Social Engineering 101 – Bootcamp

By Afshan Naqvi

About me

Cyber Security Research Engineer – Cyber Life

Instructor - SOC Experts & Securzy.io

Member - Breaking Barriers Women in Cyber Security

Content Creator – AFS Hackers - Afshan (YouTube Channel)

Afshan Naqvi

Agenda - Day 1

- What is Social Engineering?
- Phases of Social Engineering
- Common Targets of Social Engineering
- Different types of Social Engineers
- How to gather information about the target?
- Social Engineering Attack
- Emotions Used in Social Engineering Attacks
- Phishing Email Sample
- Best Practices to Prevent Social Engineering Attacks
- Reconnaissance: Google Dorking and Shodan

Agenda - Day 2

- Reconnaissance
- Search Engines: Google Dorking and Shodan
- Social Engineering Toolkit (SEToolKit)
- Maltego
- theHarvester – [Updated tutorial]
- Recon-ng – [Updated tutorial]

What is Social Engineering?

According to NIST,

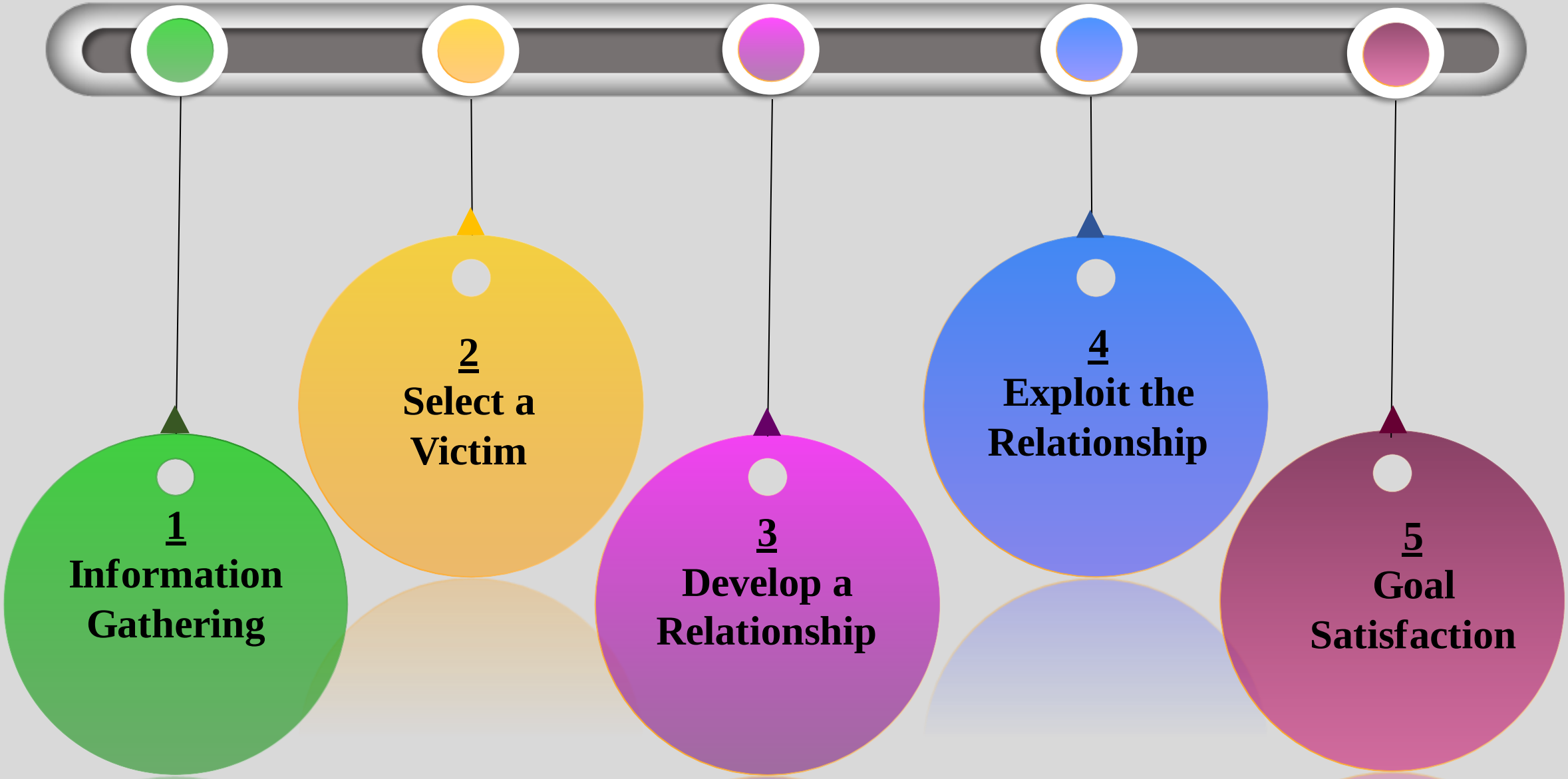
An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

OR

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps.

Phases of a Social Engineering



Phase 1 – Information Gathering

Information gathering is necessary when performing any type of cybersecurity task because it gives the user more knowledge about target systems and networks in order to make an informed decision on how they want to proceed with their attack vector.

Social engineering information gathering process often includes:

1) **Passive reconnaissance**
2) **Active reconnaissance**
3) **Physical reconnaissance**

Phase 1 – Information Gathering

1) Passive reconnaissance

Passive reconnaissance is an attempt to gain information about targeted computers and networks without actively engaging with the systems.

Passive recon tools:

1. **Shodan**
2. **Google**
3. **Google dork**
4. **Wappalyzer**
5. **Whois**

Phase 1 – Information Gathering

2) Active reconnaissance

In active reconnaissance, in contrast, the attacker engages with the target system, typically conducting a port scan to find any open ports.

Active recon tools:

1. **Nmap**
2. **Nikto**
3. **Nessus**
4. **Metasploit**

Phase 1 – Information Gathering

3) Physical reconnaissance

If the exercise is going to be partly conducted onsite, it is imperative to familiarize yourself with that environment.

Some questions to bear in mind while doing physical reconnaissance:

- **What are the employees wearing?**
- **What are the normal office hours?**
- **Employees ID cards.**

Phase 1 – Information Gathering

How to gather information?

