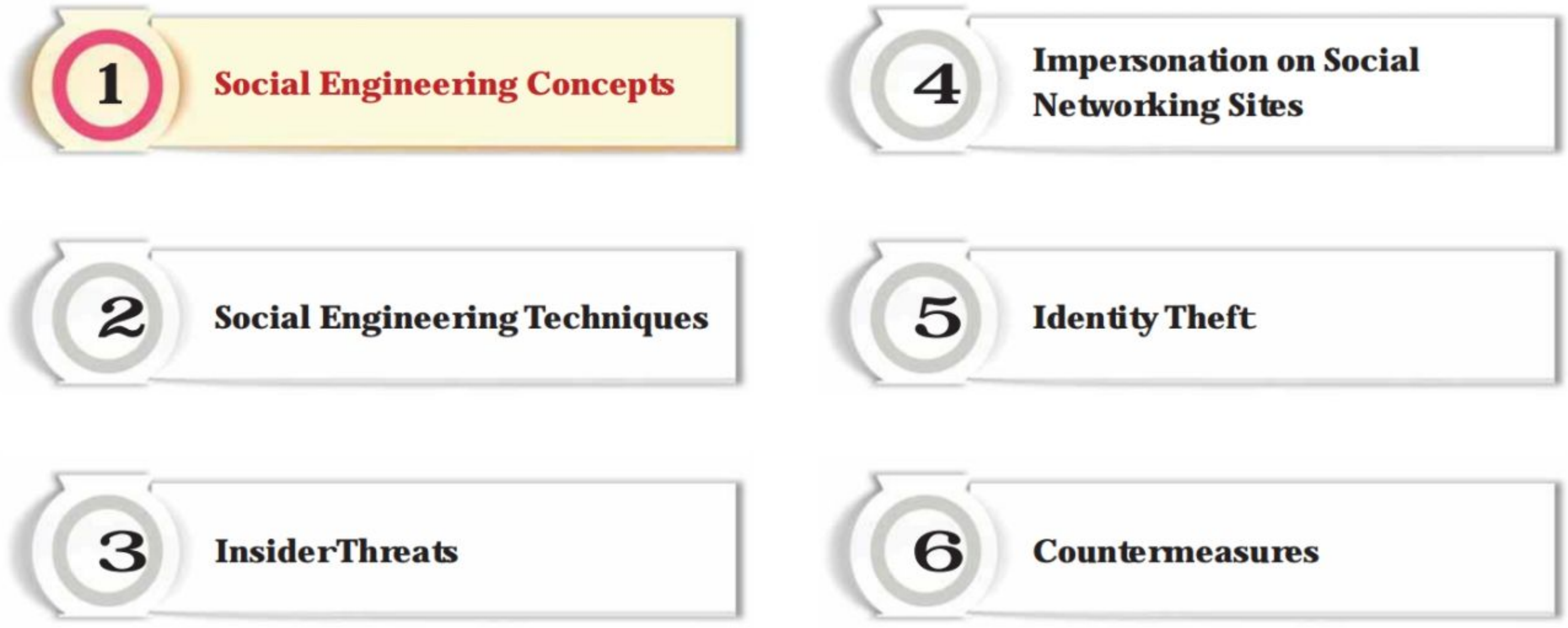
Module Flow



1 Social Engineering Concepts

2 Social Engineering Techniques

3 InsiderThreats

4 Impersonation on Social Networking Sites

5 Identity Theft

6 Countermeasures

What is Social Engineering?

- Social engineering is the art of convincing people to reveal confidential information
- Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- 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

Impactof Attack on an Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

Behaviors Vulnerable to Attacks

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust
- Greed

What is Social Engineering? (Cont'd)

Factors thatMake Companies Vulnerable to Attacks

- Insufficient security training
- Unregulated access to information
- Several organizational units
- Lack of security policies

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and human behavior is the most susceptible factor
- It is difficult to detect social engineering attempts
- There is no method that can be applied to ensure complete security from social engineering attacks
- There is no specific software or hardware to defend against a social engineering attack

Phases of a Social Engineering Attack

Research the TargetCompany

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

Selecta Target

- Identify frustrated employees of the target company

Develop a Relationship

- Develop a relationship with the selected employees

Exploitthe Relationship

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. InsiderThreats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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
  - Diversion Theft
  - Honey Trap
  - Baiting and Quid Pro Quo
  - Elicitation

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.
- Impersonation helps attackers to trick a target into revealing sensitive information
- The most common human-based social engineering technique

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 importantuser

- 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?"

Posing as a technical supportagent

- The attacker poses as technical support staff and requests IDs and passwords

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"

Human-based Social Engineering (Cont'd)

Eavesdropping

- Unauthorized listening of conversations, or reading of messages
- Interception of audio, video, or written communication
- Can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Can also be done from a farther distance with the aid of vision enhancing devices such as binoculars

Dumpster Diving

- Looking for treasure in someone else's trash
- Involves collecting phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins or printer bins, or user desks (e.g., sticky notes), etc.

