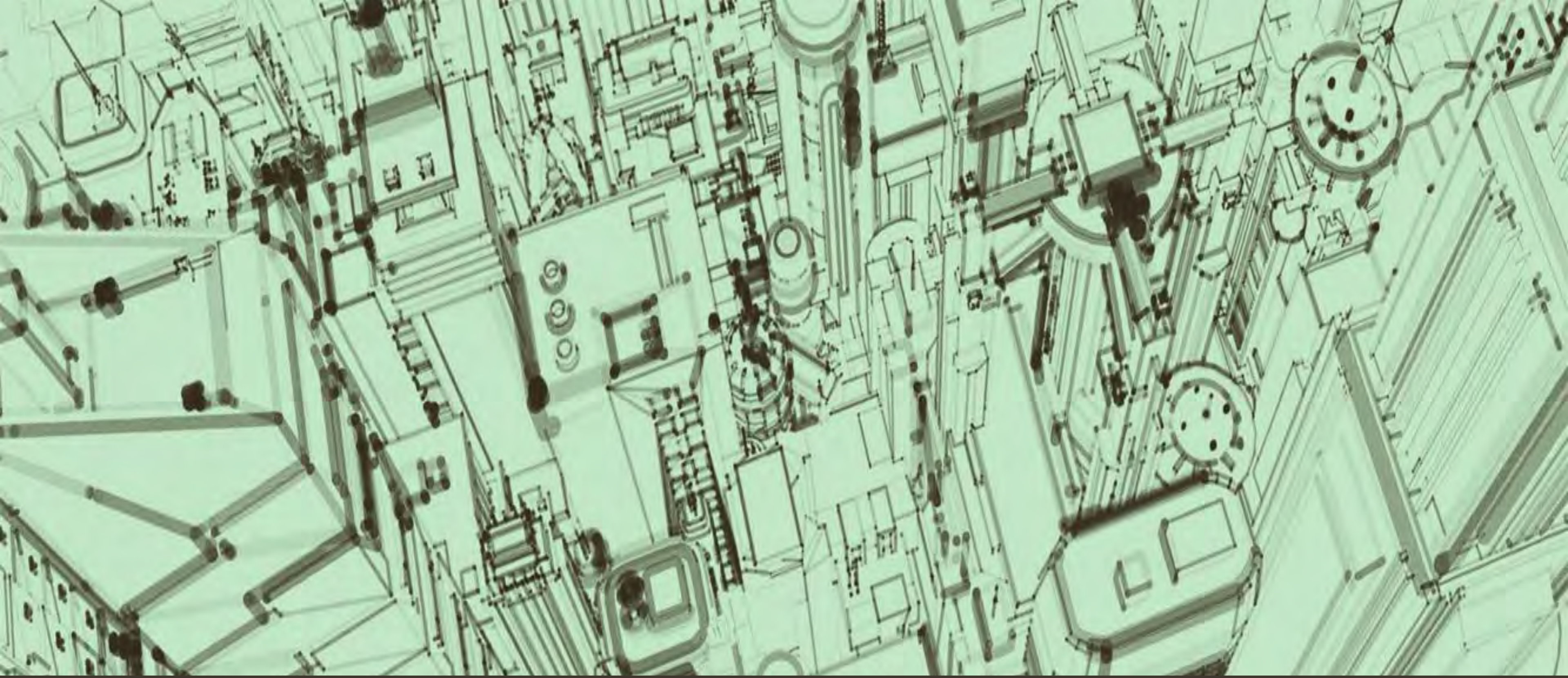


Cyber Security Awareness

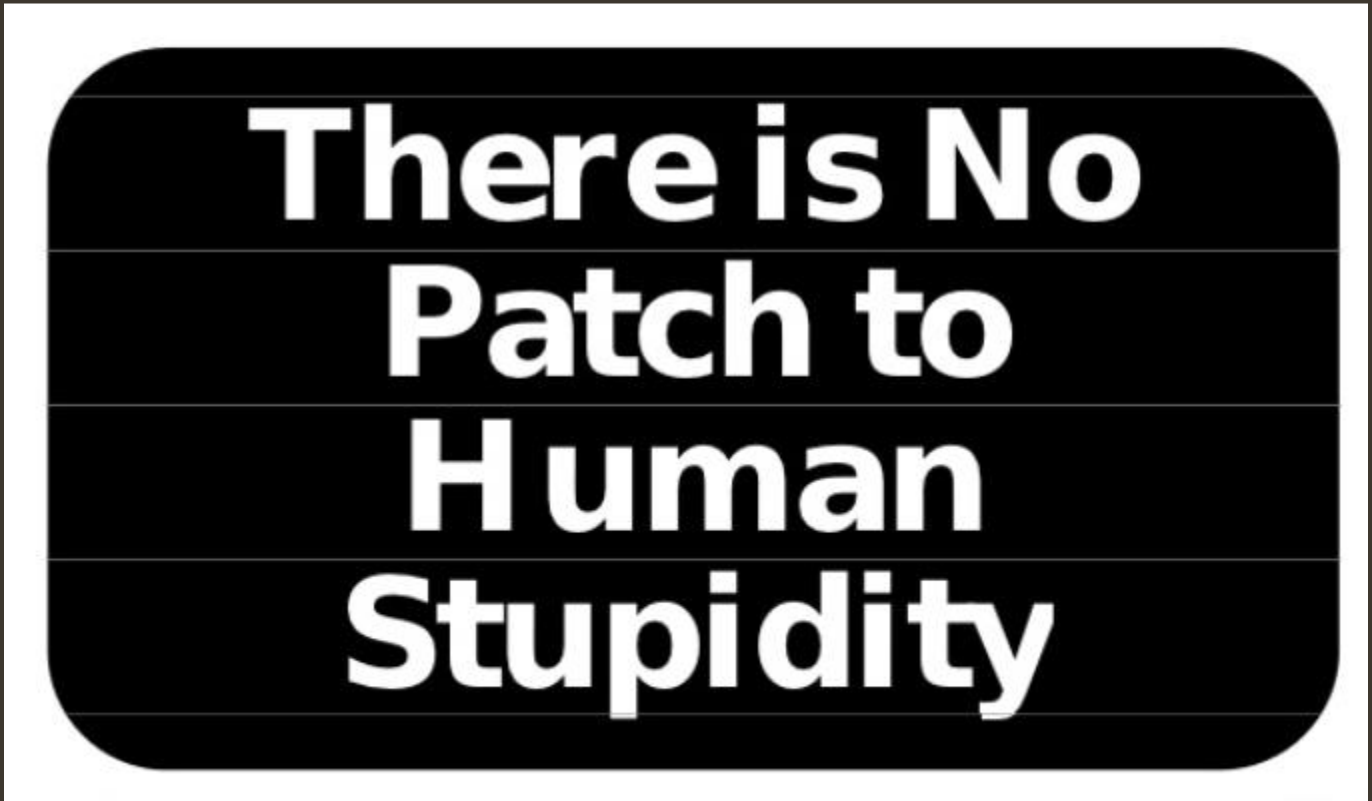
Miftah Rahman Syahrial S.Kom, MT
CCNP, JNCIA, CEH, ITIL4F

Miftah Rahman Syahrial S.Kom, MT
CCNP, JNCIA, CEH, ITIL4F

- **Bachelor Degree at Bina Nusantara University**
- **Master Degree at Mercu Buana University**
- **IT Instructor at Inixindo with Computer Network as its main discipline, with InfoSec Management and IT Service Management as branch discipline**
- **Security Auditor for BestPath Network**
- **Freelance Network Engineer as a part-time job**