1) Gathering information from Websites

Spending some quality time with the site can lead to clearly understanding:

- **What they do**
- **The products and services they provide**
- **Physical locations**
- **Contact numbers**
- **Job openings**
- **Board of Directors and Employees detail**
- **Support forum**
- **Email naming conventions**

Phase 1 – Information Gathering

How to gather information?

2) Search Engines

Web crawlers can be used to fetch information about anything, and this includes companies, persons, services, and even real hacks.

3) Social Media:

Many companies have embraced social media. It's cheap marketing that touches a large number of potential customers. Facebook, Twitter, LinkedIn and other social networks are great sources of information to build a profile, especially when targeting individuals.

4) User sites, Blogs, and YouTube channel: user sites such as blogs, wikis, and online videos may provide not only info about the target company but also offer the personal details and connections.

5) Simple Observation

Phase 2 – Select a Victim or Group

On the basis of the investigation attacker select a victim or a group of non-technical people. They are weakest link in the organization because they're not well aware of the social engineering term so it will be very easy for an attacker to fool them and gather sensitive information.

Name: **Dark Shadow**
Job title: Salesperson
Company: Evil Eye

Name: **Black Shadow**
Job title: Security Analyst
Company: Evil Eye

Phase 3 – Develop relationship

In this step attacker trying to develop a relationship with a victim on Social media such as LinkedIn, Facebook, and maybe face to face contact.

This is a critical point, as the quality of the relationship dictates the level of collaboration and the lengths to which the target will go to assist the attacker in achieving the attacker's aim.

In this step, an attacker can connect on a personal level on phone or in-person meeting. They can also build an online relationship with the target through a fake profile on a dating site or social networking site.

Phase 4 – Exploit Relationship

This is when the attacker uses both information and relationships to actively infiltrate the target. In this phase, the attacker focuses on maintaining the momentum of compliance established in phase 2 without raising suspicion.

Examples of successful exploitation include:

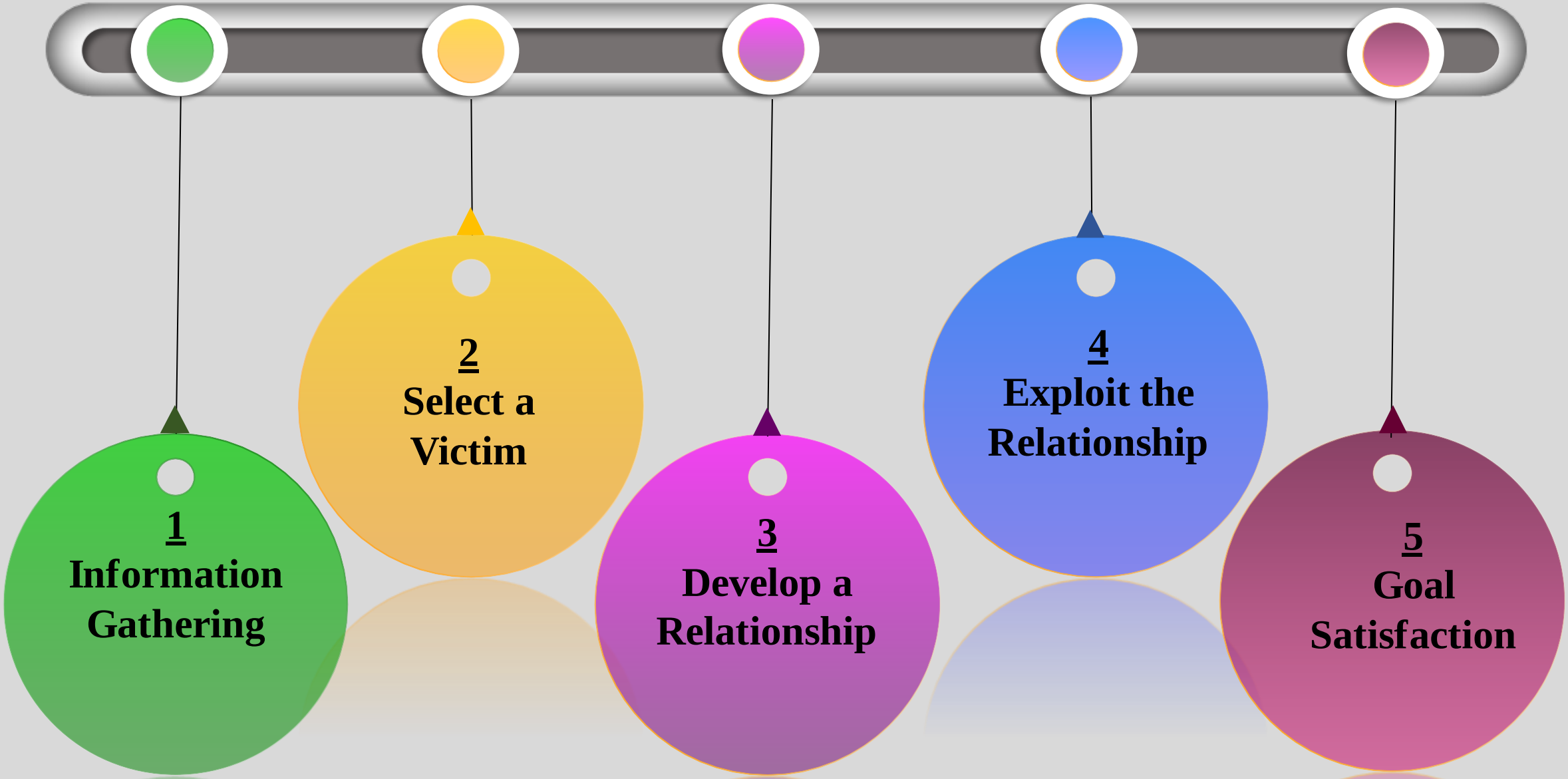
- **The act of holding the door open or otherwise allowing the attacker inside the facilities**
- **Disclosing password and username over the phone**
- **Inserting a USB drive with a malicious payload to a company computer**
- **Opening an infected email attachment**