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

Diversion Theft

- The attacker tricks a person responsible for making a genuine delivery into delivering the consignment to a location other than the intended location

Human-based Social Engineering (Cont'd)

Honey Trap

- Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain confidential information about the target company

Baiting

- Attackers offer end users something alluring in exchange for important information such as login details and other sensitive data
- A physical device such as USB flash drive containing malicious files is left in a location where people can easily find it

Quid Pro Quo

- Attackers call numerous random numbers within a company, claiming to be from technical support
- They offer their service to end users in exchange for confidential data or login credentials

Elicitation

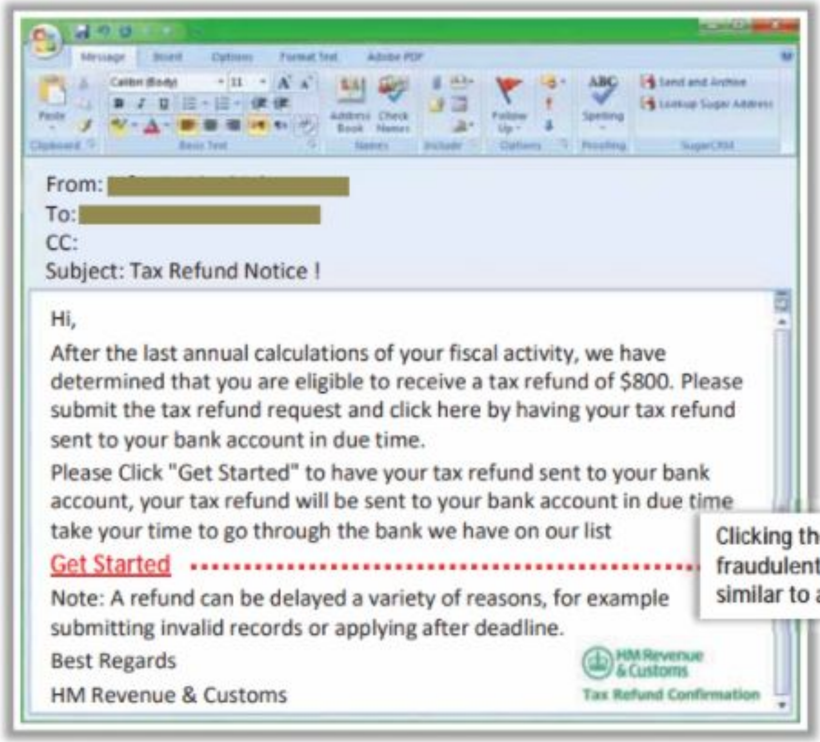
- Attackers extract information from the victim by engaging him/her in normal and disarming conversations
- Based on the victim's interests, attackers must work to target their elicitation approach to extract the relevant information

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
InstantChat 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



From: [redacted]
To: [redacted]
CC:
Subject: Tax Refund Notice !

Hi,

After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of $800. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time.

Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list

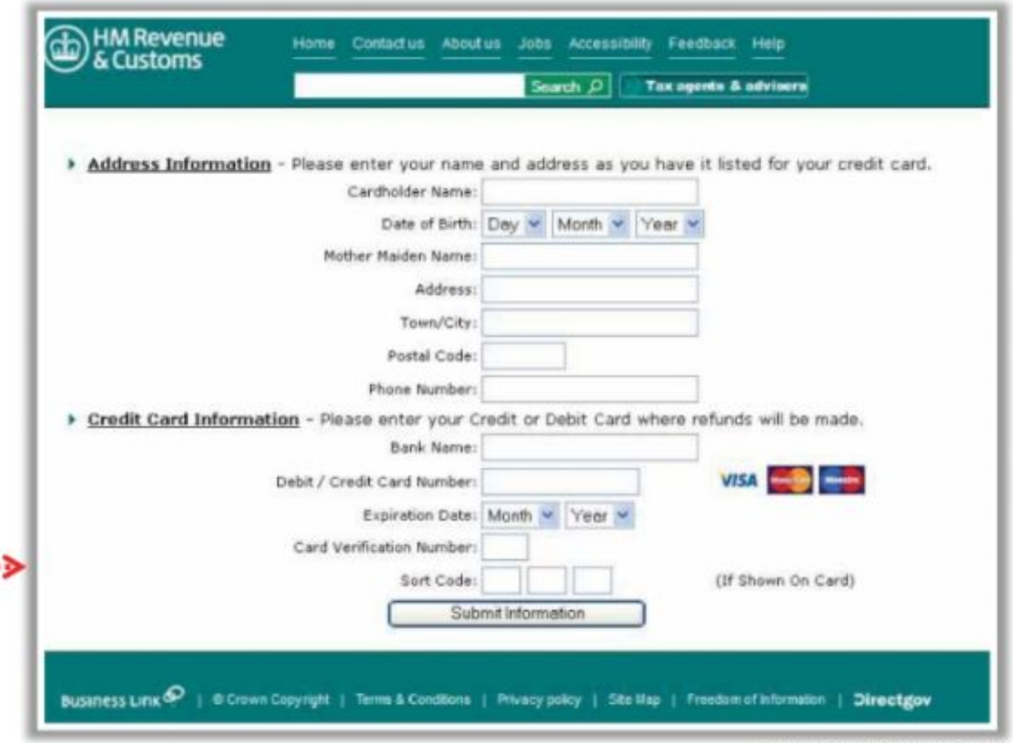
Get Started

Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Best Regards

HM Revenue & Customs

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



Address Information - Please enter your name and address as you have it listed for your credit card.

