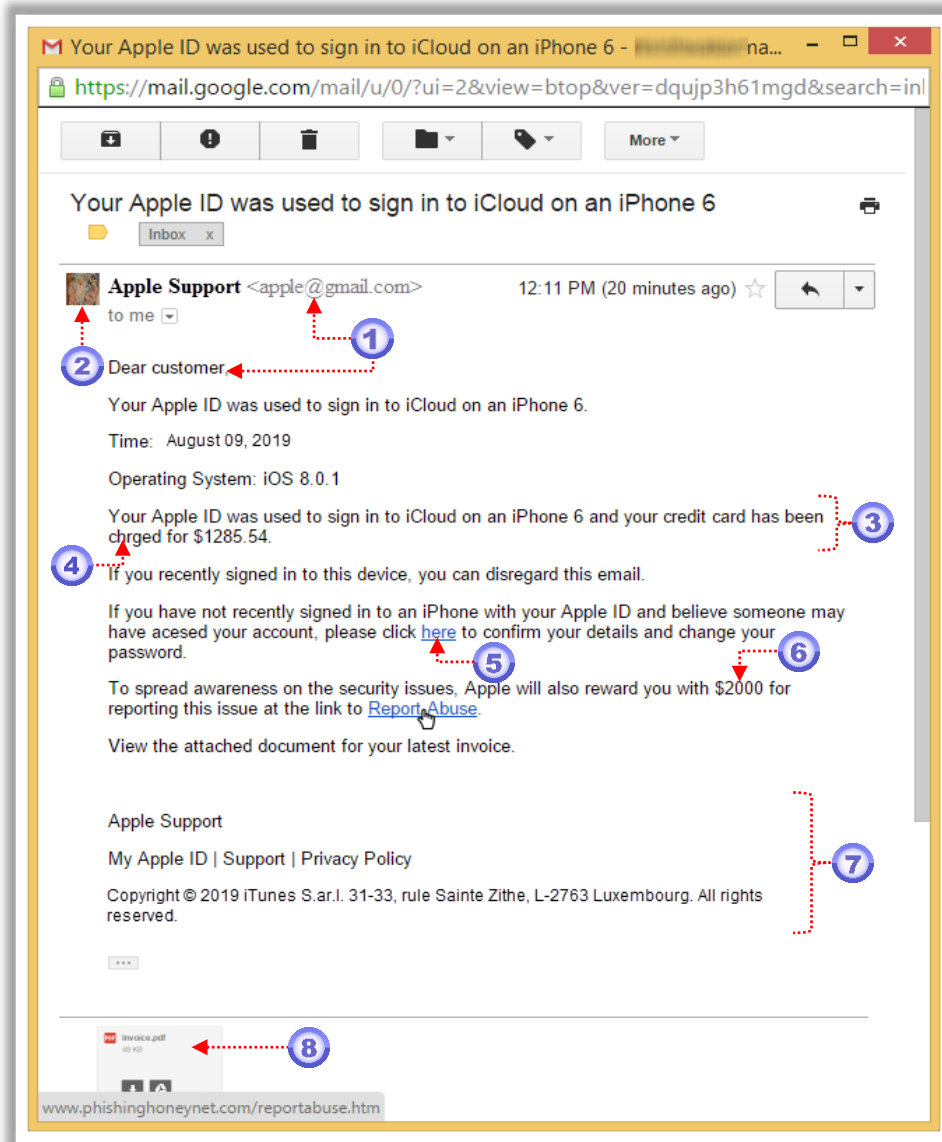
Never give any personal information over the **phone**



Keep your mail secure by **emptying the mailbox** quickly



How to Detect Phishing Emails?



1

Appears to be from a **bank, company, or social networking site**, and has a **generic greeting**

2

Appears to be from a person listed in your **email address book**

3

Gives a sense of **urgency** or a **veiled threat**

4

May contain **grammatical/spelling mistakes**

5

Includes links to **spoofed websites**

6

May contain **offers that seem to be too good to be true**

7

Includes **official-looking logos** and other information taken from legitimate websites