Phase 5 – Goal Satisfaction

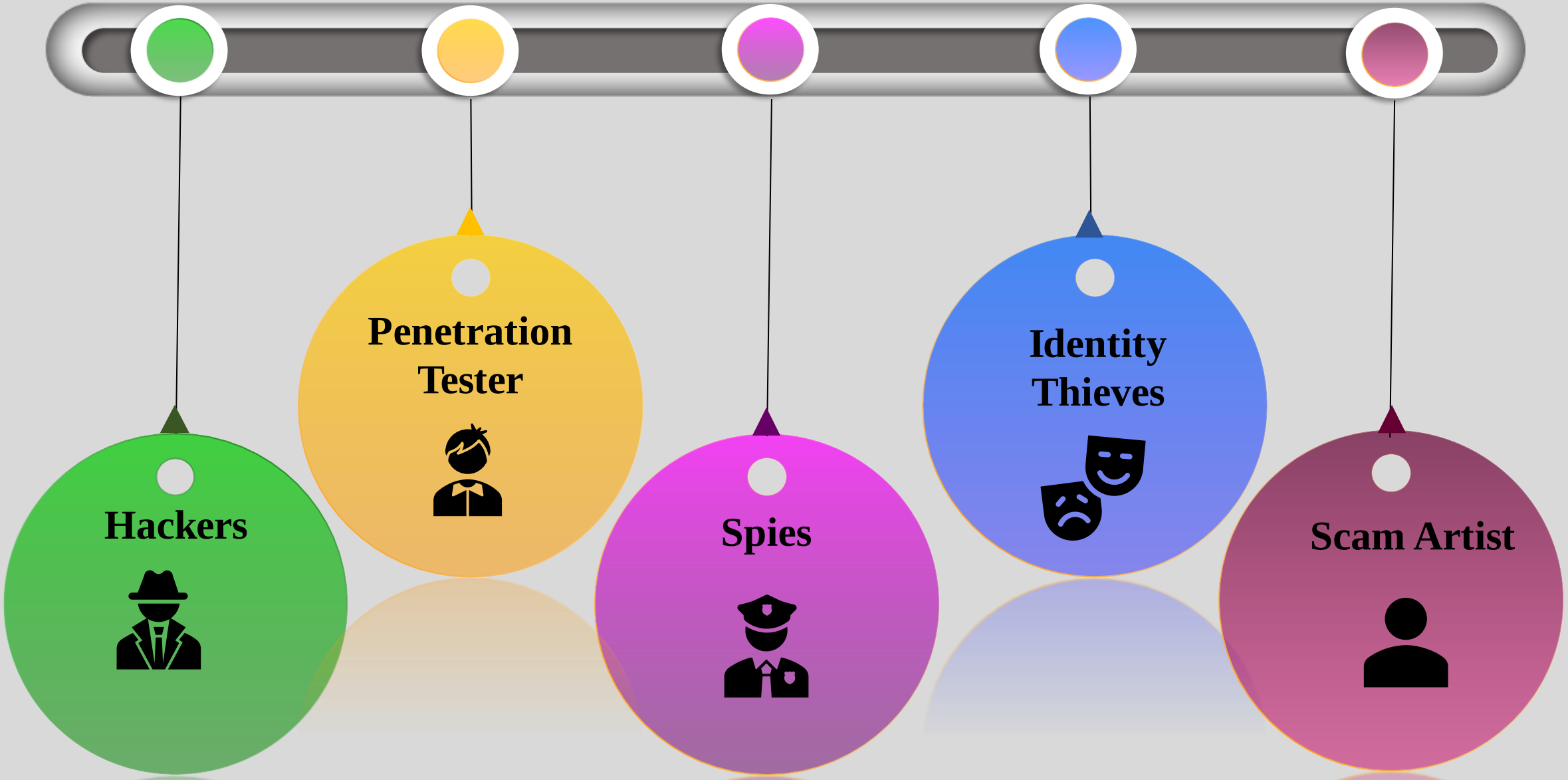
If the goal is achieved in the exploitation phase, the interactions need to be closed down without any suspicions. The objective is to end the engagement without getting noticed by the target. It's important to end the interactions as naturally as possible.

In addition, the attacker erases digital footprints and ensures no items or information are left behind. As a result, the attacker accomplishes two important goals. First, the target does not know an attack took place. Second, the attacker keeps his/her identity hidden. A well-planned and smooth exit strategy is the attacker's goal and final act in the attack.