Cardholder Name:
Date of Birth: Day Month Year
Mother Maiden Name:
Address:
Town/City:
Postal Code:
Phone Number:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Bank Name:
Debit / Credit Card Number:
Expiration Date: Month Year
Card Verification Number:
Sort Code: (If Shown On Card)

http://www.hmrc.gov.uk

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

Types of Phishing

SpearPhishing

- A targeted phishing attack aimed at specific individuals within an organization
- Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people

Whaling

- An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information
- The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing

Pharming

- The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server
- Also known as "phishing without a lure", and performed by using DNS Cache Poisoning or Host File Modification

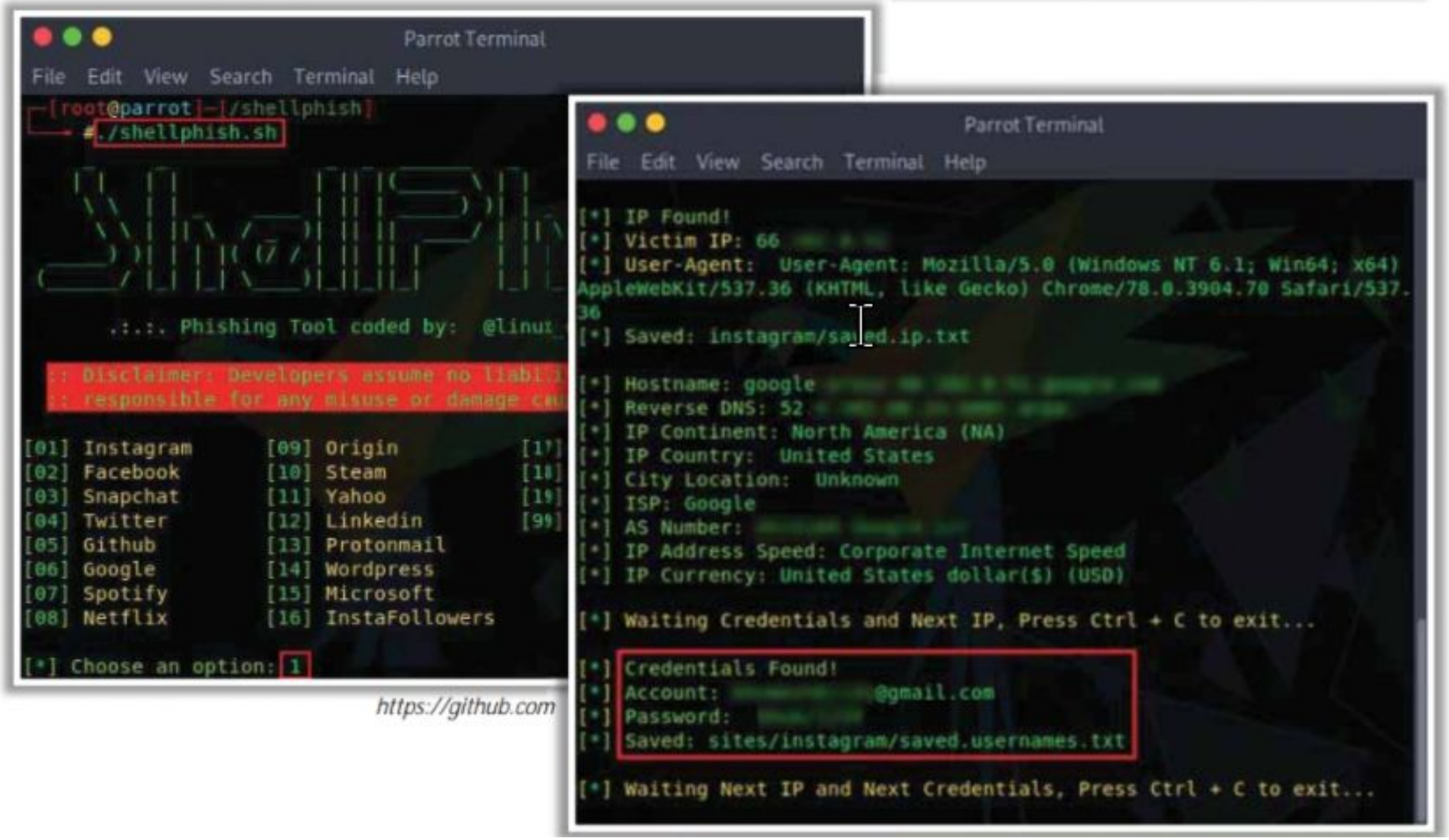
Spimming

- A variant of spam that exploits Instant Messaging platforms to flood spam across the networks
- Attacker uses bots to harvest Instant Message IDs and spread spam

Phishing Tools

ShellPhish

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



```
┌─[root@parrot]─[/shellphish]
└──╼ #./shellphish.sh

     .:.:. Phishing Tool coded by:  @linux

:: Disclaimer: Developers assume no liabi
:: responsible for any misuse or damage ca

[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

```
[*] IP Found!
[*] Victim IP: 66 [redacted]
[*] 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 [redacted]
[*] Reverse DNS: 52 [redacted]
[*] IP Continent: North America (NA)
[*] IP Country:  United States
[*] City Location:  Unknown
[*] ISP: Google
[*] AS Number: [redacted]
[*] 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: [redacted]@gmail.com
[*] Password: [redacted]
[*] Saved: sites/instagram/saved.usernames.txt