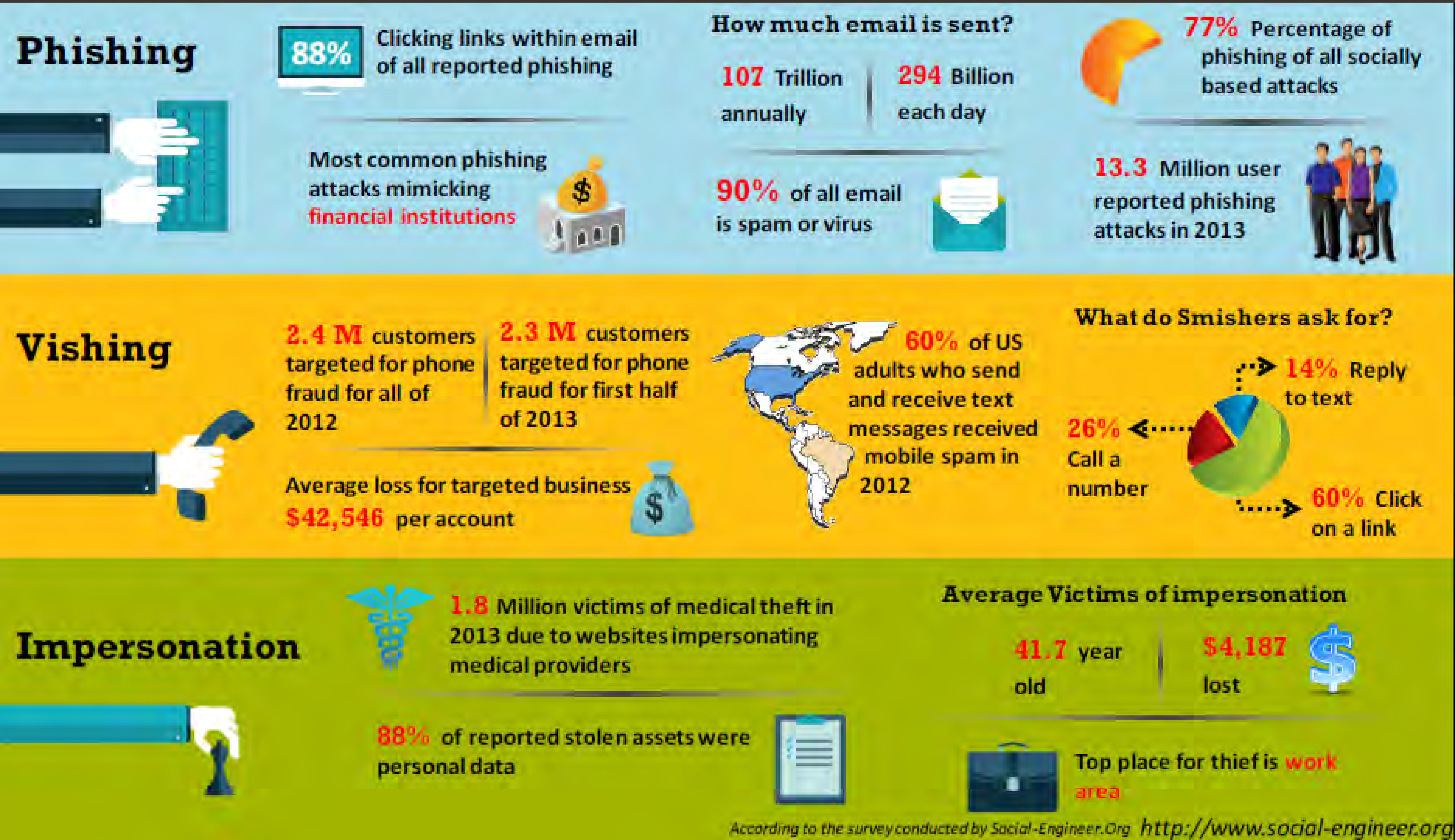
Miftah Rahman Syahrial, S.Kom, MT

IT Network Instructor and a Lecturer



There is No Patch to Human Stupidity

Social Engineering Statistics



Phishing

88% Clicking links within email of all reported phishing

Most common phishing attacks mimicking financial institutions

How much email is sent?

107 Trillion annually | 294 Billion each day

90% of all email is spam or virus

77% Percentage of phishing of all socially based attacks

13.3 Million user reported phishing attacks in 2013

Vishing

2.4 M customers targeted for phone fraud for all of 2012

2.3 M customers targeted for phone fraud for first half of 2013

Average loss for targeted business $42,546 per account

60% of US adults who send and receive text messages received mobile spam in 2012

What do Smishers ask for?

14% Reply to text

26% Call a number

60% Click on a link

Impersonation

1.8 Million victims of medical theft in 2013 due to websites impersonating medical providers

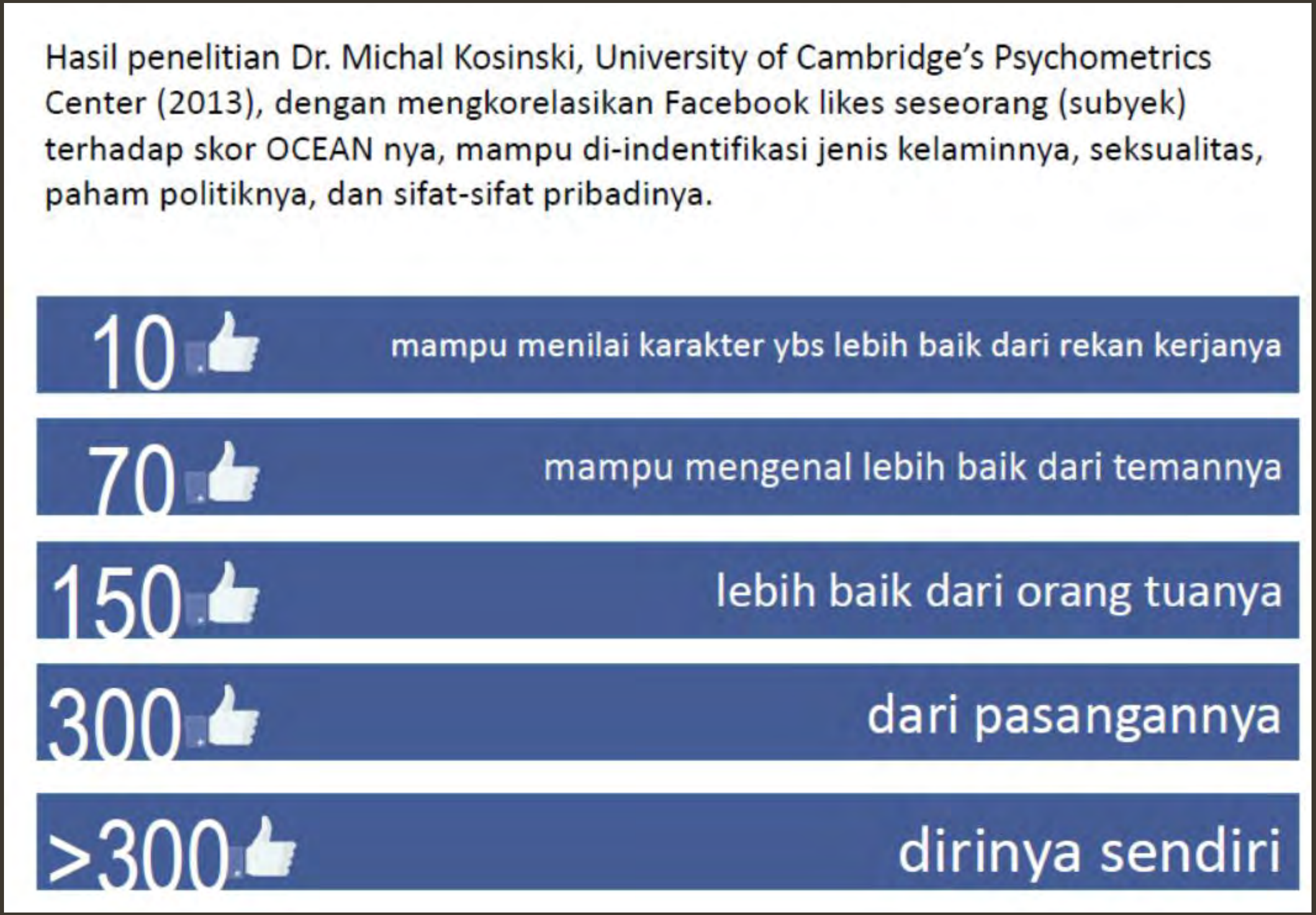
88% of reported stolen assets were personal data