8

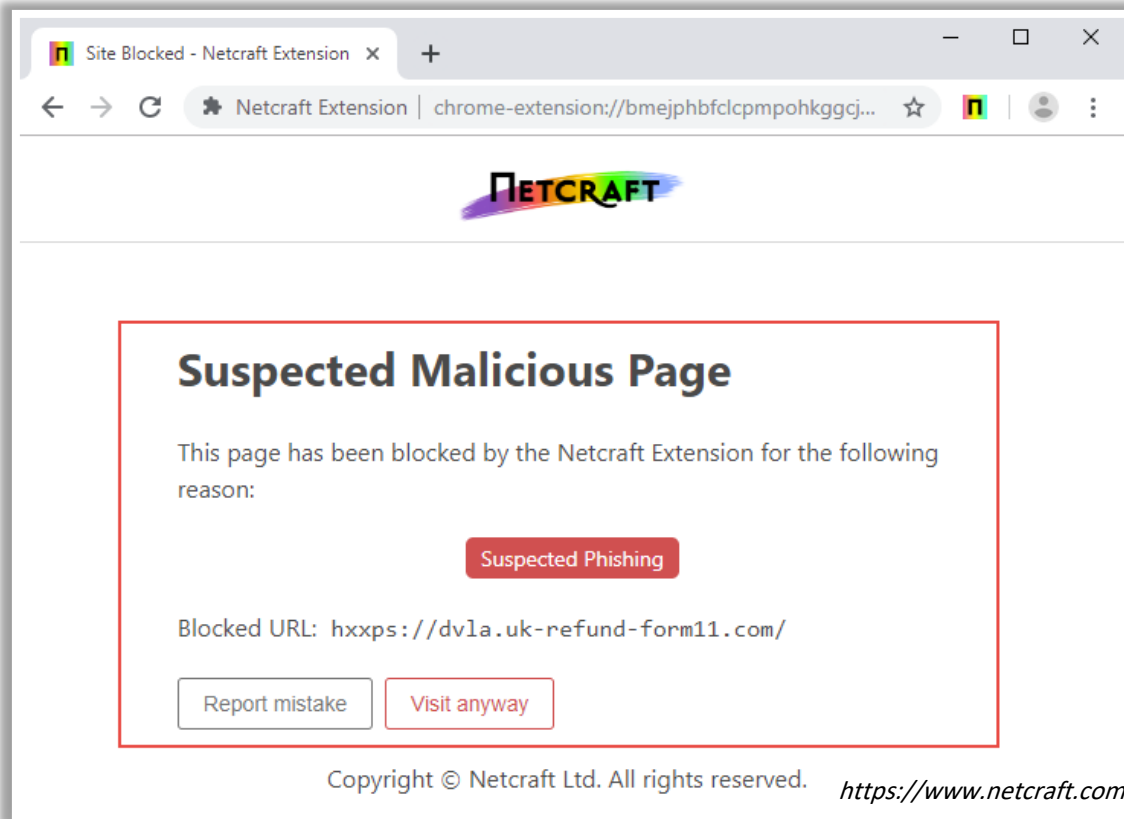
May contain a **malicious attachment**

Anti-Phishing Toolbar

Netcraft



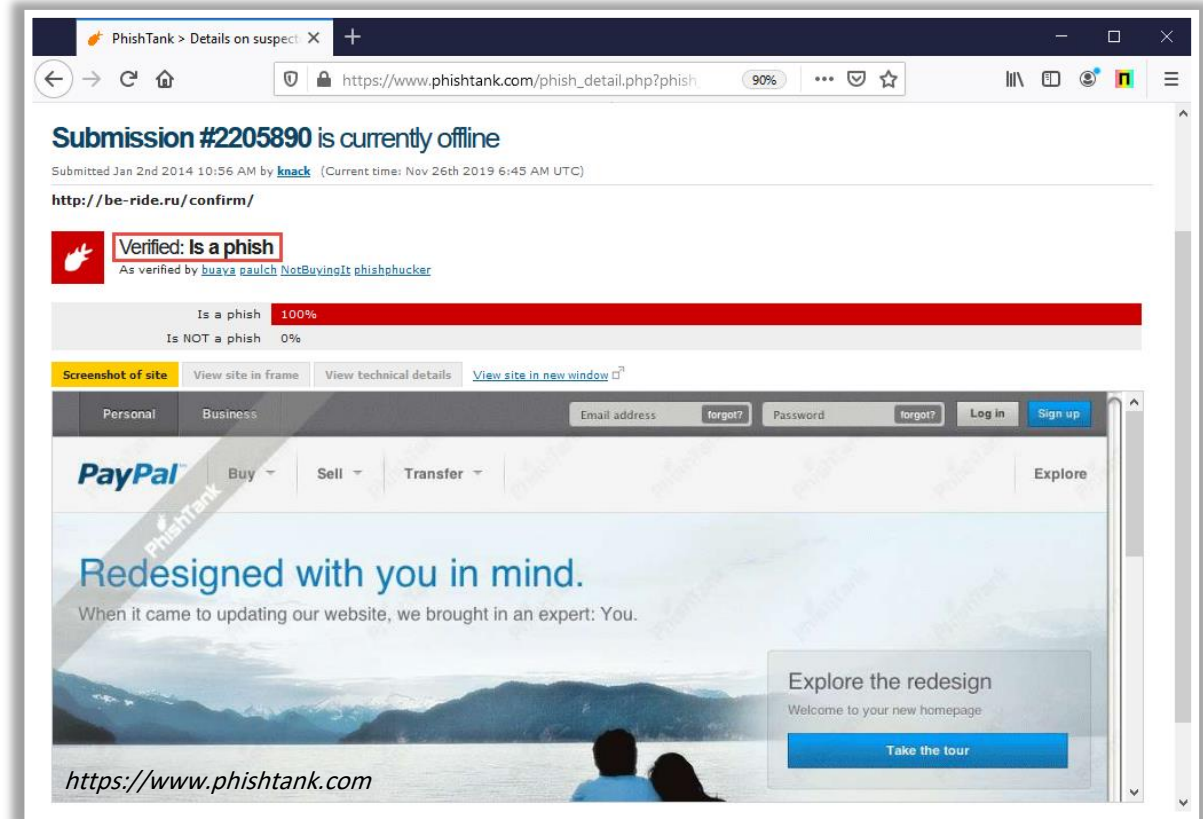
- ❑ The Netcraft **anti-phishing community** is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks