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

BLACKEYE
https://github.com

PhishX
https://github.com

Modlishka
https://github.com

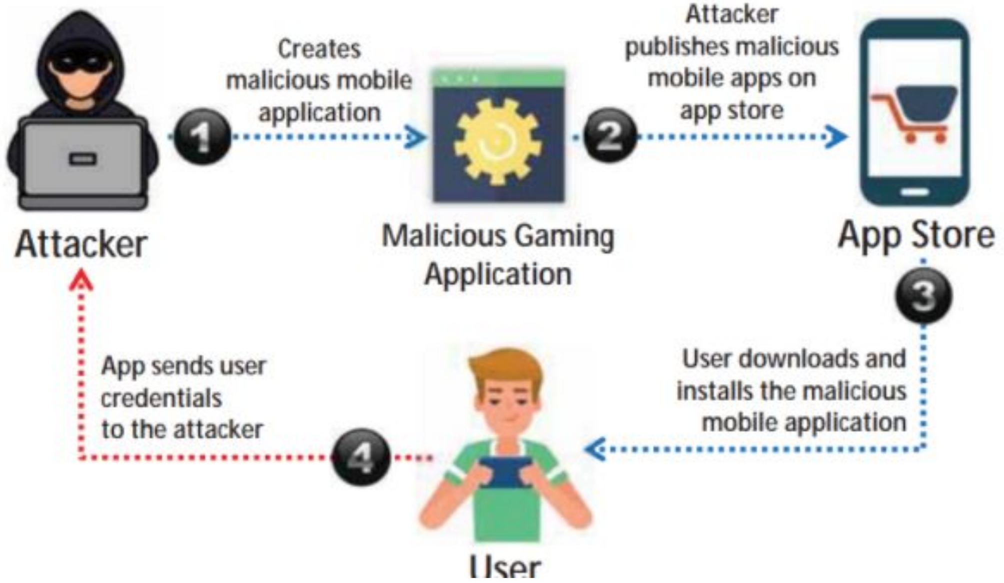
Trape
https://github.com

Evilginx
https://github.com

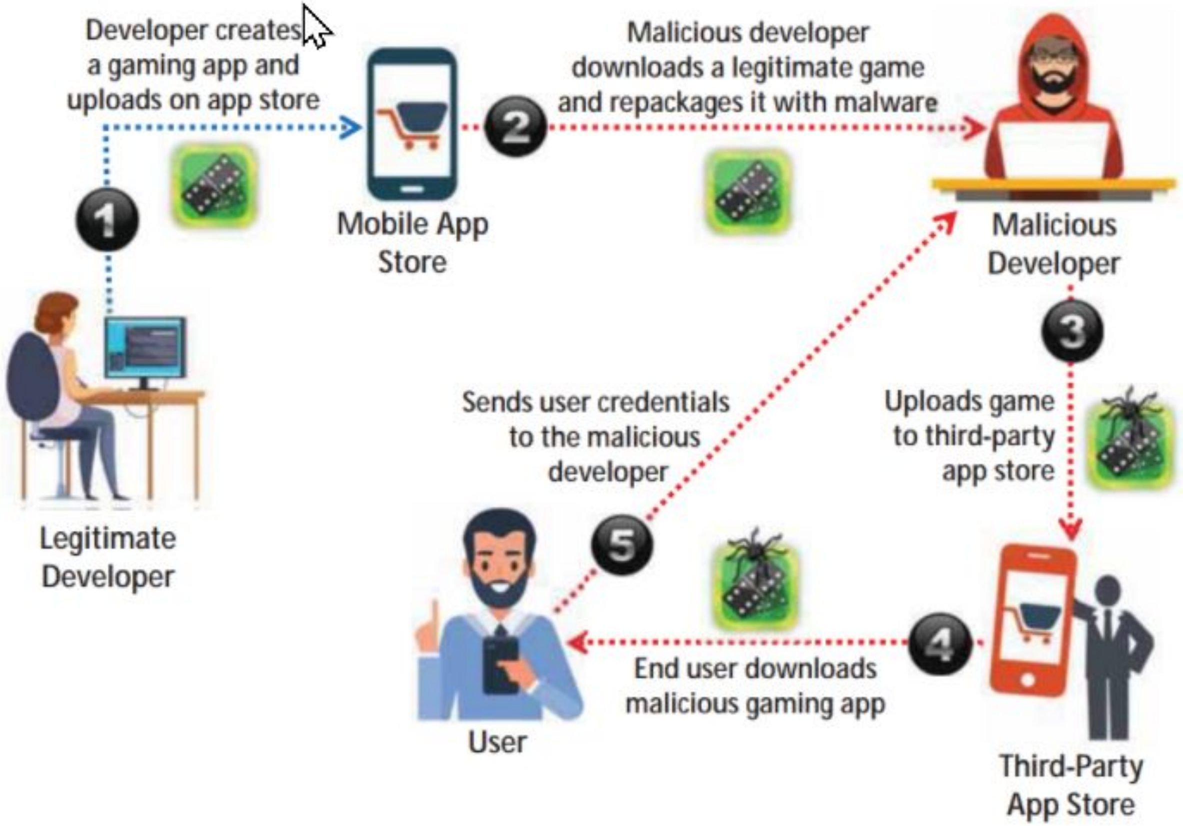
Mobile-based Social Engineering: Publishing Malicious Apps and Repackaging Legitimate Apps

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


Attacker
1
Creates malicious mobile application
Malicious Gaming Application
2
Attacker publishes malicious mobile apps on app store
App Store
3
User downloads and installs the malicious mobile application
User
4
App sends user credentials to the attacker