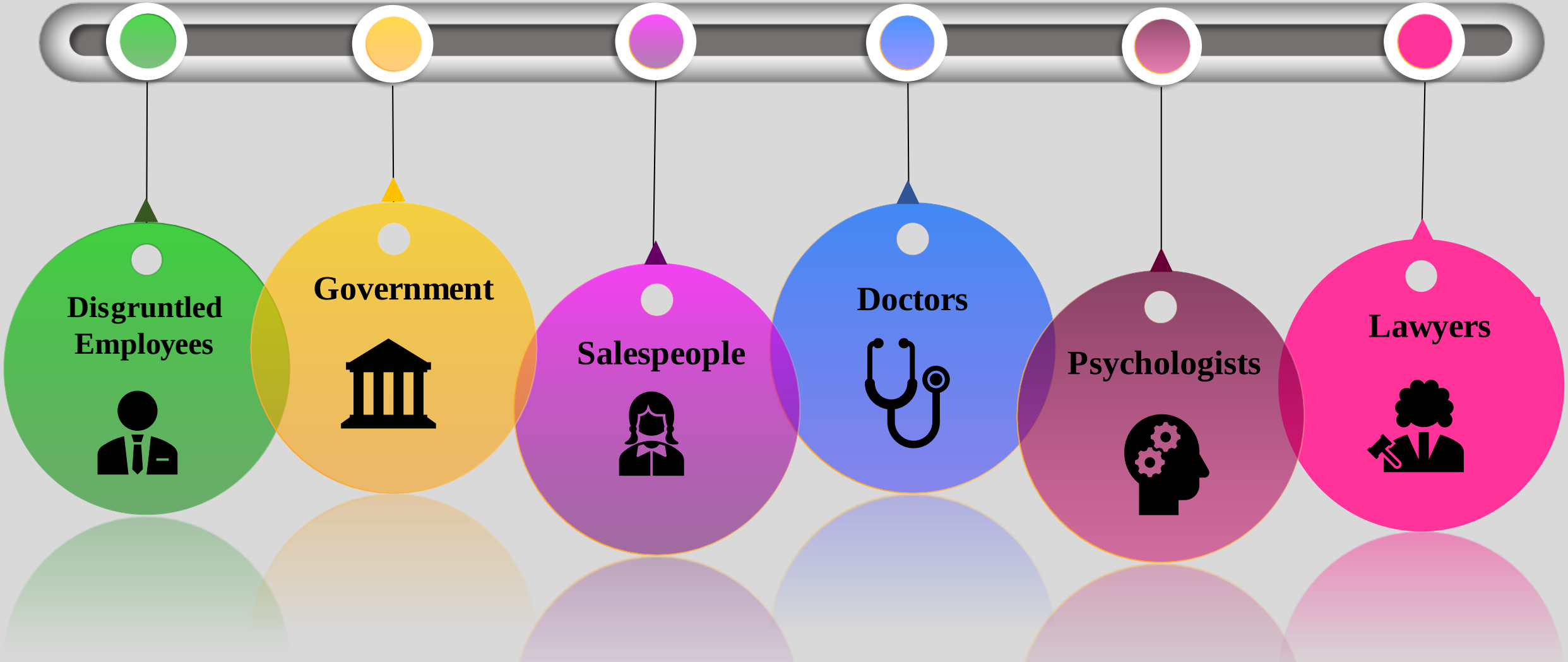
Phases of a Social Engineering



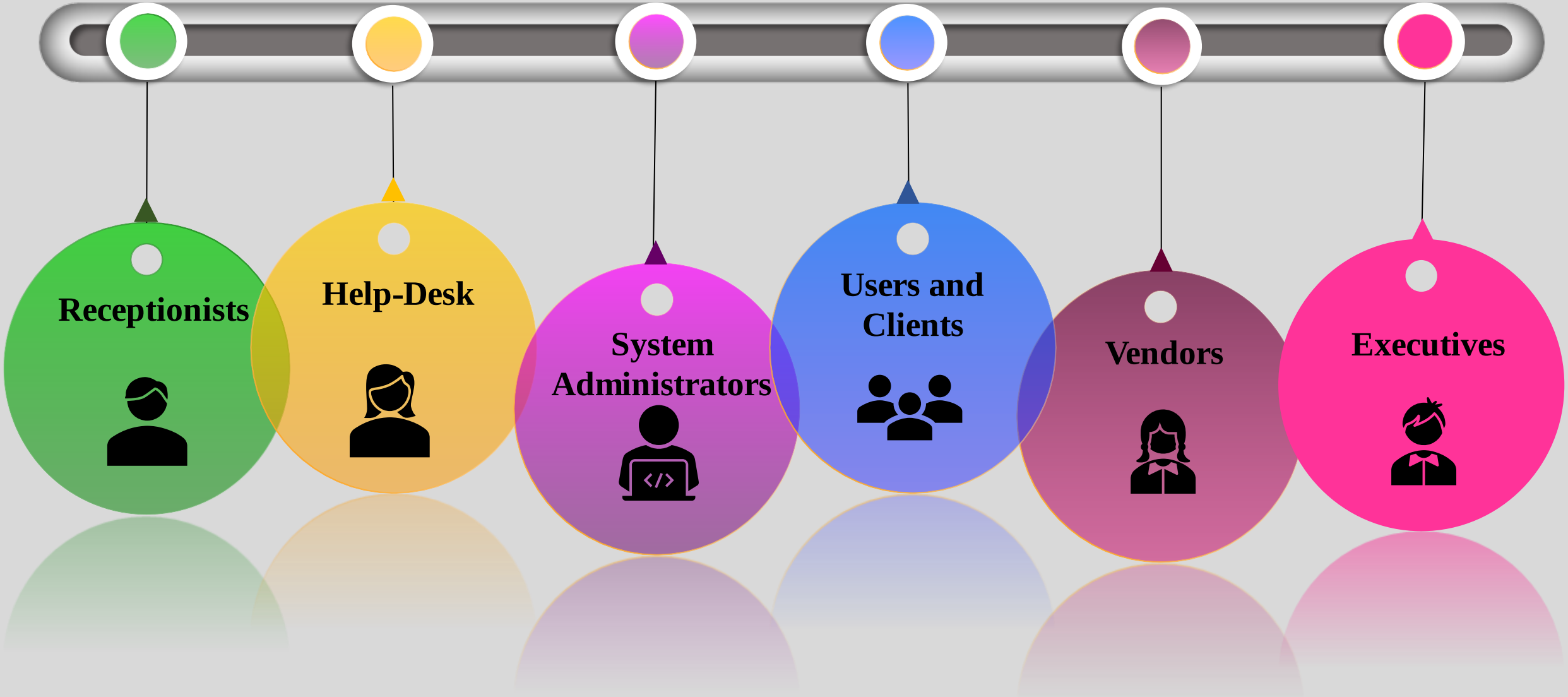
Different types of Social Engineers



Different types of Social Engineers



Common Targets of Social Engineering



Types of Social Engineering Attack

computer-based social engineering relies on computers and Internet. Computer-based social engineering attacks usually include sending email attachments containing malicious code, data collection through fake websites and pop-up windows.

Human-based social engineering involves human interaction. Social engineer can perform attacks by gaining information through communications, impersonation, and dumpster diving. Such attacks are known to be human-based social engineering.

Social Engineering Online Attack Types

01

Phishing

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information.

02

Whaling

A phishing attack that is specifically aimed at wealthy, powerful, or famous individuals.

03

Vishing

Vishing is short for "voice phishing, "which involves making phone calls or leaving voice messages pretending to be from reputable companies.

04

Smishing

Sending fraudulent text messages pretending to be from reputable companies.

05

Pop-Up Windows

Pop-ups trick users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, trojans, or spyware.

06

Spear Phishing

This type of phishing targets a specific person or organization.

Social Engineering Online Attack Types

07

Pharming

It is an online fraud that involves the use of malicious code to direct victims to spoofed websites in an attempt to steal their credentials and data.

02

Quid Pro Quo

Social engineering attack where a hacker promises a profit in exchange for information that can later be used to steal money, data, or take control of a user account on a website

03

Baiting

Phishing attacks that invite users to click on a link to get free stuff.

Social Engineering Offline Attack Types

01

Tailgating

Gaining entry to electronically locked system is to follow someone through the door they just unlocked.

02

Dumpster Diving

Dumpster diving involves looking in the trash for any valuable information, like data written on pieces of paper or computer printouts.

03

Shoulder Surfing

Watching someone "over their shoulder" when they enter sensitive data such as password or credit card information.

04

Pretexting

The act of creating an invented scenario in order to persuade a targeted victim to release information or perform some action.