Average Victims of impersonation

41.7 year old | $4,187 lost

Top place for thief is work area

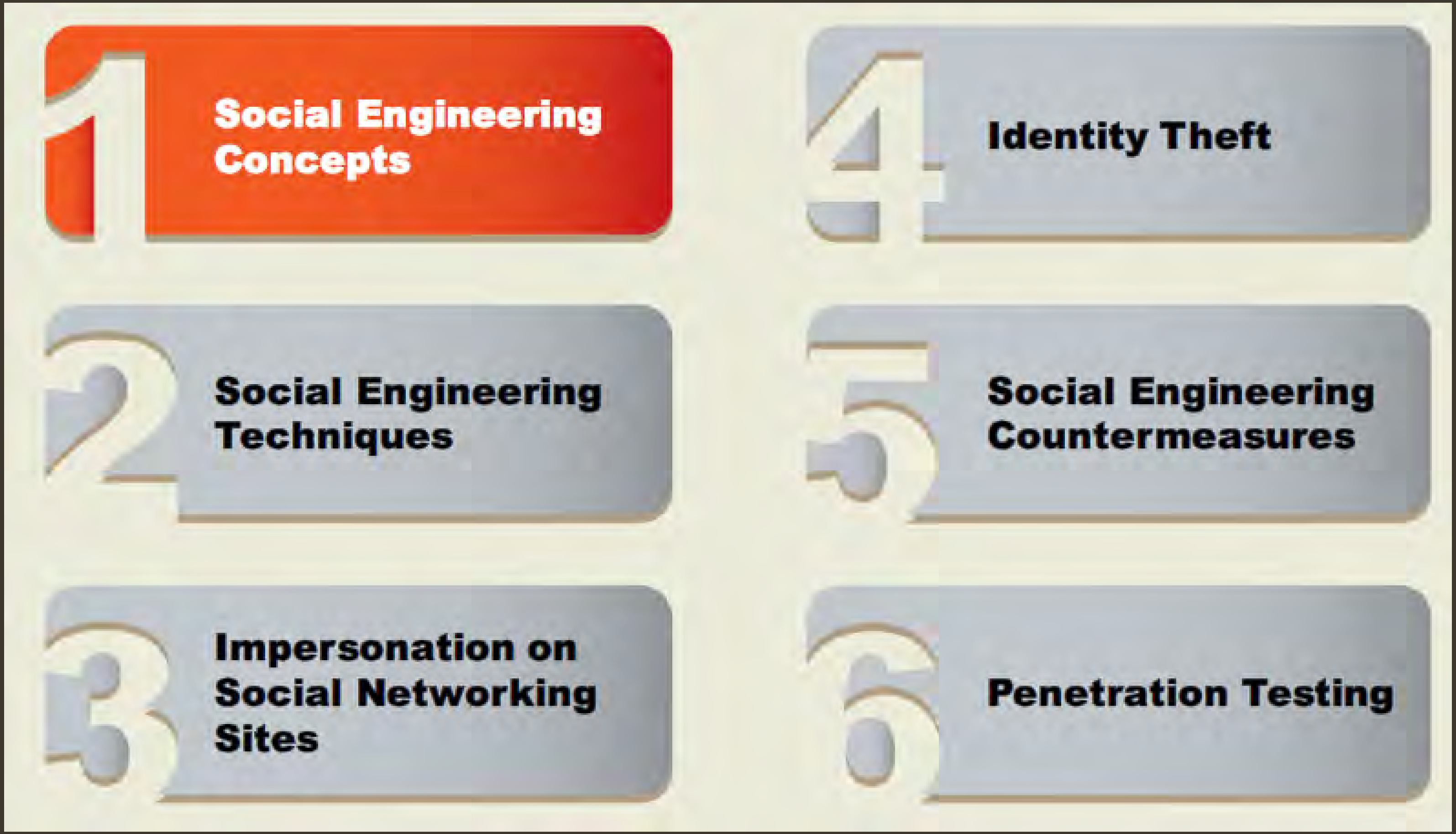
According to the survey conducted by Social-Engineer.Org http://www.social-engineer.org



Hasil penelitian Dr. Michal Kosinski, University of Cambridge's Psychometrics Center (2013), dengan mengkorelasikan Facebook likes seseorang (subyek) terhadap skor OCEAN nya, mampu di-indentifikasi jenis kelaminnya, seksualitas, paham politiknya, dan sifat-sifat pribadinya.

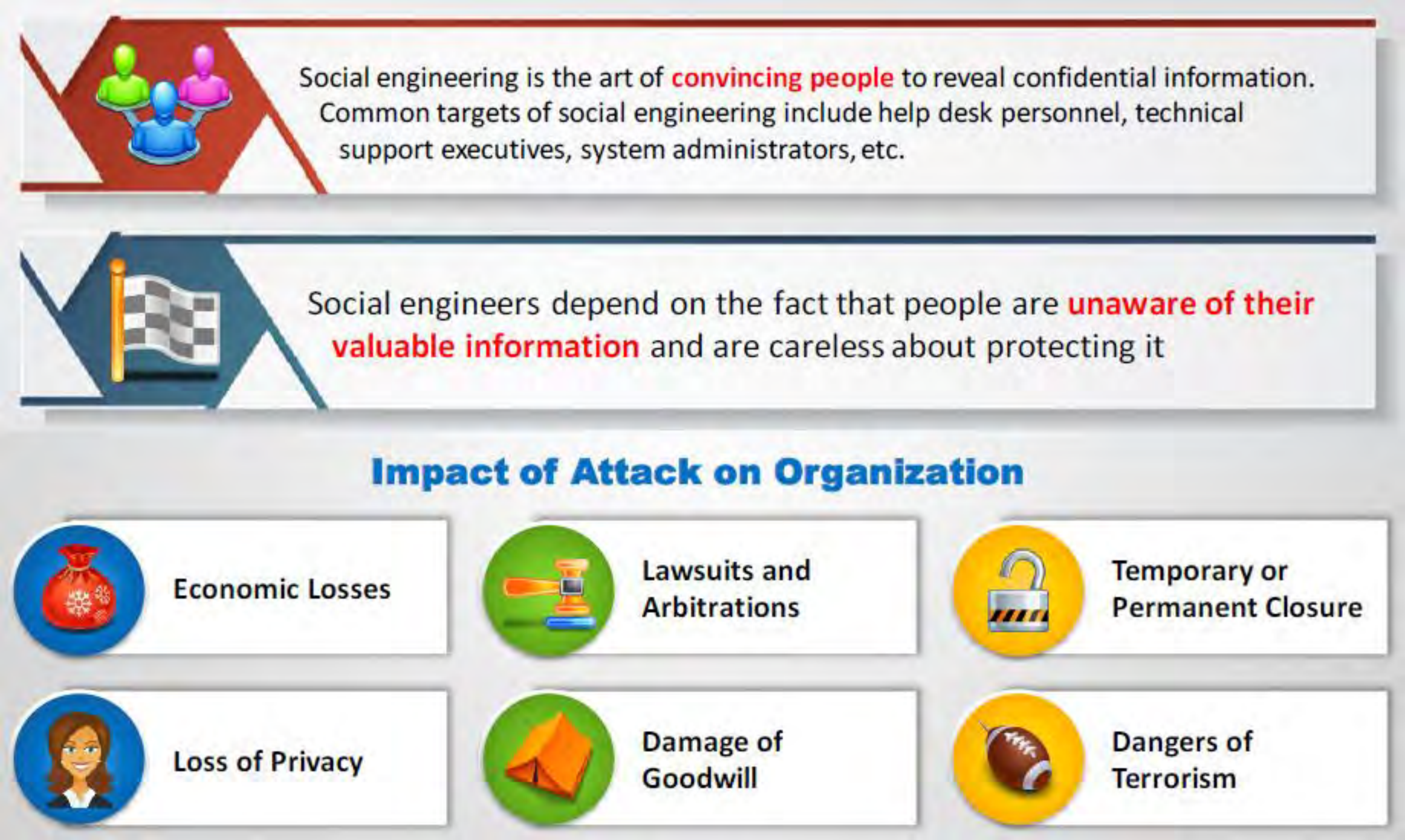
10 👍	mampu menilai karakter ybs lebih baik dari rekan kerjanya
70 👍	mampu mengenal lebih baik dari temannya
150 👍	lebih baik dari orang tuanya
300 👍	dari pasangannya
>300 👍	dirinya sendiri