Repackaging Legitimate Apps


Developer creates a gaming app and uploads on app store
1
Legitimate Developer
Mobile App Store
2
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
3
Uploads game to third-party app store
Third-Party App Store
4
End user downloads malicious gaming app
User
5
Sends user credentials to the malicious developer

Mobile-based Social Engineering: Fake Security Applications

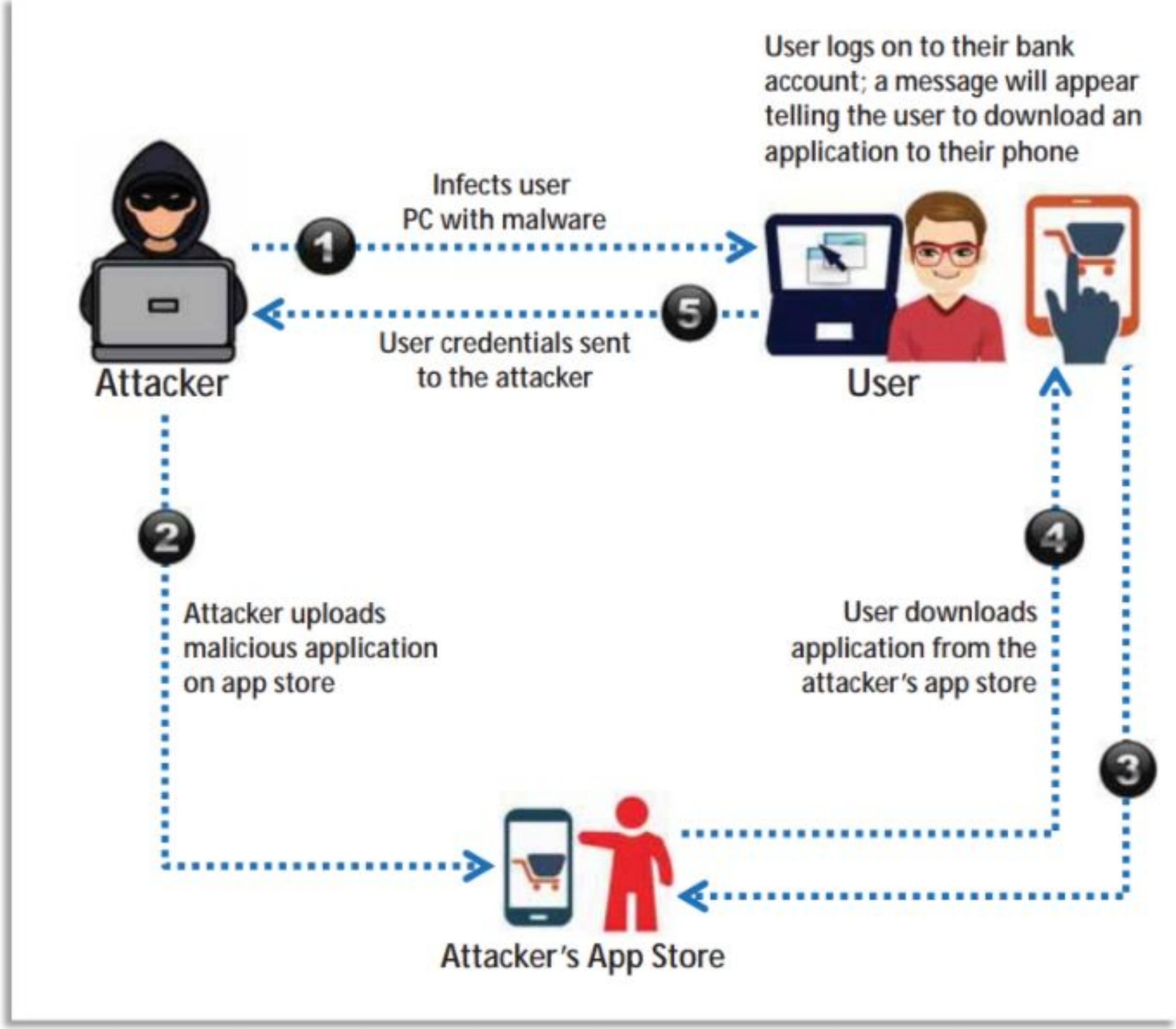
1. Attacker infects the victim's PC

2. Attacker uploads a malicious app to an app store

3. Victim logs into his or her bank account. Malware in the system displays a pop-up message telling the victim to download an app onto his or her phone to receive security messages

4. Victim downloads the malicious app on his or her phone

5. At this point, the attacker can access two-factor authentication information sent to the victim from the bank via SMS



User logs on to their bank account; a message will appear telling the user to download an application to their phone