05

Eavesdropping

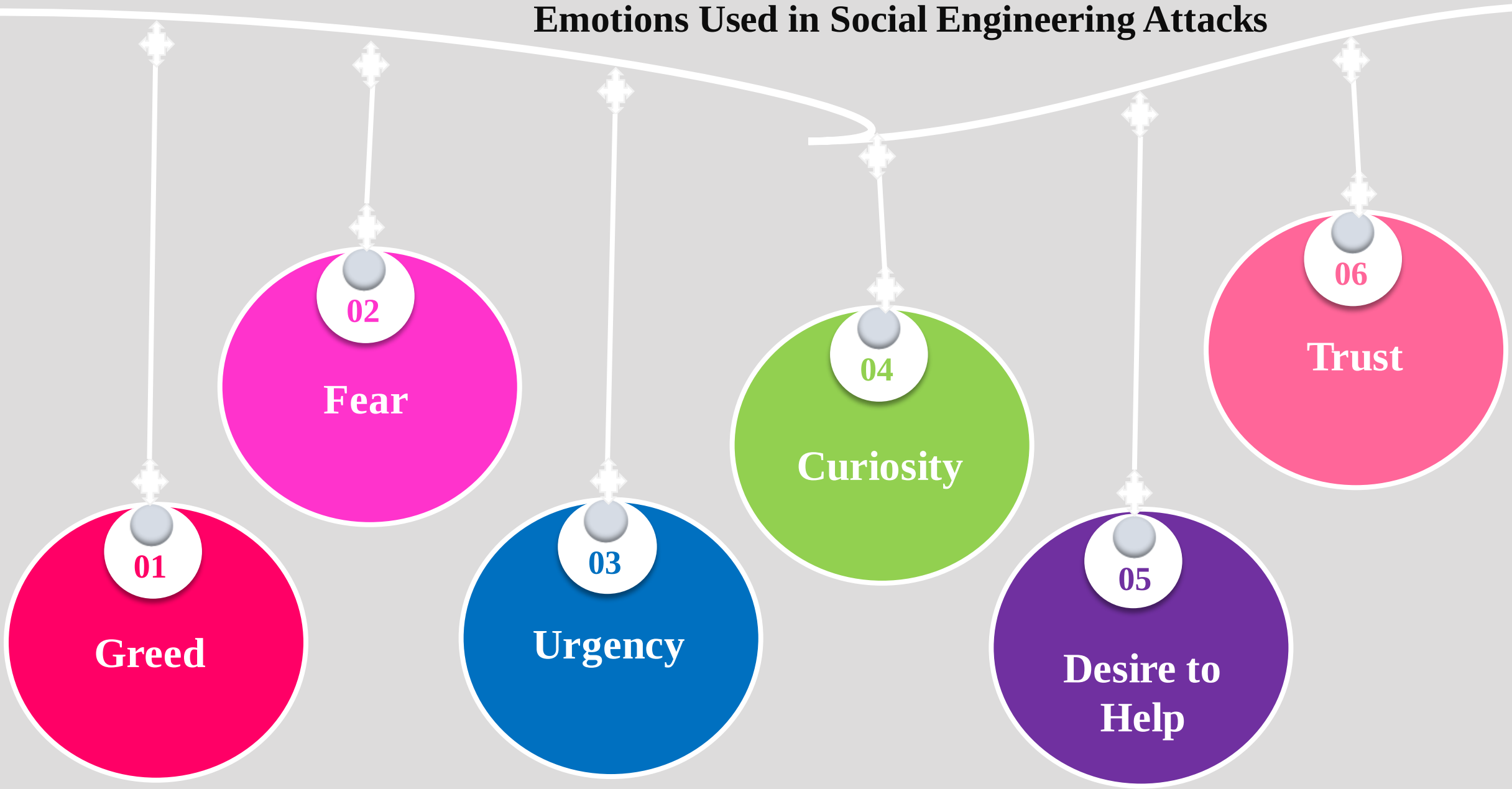
The act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information.

06

Piggybacking

An authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door.

Emotions Used in Social Engineering Attacks



Ways to detect phishing email 

1. The domain name is misspelt. (netflix→netfIx)
2. The email is poorly written.
3. It includes suspicious attachments or links.
4. The message creates a sense of urgency.
5. The message is sent from a public email domain (@gmail.com)
6. A generic greeting is used in place of a name. (dear customer, dear user, Hi mam/Sir)
7. Links in the body message do not match the sender's domain.

Phishing Email Samples

Urgency

1 Urgency

Subject: Urgent! Your order has been cancelled!

Dear Amazon Customer,

Your recent order in AMAZON.COM has bin canceled due to fraudulent activity detected by our automatic systems. Your account has been suspended on a temprary bases.

Youre requested to activate yur account by verifying email and payment information.

Click the link below to log in to Amazon accout and complete the process

https://www.amazon.com/account-verification

Thanks for using Amazon!

From: CustomerService@annazon.net

To: ken@gmail.com

Urgency

Subject: Urgent! Your order has been cancelled!

Dear Amazon Customer,

Your recent order in AMAZON.COM has bin canceled due to fraudulent activity detected by our automatic systems. Your account has been suspended on a temprary bases.

Youre requested to activate yur account by verifying email and payment information.

Click the link below to log in to Amazon accout and complete the process

https://www.amazon.com/account-verification

Thanks for using Amazon!

From: CustomerService@annazon.net

To: ken@gmail.com

2
Urgency

Subject: Invoice Failed - Account Blocked

Dear Customer,

We are having some trouble with your current billing information. we will try again, but in the mean time you may want to update your MASTERCARD in your payment details.

https://www.netflix.com/account-update

We are here to help if you need it. Visit the help Centre for more info or contact us.

Thanks for using Netflix!

NETFLIX

From: subscriptions@netflix.com

To: josh@gmail.com

2
Urgency

Subject: Invoice Failed - Account Blocked

Dear Customer,

We are having some trouble with your current biling information. we will try again, but in the mean time you may want to update your MASTERCARD in your payment details.

https://www.netflix.com/account-update

We are here to help if you need it. Visit the help Centre for more info or contact us.

Thanks for using Netflix!

NETFLIX

From: subscriptions@netflix.com

To: josh@gmail.com

Fear

3
Fear

Subject: Urgent! Your account has been disabled.