Agenda



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

Social Engineering



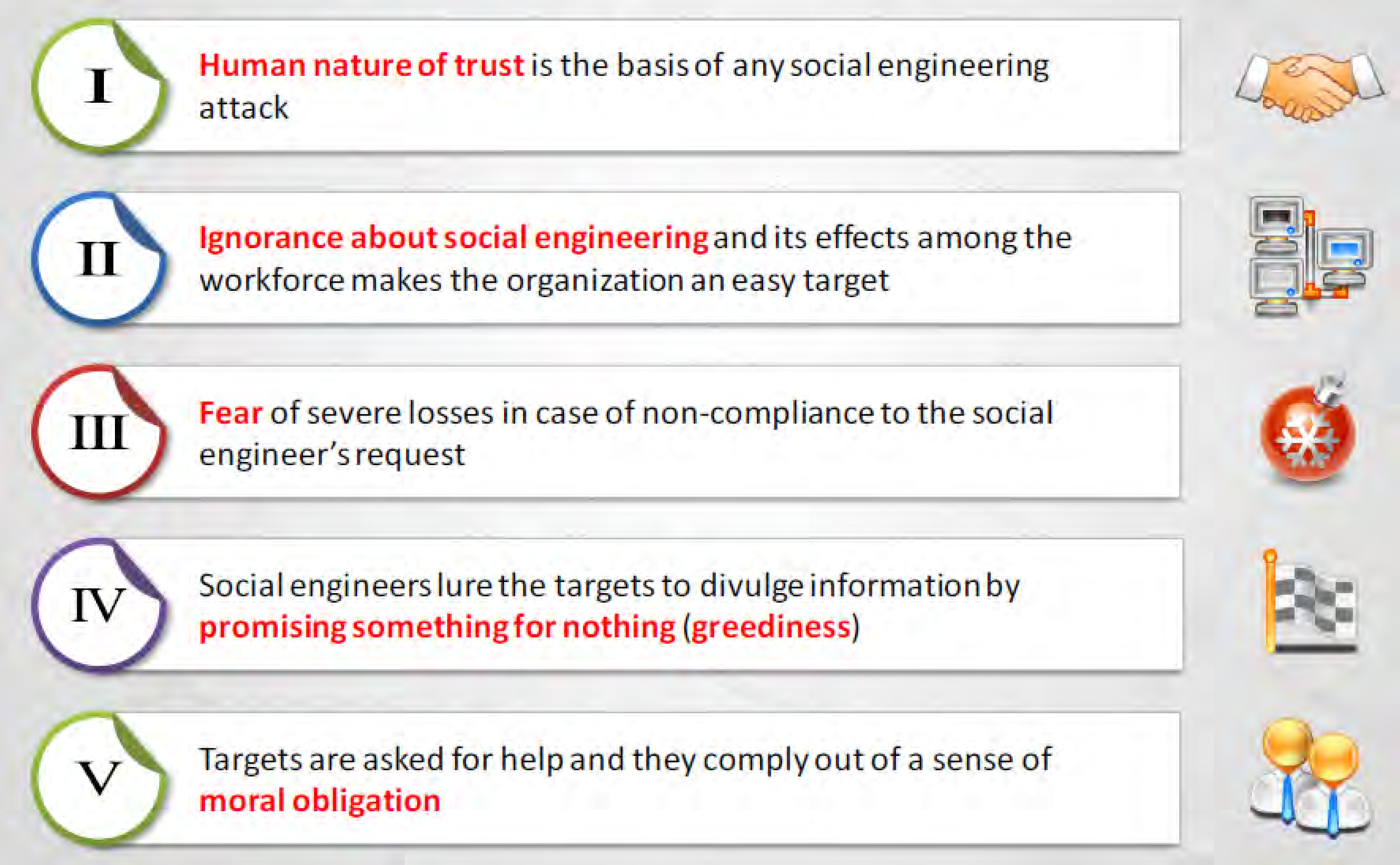
Social engineering is the art of **convincing people** to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.

Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it

Impact of Attack on Organization

- Economic Losses
- Lawsuits and Arbitrations
- Temporary or Permanent Closure
- Loss of Privacy
- Damage of Goodwill
- Dangers of Terrorism

Behaviors Vulnerable to Attacks



I **Human nature of trust** is the basis of any social engineering attack

II **Ignorance about social engineering** and its effects among the workforce makes the organization an easy target

III **Fear** of severe losses in case of non-compliance to the social engineer's request

IV Social engineers lure the targets to divulge information by **promising something for nothing** (**greediness**)

V Targets are asked for help and they comply out of a sense of **moral obligation**

Factor that Make Companies Vulnerable to Attacks

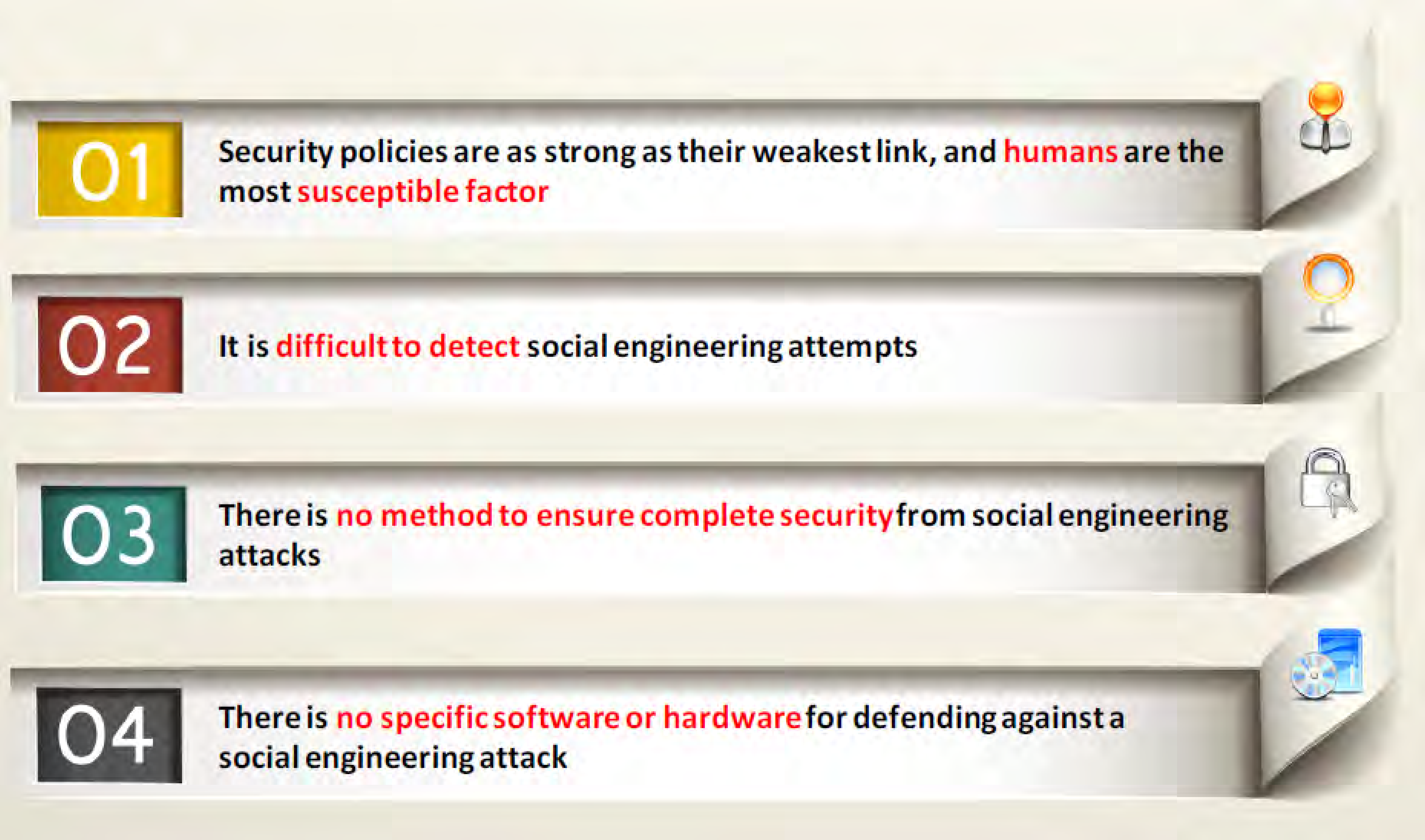
01 Insufficient Security Training

02 Unregulated Access to the Information

03 Several Organizational Units

04 Lack of Security Policies

Why is Social Engineering Effective?