1 Infects user PC with malware

5 User credentials sent to the attacker

2 Attacker uploads malicious application on app store

4 User downloads application from the attacker's app store

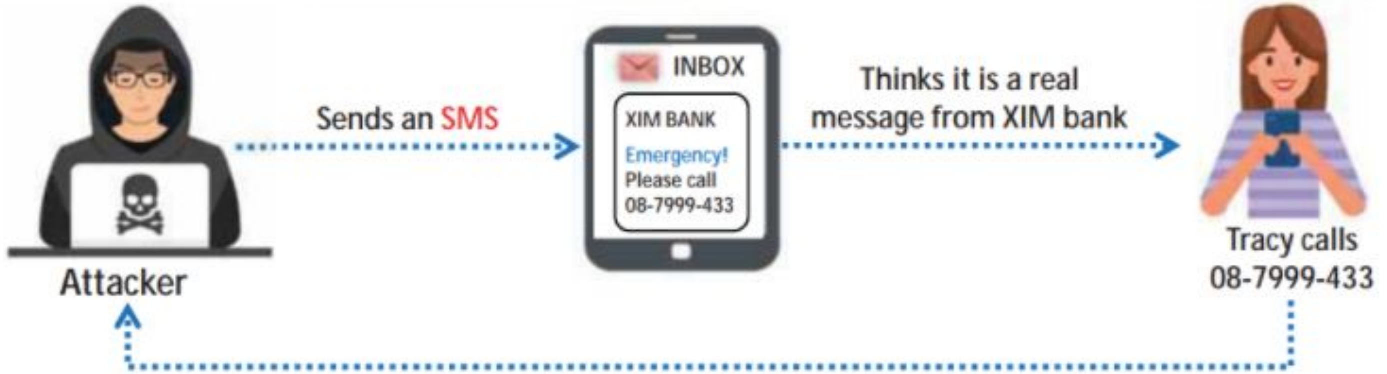
3

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

1. Tracy receives an SMS (text message), ostensibly from the security department at XIM Bank
2. It claims to be urgent and instructs Tracy to call the phone number in the SMS immediately
3. Worried, she calls, thinking it is an XIM Bank customer service number. She hears a recording asking her to provide her credit or debit card number
4. Tracy reveals the sensitive information due to the fraudulent texts



Attacker

Sends an SMS

INBOX

XIM BANK
Emergency!
Please call
08-7999-433

Thinks it is a real message from XIM bank

Tracy calls 08-7999-433

A recording asks her to provide her credit or debit card number. Tracy reveals sensitive information

Insider Threats/Insider Attacks

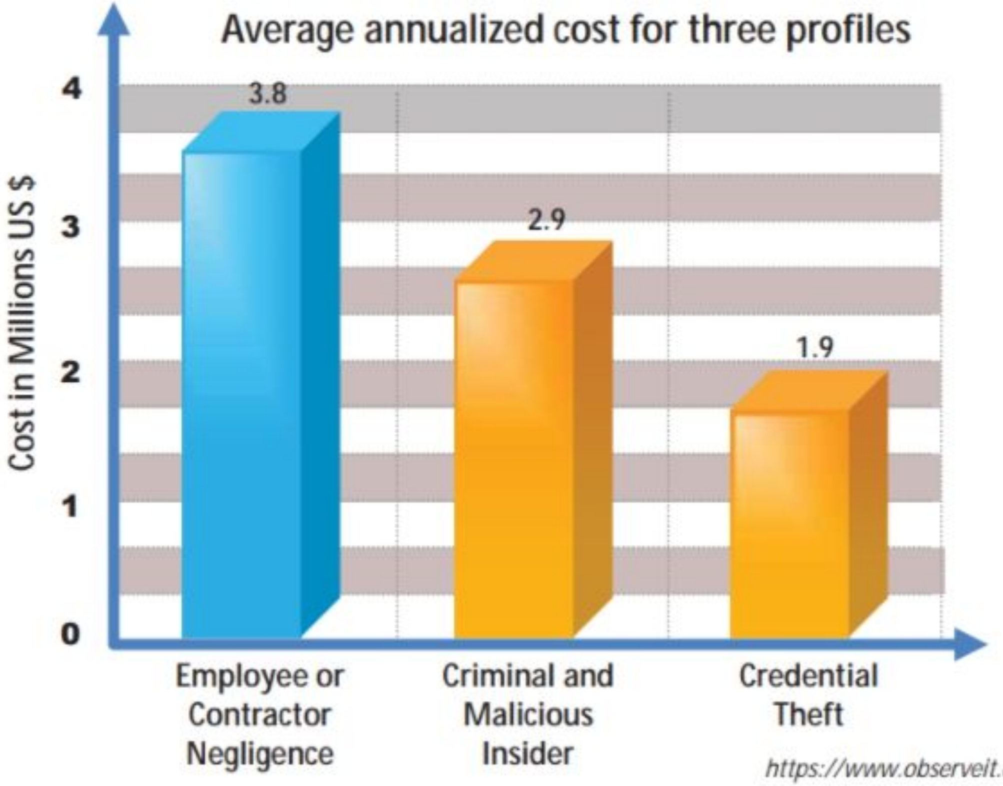
- An insider is any employee (trusted person or people) who have access to critical assets of an organization
- An insider attack involves using privileged access to intentionally violate rules or cause threat to the organization's information or information systems in any form
- Such attacks are generally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

Reasons for Insider Attacks

- Financial gain
- Steal confidential data
- Revenge
- Become future competitor
- Perform competitor's bidding
- Public announcement