Dear Rohan,

Due to suspicious recent activity, **YOUR ACCOUNT HAS BEEN DISABLED TEMPORARILY.**

When you are in a secure location, please download the attachment and review the included transactions. The reply back to this message, letting us know if this activity was yours.

Thank you for you prompt attention to this matter.

SBI Bank Team

Scanned and Cleaned by AntiVirus

Attachment: transaction.exe

SBI

From: costomercare@sbii.co.in

To: rohan@gmail.com

3
Fear

Subject: Urgent! Your account has been disabled.

Dear Rohan,

Due to suspicious recent activity, **YOUR ACCOUNT HAS BEEN DISABLED TEMPORARILY.**

When you are in a secure location, please download the attachment and review the included transactions. The reply back to this message, letting us know if this activity was yours.

Thank you for you prompt attention to this matter.

SBI Bank Team

Scanned and Cleaned by AntiVirus

Attachment: transaction.exe

From: costomercare@sbii.co.in

To: rohan@gmail.com

4
Fear

Dear valued customer,

We have received notice that you have recently attempted to withdraw $500 in another country.

If this information is not correct, then please visit our website via the link below to verify your personal information.

http://www.canara.com/general/verifinfo.asp

Once you done this, our fraud department will work to resolve this discrepancy.

Thanks for choosing Canara bank

Canara Bank
A Government of India Undertaking

From: costomercare@cenera

To: rohan@gmail.com

4
Fear

Dear valued customer,

We have received notice that you have recently attempted to withdraw $500 in another country.

If this information is not correct, then please visit our website via the link below to verify your personal information.

http://www.canara.com/general/verifinfo.asp

Once you done this, our fraud department will work to resolve this discrepancy.

Thanks for choosing Canara bank

Canara Bank
A Government of India Undertaking

From: costomercare@cenara

To: rohan@gmail.com

Greed

5 Greed

Subject: 5000 Rupees Credited to your account.

Dear Kotak Customer,

5000 Rupees credited to you bank account.

Click the following link to see the transaction history.

https://www.katak.com/transaction_history

Thanks for using Kotak!

kotak
Kotak Mahindra Bank

From: costomerfirst@katak.com

To : Samanfatima@gmail.com

5 Greed

Subject: 5000 Rupees Credited to your account.

Dear Kotak Customer,

5000 Rupees credited to you bank accont.

Click the folowing link to see the transaction history.

https://www.kotak.com/transaction_history

Thanks for using Kotak!

kotak
Kotak Mahindra Bank

From: costomerfirst@katak.com

To : Samanfatima@gmail.com

6 Greed

Dear Paypal user,

We haven't seen you in awhile.

Youve been rewarded $500 dollars to you account. All you need to do is sign in to your paypal account with this link to claim your prize!

Claim $500 NOW

Time is running out and we'd love to see you back online. Hurry and claim your $$ today!

PayPal

From: peypal@notfake.peypal.com

To : anjali@gmail.com

6 Greed

Dear Paypal user,

We haven't seen you in awhile.

Youve been rewarded $500 dollars to you account. All you need to do is sign in to your paypal account with this link to claim your prize!

Claim $500 NOW

Time is running out and we'd love to see you back online. Hurry and claim your $$ today!

PayPal

From: peypal@notfake.peypal.com

To : anjali@gmail.com

Desire to Help

7
Help

Subject: HELP UKRAIN - stop the War!

Army of Ukraine need your support! please help us defend our freedom an independance!

The National Bank of Ukraine has decided to open a special fundraising account to support the Armed Foreces of Ukraine.

PLEASE, DO NOT IGNORE THIS MESSAGE!

Stand with the people of Ukraine.

Now, we are accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - 123457890010

ETH and USDT - 123456789010

Thank you for your support.

From: helpukrain@gmail.com

To : ali@gmail.com

7
Help

Subject: HELP UKRAIN - stop the War!

Army of Ukraine need your support! please help us defend our freedom an independance!

The National Bank of Ukraine has decided to open a special fundraising account to support the Armed Foreces of Ukraine.

PLEASE, DO NOT IGNORE THIS MESSAGE!

Stand with the people of Ukraine.

Now, we are accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - 123457890010

ETH and USDT - 123456789010

Thank you for your support.

From: helpukrain@gmail.com

To : ali@gmail.com

8
Help

Dear sir,

Go through the attachment document on saftey measures regarding the spreading of corona virus.

Click on the button below to download

Click here

share this info with your family and friends.

Symptoms comon symptoms include fever, cough, shortness of breath and breathing difficulties.

World Health Organization

From: who.health@worldhealth.com

To : lucy@gmail.com

8 Help

Dear sir,

Go through the attachment document on saftey measures regarding the spreading of corona virus.

Click on the button below to download

Click here

please share this info with your family and friends.

Symptoms comon symptoms include fever, cough, shortness of breath and breathing difficulties.

World Health Organization

From: who.health@worldhealth.com

To : lucy@gmail.com

Tips to prevent phishing scam

1. Check for typos.
2. Check the domain name carefully.
3. Don’t share sensitive information.
4. Don’t fall for URGENCY!
5. Hover over the link but DO NOT CLICK on it.
6. Regularly check your accounts.
7. Keep your devices up to date.
8. Don’t open attachments from unknown sources.

Best Practices to Prevent Social Engineering Attacks

No. 01 Set a spam filter to high.

No. 02 Never use the same password for different accounts.

No. 03 Use two-factor or multi-factor authentication.

No. 04 When in doubt, change passwords right away.

No. 05 Keep your antivirus/antimalware software updated

No. 06 Don’t open emails and attachments from suspicious sources

Best Practices to Prevent Social Engineering Attacks

No. 07 Create a "strong" password with at least 8 characters that includes a combination of mixed case letters and numbers.

No. 08 Don’t make it easy for hackers to compromise multiple accounts by using the same password. Change your password frequently and don't use the same password for all of your account.

No. 09 Avoid using public Wi-Fi when transmitting sensitive data.

No. 10 Never leave a computer unattended while using Online Banking.

No. 11 Never conduct banking transactions while multiple browsers are open on your computer.

No. 12 Only use sites that contain HTTPS in the address.

Best Practices to Prevent Social Engineering Attacks

No. 13 Never share username and password information with third-party providers.

No. 14 Avoid using an automatic login feature that saves usernames and passwords.