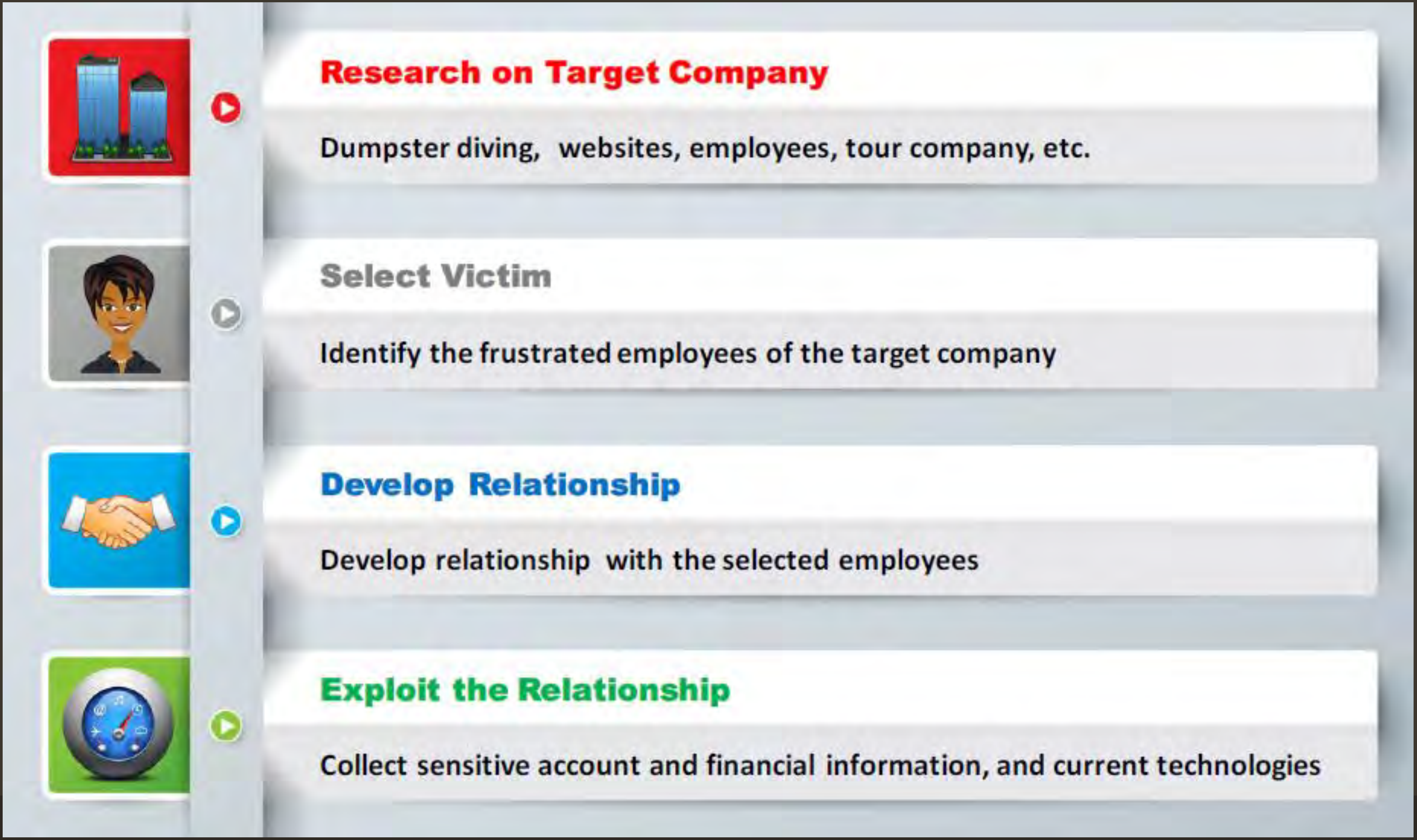
01 Security policies are as strong as their weakest link, and humans are the most susceptible factor