Insider Threat Statistics

According to a 2018 Cost of Insider Threats Study, an attack performed by employee or contractor negligence is costlier than criminal or malicious insider attacks and credential theft



https://www.observeit.com

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

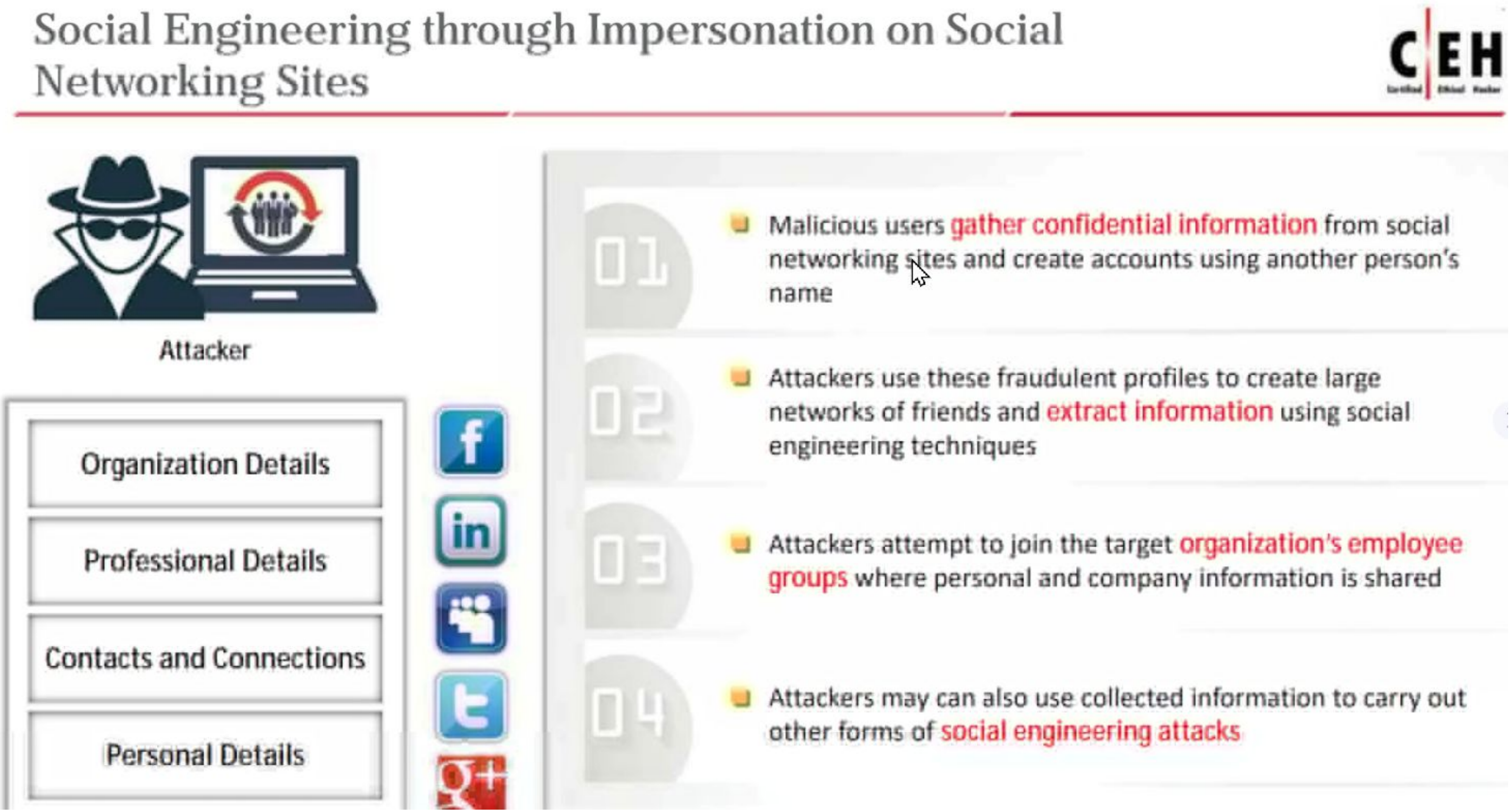
- An insider with access to critical assets of an organization who is compromised by an outside threat actor

Why are Insider Attacks Effective?

- Easy to launch
- Prevention is difficult
- Succeed easily
- Employees can easily cover their tracks
- Differentiating harmful actions from the employee's regular work is very difficult
- Can go undetected for years and remediation is very expensive

Behavioral Indications of an Insider Threat

1. Data exfiltration alerts
2. Missing or modified network logs
3. Changes in network usage patterns
4. Multiple failed login attempts
5. Behavioral and temperament changes
6. Unusual time and location of access
7. Missing or modified critical data
8. Unauthorized downloading or copying of sensitive data
9. Logging of different user accounts from different systems
10. Temporal changes in revenue or expenditure
11. Unauthorized access to physical assets
12. Increase or decrease in productivity of employee
13. Inconsistent working hours
14. Unusual business activities



Social Engineering through Impersonation on Social Networking Sites

Attacker

Organization Details

Professional Details

Contacts and Connections

Personal Details

01 Malicious users **gather confidential information** from social networking sites and create accounts using another person's name