PhishTank



- ❑ PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet
- ❑ It provides an **open API** for developers and researchers to integrate **anti-phishing** data into their apps



Social Engineering Tools: Social Engineering Toolkit (SET)



The Social-Engineer Toolkit (SET) is an open-source **Python-driven tool** aimed at penetration testing around social engineering

```
Parrot Terminal
File Edit View Search Terminal Help

.M""bgd `7MM""YMM MMP"MM"YMM
,MI  "Y  MM  `7 P'  MM  `7
`MMb.  MM  d    MM
`YMMNq. MMmmMM  MM
  `MM  MM  Y    MM
Mb  dM  MM  ,M  MM
P"Ybmmd" .JMMmmmmMM .JMLL

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
[---] Version: 8.0.1 [---]
[---] Codename: 'Maverick - BETA' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

<https://www.trustedsec.com>

```
Parrot Terminal
File Edit View Search Terminal Help

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```



SpeedPhish Framework (SPF)
<https://github.com>



Gophish
<https://getgophish.com>



King Phisher
<https://github.com>



LUCY
<https://www.lucysecurity.com>



MSI Simple Phish
<https://microsolved.com>

Audit Organization's Security for Phishing Attacks using OhPhish



OhPhish is a web-based portal to **test employees' susceptibility to social engineering attacks**



OhPhish is a phishing simulation tool that provides the organization with a **platform to launch phishing simulation campaigns** on its employees



The screenshot shows the OhPhish dashboard in a web browser. The browser address bar displays <https://portal.ohphish.com/dashboard>. The dashboard features a sidebar with navigation links: Home, Users, Groups, Campaigns, Reports, Trainings, Templates, and Support. The main content area includes a 'Dashboard' section with a recommendation to refer to a link before starting. Below this are six campaign mode options: Entice to Click, Credential Harvesting, Send Attachment, Training, Vishing, and Smishing. A 'Live Phishing Campaigns' table is also visible, showing columns for Campaign, Campaign Type, Status, Assigned Training, Started, Stopped, Scheduled, Sent, Clicked, and Compliance. The table contains one row for an 'Email' campaign with a status of 'In Progress' and 100% compliance. The footer of the dashboard includes the copyright notice '© 2020 Shield Alliance International Limited.' and the URL <https://ohphish.eccouncil.org>.

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compl
[Icon]	Email	In Progress	URL Padding			NA	1	0	100

Module Summary



This module discussed social engineering concepts along with various phases of social engineering attack



It also discussed various human-based, computer-based, and mobile-based social engineering techniques



The module discussed insider threats, including the various types of insider threats



It also discussed identity theft and the types of identity theft



The module ended with a detailed discussion of countermeasures to employ in order to defend against social engineering attacks, insider threats, and identity theft



In the next module, we will discuss in detail on various network level attacks and countermeasures