No. 15 Keep yourself informed about new cybersecurity risks

No. 16 If you get a message from your bank, whether it be a pop-up, on a webpage, an email, or a text, don't click the link. Instead, open a new browser window, type the address of your bank, and log in completely independently from that link that was sent to you.

No. 17 Don’t download software or content from untrustworthy sites

No. 18 Read the privacy policy of a website before providing personal information

1

Knowledge Check

You receive a text message from your bank stating that your account has been locked due to fraudulent activity, and to unlock it you need to click a link and log in. What should you do next?

A. Delete the message and call your bank directly to confirm.
B. Forward the text to a friend and see if they think it's suspicious.
C. Click the link so you can fix your account.
D. none of the above

1

Knowledge Check

You receive a text message from your bank stating that your account has been locked due to fraudulent activity, and to unlock it you need to click a link and log in. What should you do next?

A. **Delete the message and call your bank directly to confirm.**
B. **Forward the text to a friend and see if they think it's suspicious.**
C. **Click the link so you can fix your account.**
D. **None of the above**

2

Knowledge Check

What type of social engineering involves the criminal pretending to be a delivery person, and they need to be let into the building?

A. Shoulder Surfing
B. Piggybacking
C. Pretexting
D. Phishing

2

Knowledge Check

What type of social engineering involves the criminal pretending to be a delivery person, and they need to be let into the building?

A. Shoulder Surfing
B. Piggybacking
C. Pretexting
D. Phishing

3

Knowledge Check

How can you protect your PIN number at a cash machine from a criminal using "shoulder surfing"?

A. Cover your pin as you enter it
B. Use the cash machine in daylight
C. Get cash back from a shop
D. none of the above

3

Knowledge Check

How can you protect your PIN number at a cash machine from a criminal using "shoulder surfing"?

A. **Cover your pin as you enter it**
B. **Use the cash machine in daylight**
C. **Get cash back from a shop**
D. **none of the above**

4

Knowledge Check

What information are scammers looking to gain through social engineering?

A. Bank details
B. Passwords
C. Address details
D. All of above

4

Knowledge Check

What information are scammers looking to gain through social engineering?

A. Bank details
B. Passwords
C. Address details
D. All of above

5

Knowledge Check

How could you mitigate against phishing?

A. Type carefully
B. Hide typing
C. Not giving away login information
D. Read an email very carefully before clicking any links

5

Knowledge Check

How could you mitigate against phishing?

A. Type carefully
B. Hide typing
C. Not giving away login information
D. **Read an email very carefully before clicking any links**

6

Knowledge Check

What is the type of social engineering that promises goods in return for you entering your personal information?

A. Quid Pro Quo
B. Pretexting
C. Baiting
D. Phishing

6

Knowledge Check

What is the type of social engineering that promises goods in return for you entering your personal information?

A. Quid Pro Quo
B. Pretexting
C. Baiting
D. Phishing

7

Knowledge Check

What type of social engineering involves the attacker offering something, like a favor, in exchange for access to some personal information?

A. Quid Pro Quo
B. Pharming
C. Shoulder Surfing
D. Phishing

7

Knowledge Check

What type of social engineering involves the attacker offering something, like a favor, in exchange for access to some personal information?

A. **Quid Pro Quo**
B. **Pharming**
C. **Shoulder Surfing**
D. **Phishing**

8

Knowledge Check

You receive a call from “Credit Services.” The person on the line compliments you on your great credit history and also informs you that you have qualified for a card with better features and a lower rate. They’ll only need a few minutes of your time to go over some personal information before they can get the card out to you. Which of the following is the biggest red flag in this scenario?

A. You'll have to provide personal information.
B. They'll only need a few minutes of your time.
C. You have qualified for a credit card.
D. You received a call from "Credit Services."

8

Knowledge Check

You receive a call from “Credit Services.” The person on the line compliments you on your great credit history and also informs you that you have qualified for a card with better features and a lower rate. They’ll only need a few minutes of your time to go over some personal information before they can get the card out to you. Which of the following is the biggest red flag in this scenario?

A. **You'll have to provide personal information.**
B. **They'll only need a few minutes of your time.**
C. **You have qualified for a credit card.**
D. **You received a call from "Credit Services."**

9

Knowledge Check

You receive an email from an online music service you subscribe to. The message indicates there was a problem while processing a recent payment. It also says your account will be deactivated if you don't update your payment information within 60 minutes of reading this message. The bottom of the message includes a reassuring notification that the included link has been scanned and is clean of any viruses. Which of the following is the biggest red flag in this scenario?

A. There was a problem with processing a recent payment.
B. You received an email from your online music service.
C. The included link was scanned for viruses.
D. You'll have to act with 60 minutes of reading the message.

9

Knowledge Check

You receive an email from an online music service you subscribe to. The message indicates there was a problem while processing a recent payment. It also says your account will be deactivated if you don't update your payment information within 60 minutes of reading this message. The bottom of the message includes a reassuring notification that the included link has been scanned and is clean of any viruses. Which of the following is the biggest red flag in this scenario?

A. There was a problem with processing a recent payment.
B. You received an email from your online music service.
C. The included link was scanned for viruses.
D. You'll have to act with 60 minutes of reading the message.

10

Knowledge Check

Someone from the IT department calls you and states that he needs your username and password so the can run an update on your computer. How should you handle this situation?

A. Promptly end the phone call and report the incident to management.
B. Tell him you'll email your username and password to the IT department because that's a safer form of communication.
C. Give him your username and password since updates are a crucial part of security.
D. Put him on hold and ask your co-worker if their computer has been updated.

10

Knowledge Check

Someone from the IT department calls you and states that he needs your username and password so the can run an update on your computer. How should you handle this situation?

A. Promptly end the phone call and report the incident to management.
B. Tell him you'll email your username and password to the IT department because that's a safer form of communication.
C. Give him your username and password since updates are a crucial part of security.
D. Put him on hold and ask your co-worker if their computer has been updated.

11

Knowledge Check

Jennifer receives an email claiming that her bank account information has been lost and that she needs to click a link to update the bank's database. However, she doesn't recognize the bank, because it is not one she does business with. What type of attack is she being presented with?

A. **Phishing**
B. **Spam**
C. **Whaling**
D. **Vishing**

11

Knowledge Check

Jennifer receives an email claiming that her bank account information has been lost and that she needs to click a link to update the bank's database. However, she doesn't recognize the bank, because it is not one she does business with. What type of attack is she being presented with?