02 It is difficult to detect social engineering attempts

03 There is no method to ensure complete security from social engineering attacks

04 There is no specific software or hardware for defending against a social engineering attack

Phases in Social Engineering



Research on Target Company

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

Select Victim

Identify the frustrated employees of the target company

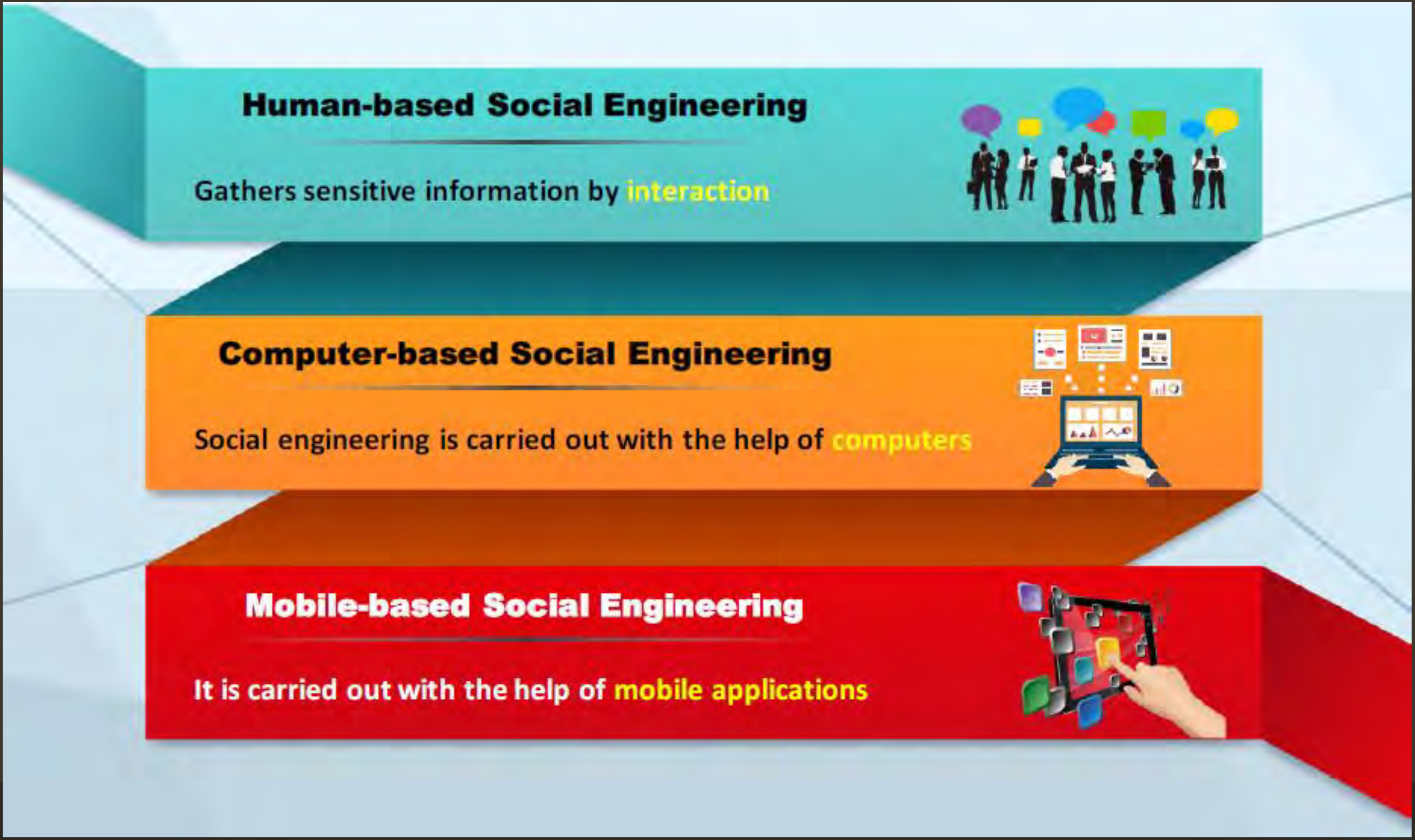
Develop Relationship

Develop relationship with the selected employees

Exploit the Relationship

Collect sensitive account and financial information, and current technologies

Type of Social Engineering



Human-based Social Engineering

Gathers sensitive information by interaction

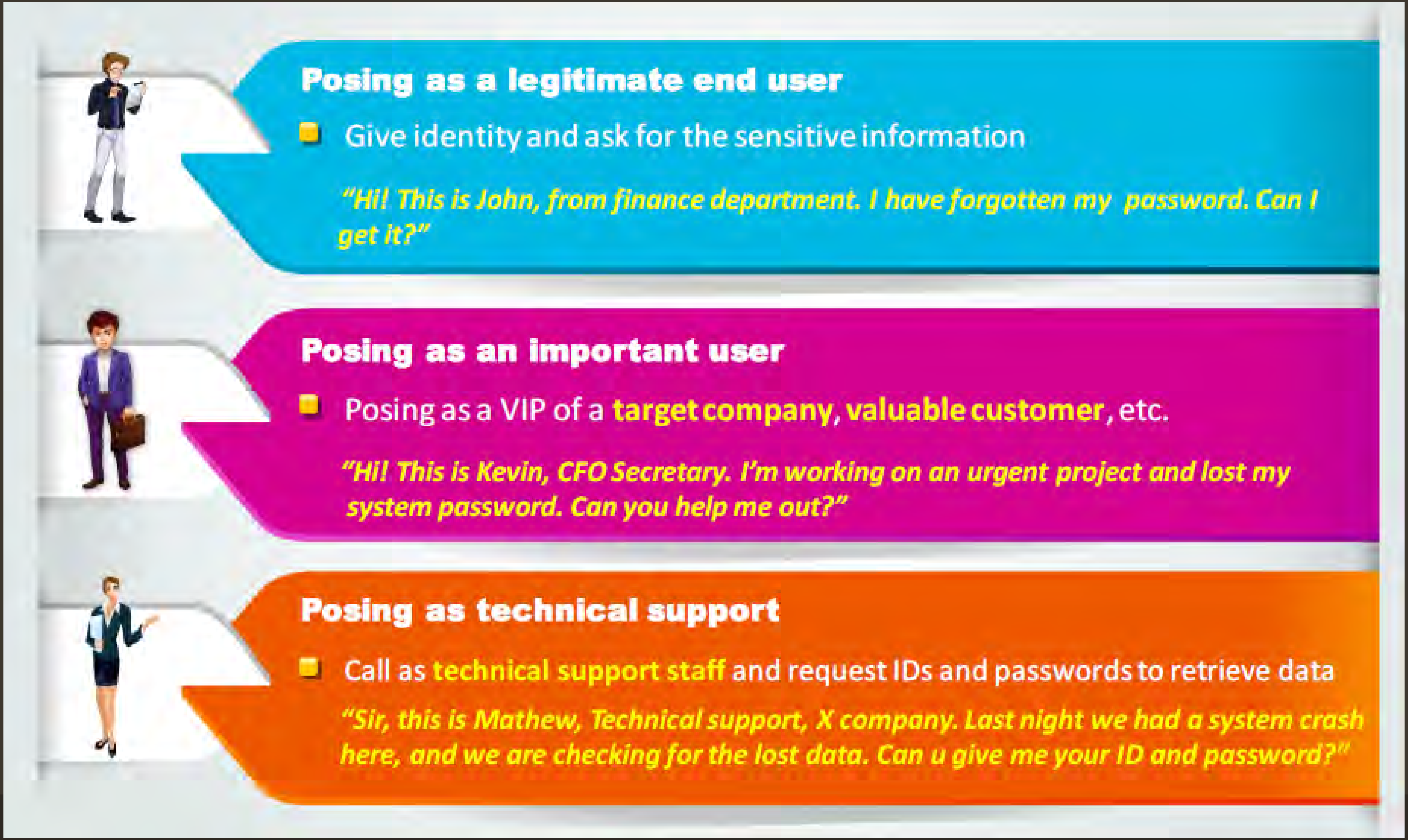
Computer-based Social Engineering

Social engineering is carried out with the help of computers

Mobile-based Social Engineering

It is carried out with the help of mobile applications

Human-based Social Engineering



Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John, from finance department. I have forgotten my password. Can I get it?"

Posing as an important user

- Posing 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 password. Can you help me out?"

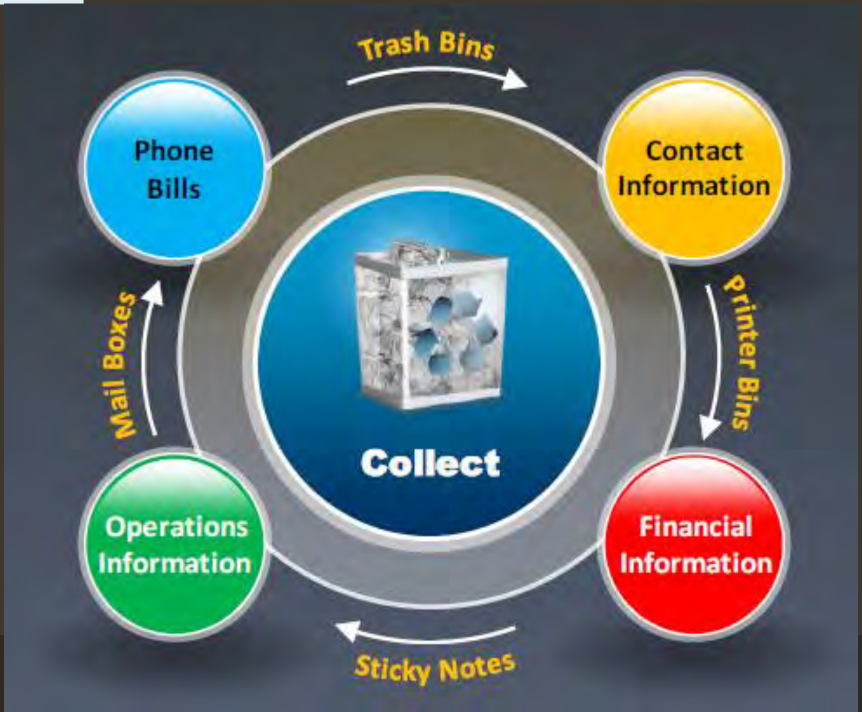
Posing as technical support

- Call as **technical support staff** and request IDs and passwords to retrieve data