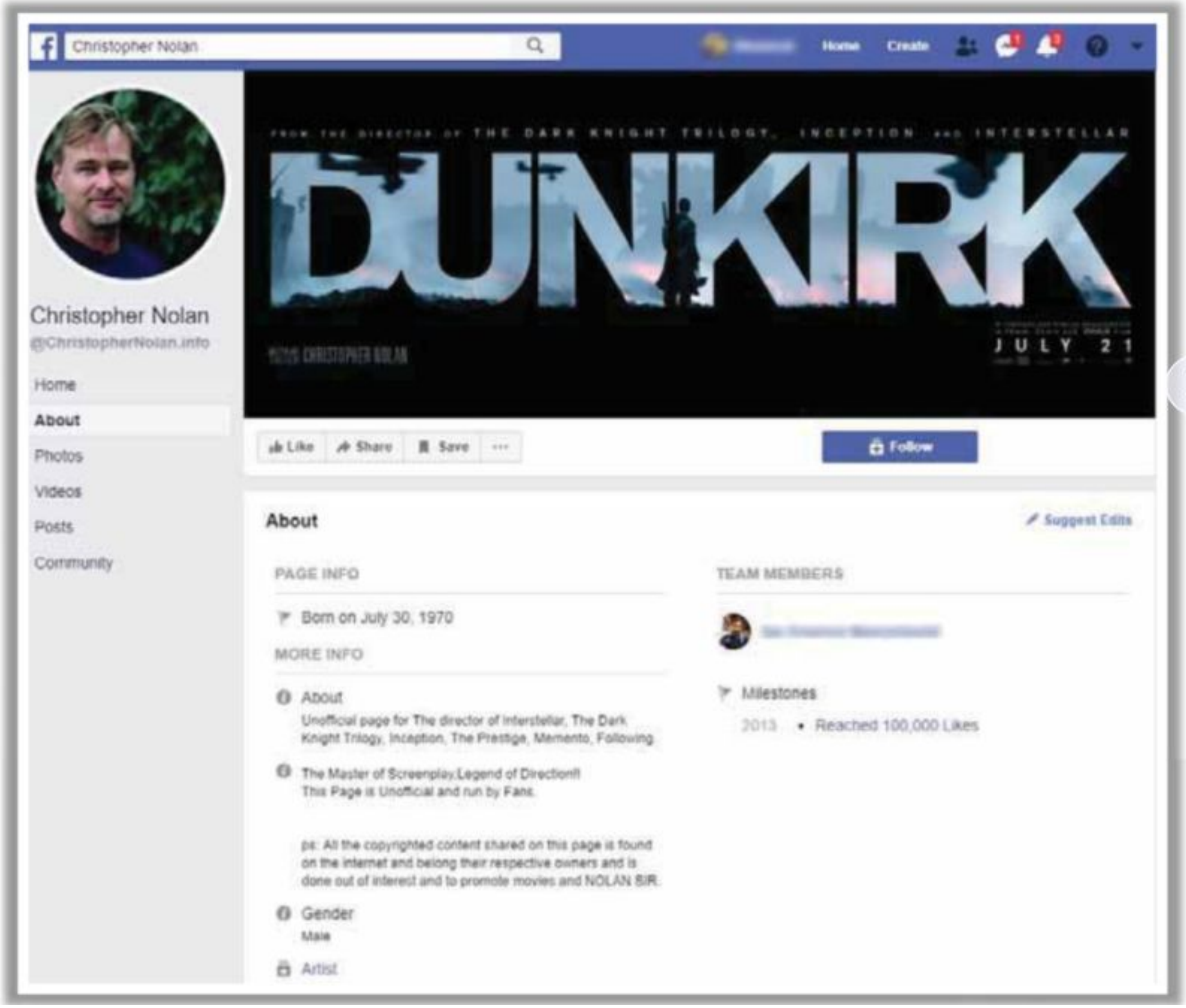
02 Attackers use these fraudulent profiles to create large networks of friends and **extract information** using social engineering techniques

03 Attackers attempt to join the target **organization's employee groups** where personal and company information is shared

04 Attackers may can also use collected information to carry out other forms of **social engineering attacks**

Impersonation on Facebook

- The attacker creates a fake user group on Facebook labeled as for “Employees of” the target company
- Using a false identity, the attacker then proceeds to "friend" or invite employees to the fake group
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, spouses’ names, etc.
- Using the details of any of these employees, the attacker can compromise a secured facility to gain access to the building
- Attackers scan details in profile pages. They use these for spear phishing, impersonation, and identity theft



Christopher Nolan
@ChristopherNolan.info

About

PAGE INFO

Born on July 30, 1970

MORE INFO

About
Unofficial page for The director of interstellar, The Dark Knight Trilogy, Inception, The Prestige, Memento, Following

The Master of Screenplay,Legend of Direction!!
This Page is Unofficial and run by Fans.

ps: All the copyrighted content shared on this page is found on the internet and belong their respective owners and is done out of interest and to promote movies and NOLAN SIR.

Gender
Male

Artist

TEAM MEMBERS

[redacted]

Milestones
2013 • Reached 100,000 Likes

Social Networking Threats to Corporate Networks

1. Data Theft
2. Involuntary Data Leakage
3. Targeted Attacks
4. Network Vulnerability
5. Spam and Phishing
6. Modification of Content
7. Malware Propagation
8. Damage to Business Reputation
9. Infrastructure and Maintenance Costs
10. Loss of Productivity

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

Types of Identity Theft

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver's license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning and Concealment
- Synthetic identity theft
- Social security identity theft

Social Engineering Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies
- The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and secure policies, plans, and processes

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

Social Engineering Countermeasures (Cont'd)

1. Train individuals on security policies
2. Implement proper access privileges
3. Presence of proper incidence response time
4. Availability of resources only to authorized users
5. Scrutinize information
6. Background check and proper termination process
7. Anti-virus/anti-phishing defenses
8. Implement two-factor authentication
9. Adopt documented change management
10. Ensure software is regularly updated