A. **Phishing**
B. **Spam**
C. **Whaling**
D. **Vishing**

12

Knowledge Check

A security camera picks up someone who doesn't work at the company following closely behind an employee while they enter the building. What type of attack is taking place?

A. Phishing
B. Walking
C. Gate running
D. Tailgating

12

Knowledge Check

A security camera picks up someone who doesn't work at the company following closely behind an employee while they enter the building. What type of attack is taking place?

A. Phishing
B. Walking
C. Gate running
D. Tailgating

13

Knowledge Check

Jason notices that he is receiving mail, phone calls, and other requests for information. He has also noticed some problems with his credit checks such as bad debts and loans he did not participate in. What type of attack did Jason become a victim of?

A. **Social engineering**
B. **Phishing**
C. **Identity theft**
D. **Bad luck**

13

Knowledge Check

Jason notices that he is receiving mail, phone calls, and other requests for information. He has also noticed some problems with his credit checks such as bad debts and loans he did not participate in. What type of attack did Jason become a victim of?

A. Social engineering
B. Phishing
C. Identity theft
D. Bad luck

14

Knowledge Check

In which of the following, a person is constantly followed/chased by another person or group of several peoples?

A. **Phishing**
B. **Bulling**
C. **Stalking**
D. **Identity theft**

14

Knowledge Check

In which of the following, a person is constantly followed/chased by another person or group of several peoples?

A. Phishing
B. Bulling
C. Stalking
D. Identity theft

Disclaimer

The information provided in this session is to be used for educational purposes only. All of the information in this session is meant to help the audience to develop hacker defense attitude to prevent the attacks. In no way you should use information to cause any kind of damage directly or indirectly. The word "hacks" or "hacking" in this session should be regarded as "Ethical hack" or "Ethical hacking" respectively.

WARNING HACKING IS A CRIME AND WE ARE NOT RESPONSIBLE FOR THE WAY YOU USE IT.

Google Dork

What is Google Dork?

A Google Dork, also known as Google Dorking or Google hacking, is a search string that uses advanced search operators to find information that is not readily available on a website.

Google + Dork = Query

Google Dork

→Google Search Filters

1. site:

If you include [site:] in your query, Google will restrict the results to those websites in the given domain.

Ex. site:microsoft.com

Google Dork

2. intitle:

This will ask google to show pages that have the term in their html title.

Ex. intitle:index

Google Dork

3. inurl:

If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the url.

Ex. inurl:fbi

Google Dork

4. related:

List web pages that are “similar” to a specified web page.

Ex. related:www.google.com

Google Dork

5. filetype:

If you include [filetype:] in your query, Google will search for certain file type.

Ex. filetype:pdf will search for all the pdf files in the websites.

Google Dork

6. ext:

If you include [ext:] in your query, Google will search for certain file extension.

It works similar to filetype.

Ex. ext:pdf - finds pdf extension files.

Google Dork

7. intext:

This will search content of the page. This works similar to the plain google search.

Ex. intext:confidential

Google Dork

8. cache:

The cache: google dork is used to view that cached version of any web document or we can say web page.

Ex. cache:facebook.com

Google Dork

9. inanchor:

This is useful when you need to search for an exact anchor text used on any links.

Ex. inanchor:"password"

Google Dork

10. before/after:

Used to search within a particular date range.

Ex. after:2020

Google Dork

11. allintext:

Searches for specific text contained on any web page.

Ex. allintext: hacking tools

Google Dork

12. lang:

Narrow search by language.

Ex. lang:en
en – English
es – Spanish
ar - Arabic
fr - French

Google Dork

13. "quote"

Find an exact phrase (though results may include related words)
Ex: "Malware Hunting"

Google Dork

14. :info

will show information about the homepage.

Ex. info:www.facebook.com

Google Dork

→Google Search Operators

1. *

This works like a wildcard. Putting an asterisk in a search tells Google ‘I don’t know what goes here’. Basically, it’s really good for finding half remembered song lyrics or names of things.

site:*.com

Google Dork

2. OR (or |)

Return results for either item. The pipe character can be used in place.

Ex: " hermetic wiper OR ransomware "
Ex: "hermetic wiper | ransomware"

Google Dork

3. AND (or &)

Return results with both items. Ampersand character can be used in place.

Ex: " cissp AND certification "
Ex: " cissp & certification "

Google Dork

Practical Time ☺

Shodan

Shodan is a search engine for Internet-connected devices. Shodan is a database of billions of publicly available IP addresses, and it's used by security experts to analyze network security.

How to Install Shodan?

$pip install shodan

Once you have installed shodan CLI tool, setup your API token

$shodan init [API_KEY]

Shodan Help

Once you have installed shodan CLI tool, setup your API token

$shodan init [API_KEY]

$shodan -h

Shodan info

$shodan info

Query credits available: 100
Scan credits available: 100

Note: A search request = 1 query credit
Scanning 1 IP = 1 scan credit

Shodan version

Show the current version number you are using.

$shodan version

Shodan count

Return the number of results for a search query.

$shodan count openssh
28000

$shodan count bigip
50000

Passive recon tools

TheHarvester is used to find email accounts, subdomain names, virtual hosts, open ports / banners, and employee names related to a domain from different public sources (such as search engines and PGP key servers).

Recon-ng is a framework written in python. It comes with powerful environment where we can conduct open source web-based reconnaissance quickly and thoroughly. Recon-ng is incorporated with independent modules, database interaction, functions and interactive help. Recon-ng interface is very similar to Metasploit framework.

SE Learning Resources

A curated list of awesome social engineering resources:

https://github.com/v2-dev/awesome-social-engineering

Social Engineering Course:

https://app.pluralsight.com/course-player?clipId=d8b5b866-a6b7-4532-87fe-6f9ecbba4cf6

SE Learning Resources

Social Engineering Books:

1. Social Engineering: The Art of Human Hacking - Chris Hadnagy

2. Social Engineering: The Science of Human Hacking

3. Unmasking the Social Engineer: The Human Element of Security - Christopher Hadnagy, Dr. Ekman Paul

4. The Art of Deception: Controlling the Human Element of Security, Kevin D. Mitnick, William L. Simon

5. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker - Kevin D. Mitnick, William L. Simon, Steve Wozniak

6. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data - Kevin Mitnick, Robert Vamosi