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

Shoulder Surfing

Eavesdropping



Trash Bins

Phone Bills

Contact Information

Collect

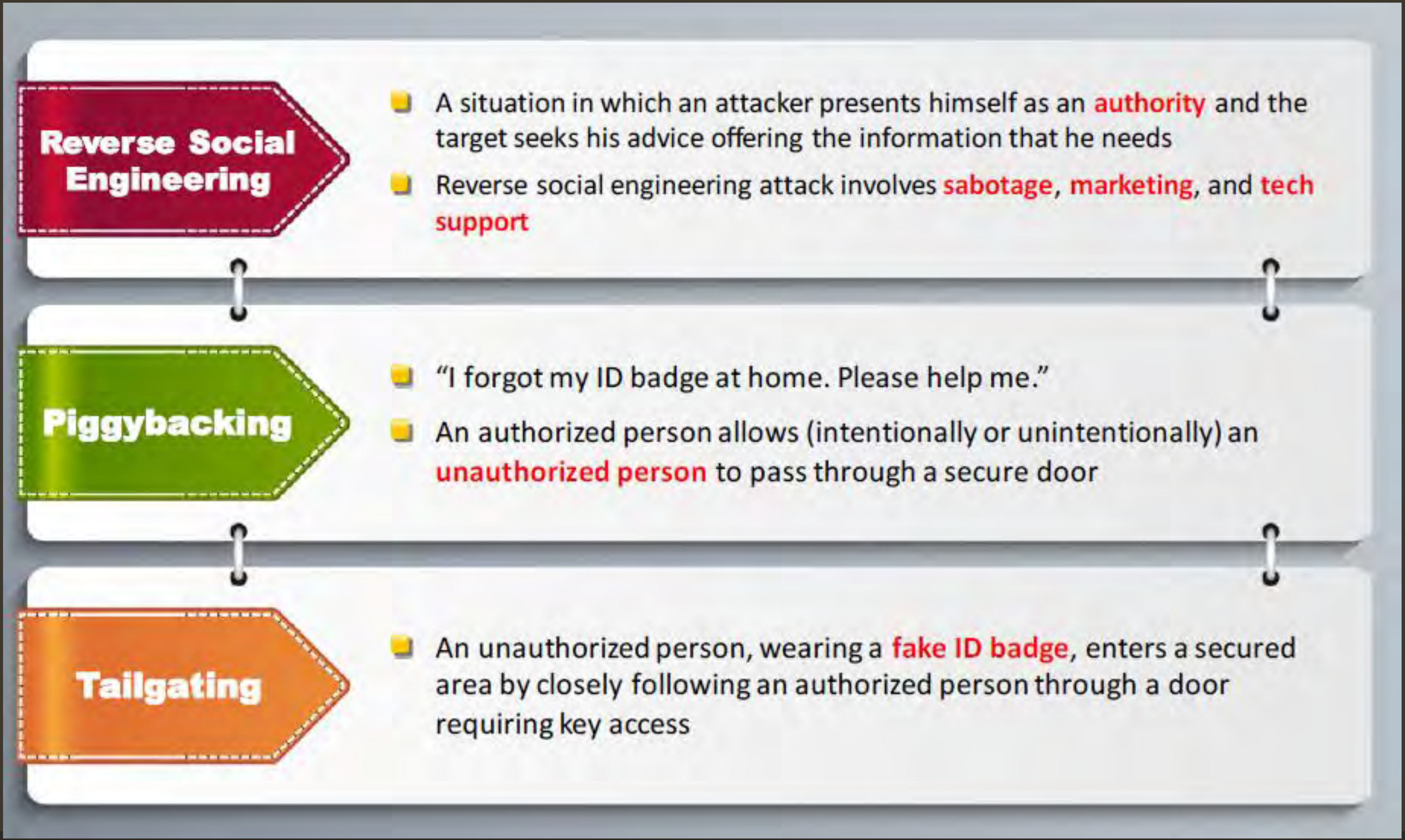
Printer Bins

Financial Information

Sticky Notes

Operations Information

Mail Boxes



Reverse Social Engineering

- A situation in which an attacker presents himself as an **authority** and the target seeks his advice offering the information that he needs
- Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**

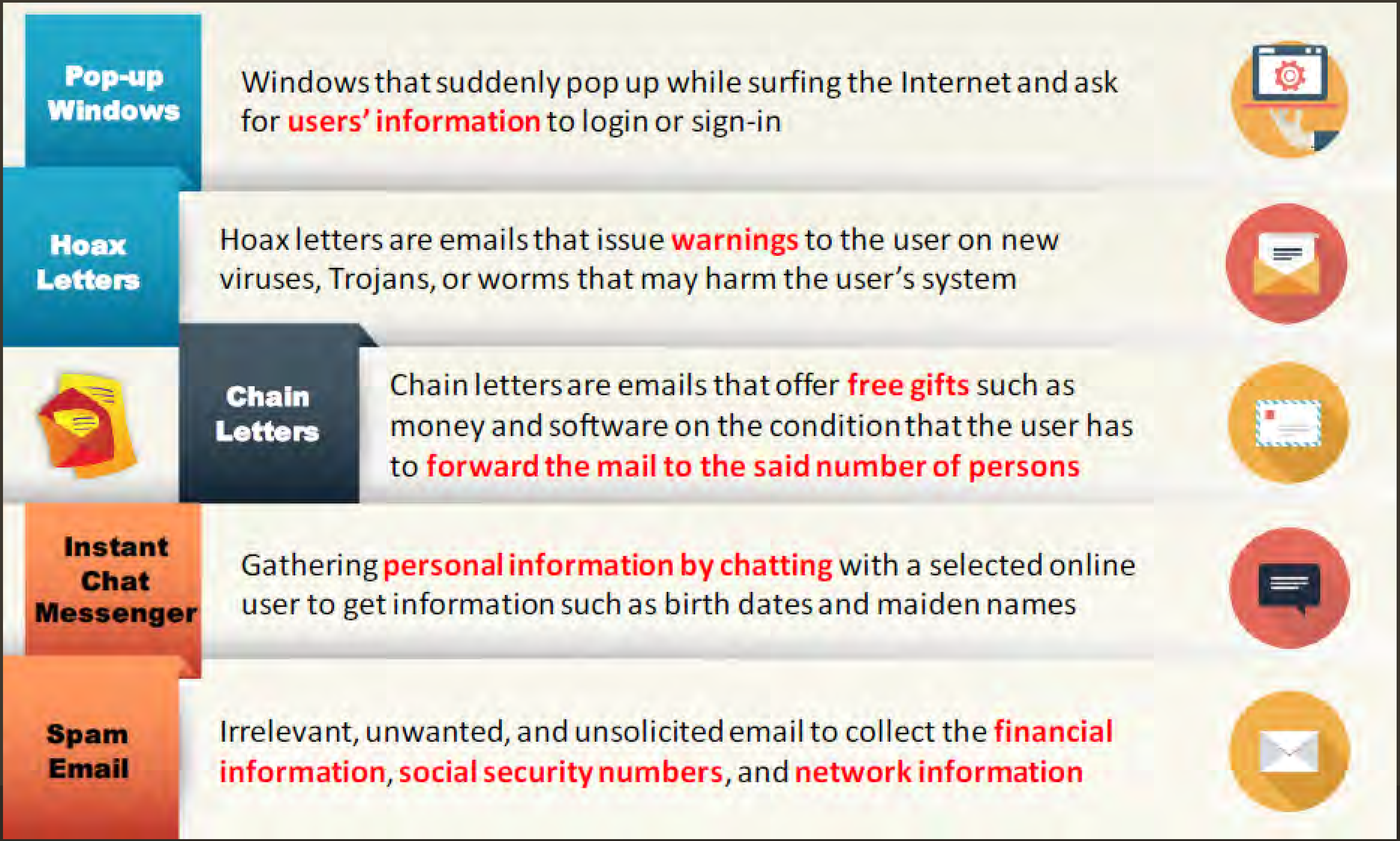
Piggybacking

- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door

Tailgating

- An unauthorized person, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door requiring key access

Computer-based Social Engineering



Pop-up Windows

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

Hoax Letters

Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system

Chain Letters

Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward the mail to the said number of persons**

Instant Chat Messenger

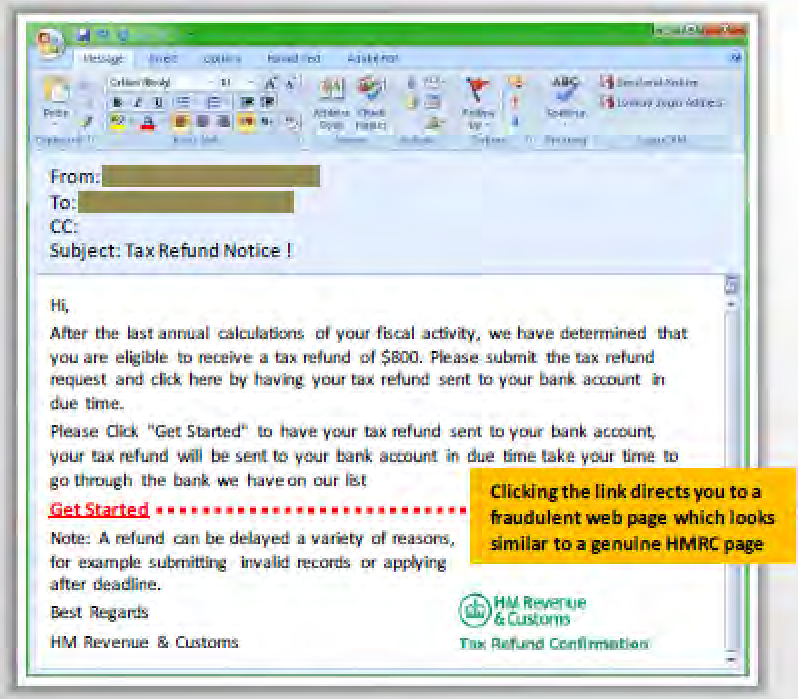
Gathering **personal information by chatting** with a selected online user to get information such as birth dates and maiden names

Spam Email

Irrelevant, unwanted, and unsolicited email to collect the **financial information**, **social security numbers**, and **network information**

An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information

Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that 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

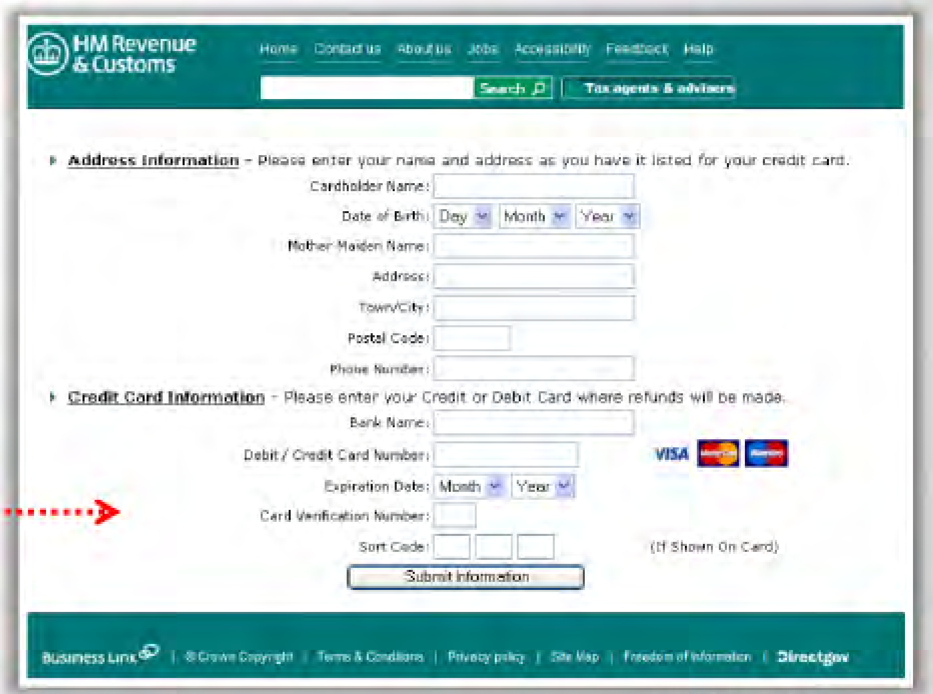
Get Started

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 which 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:

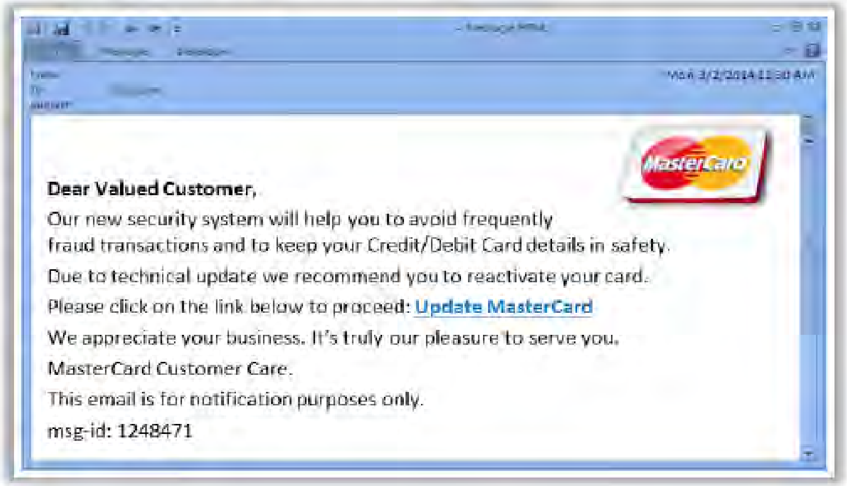
Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

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

VISA
Submit Information
Business Link | © Crown Copyright | Terms & Conditions | Privacy policy | Site Map | Freedom of Information | Directgov

http://www.hmrc.gov.uk

Examples of phishing emails:



Dear Valued Customer,

Our new security system will help you to avoid frequently
fraud transactions and to keep your Credit/Debit Card details in safety.

Due to technical update we recommend you to reactivate your card.

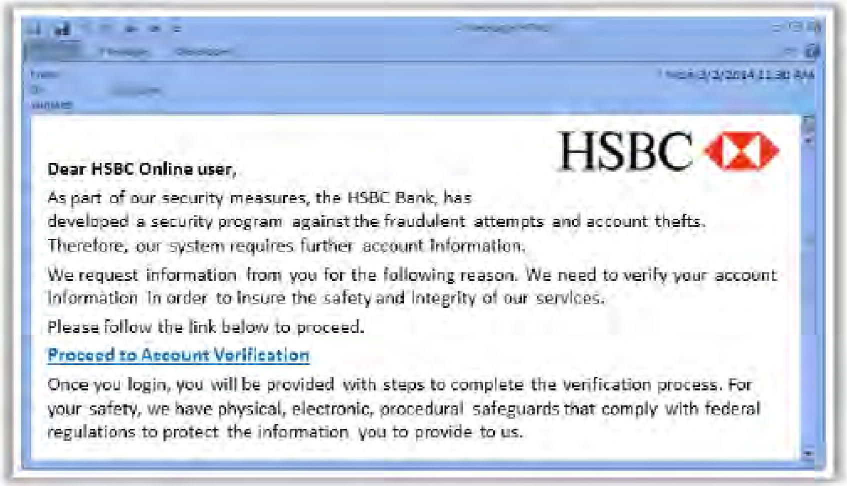
Please click on the link below to proceed: Update MasterCard

We appreciate your business. It's truly our pleasure to serve you.

MasterCard Customer Care.

This email is for notification purposes only.

msg-id: 1248471



Dear HSBC Online user,

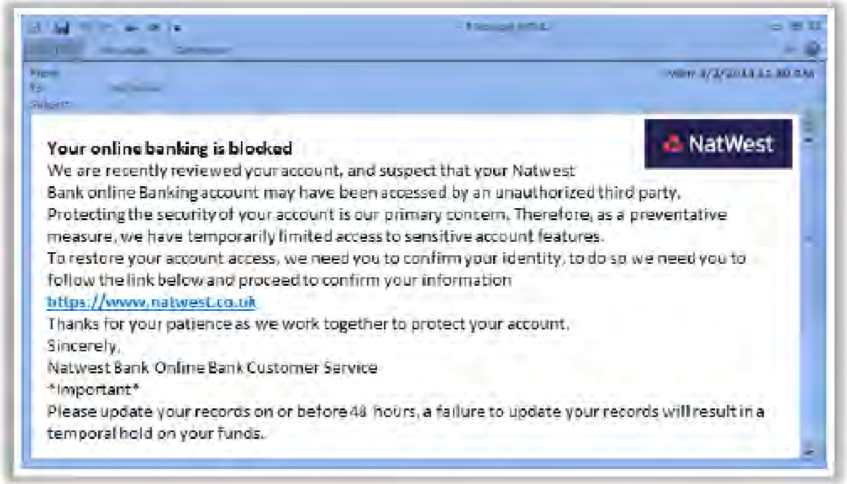
As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account Information.

We request information from you for the following reason. We need to verify your account Information In order to Insure the safety and Integrity of our services.

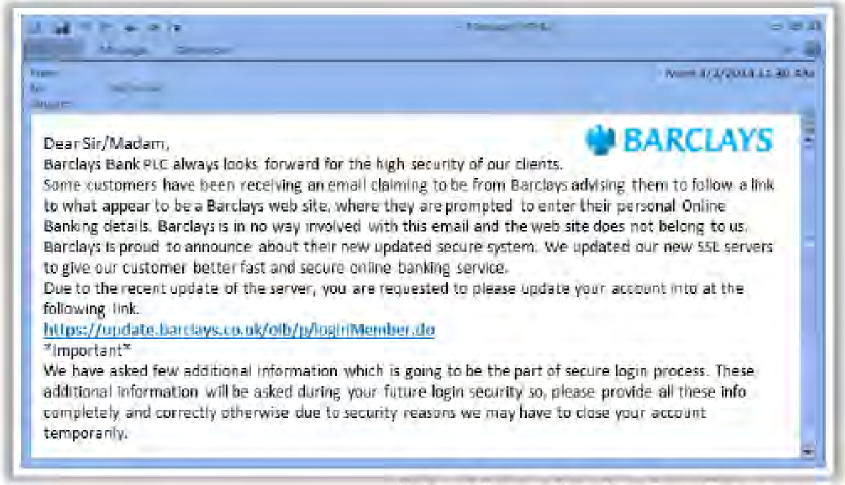
Please follow the link below to proceed.

Proceed to Account Verification

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.



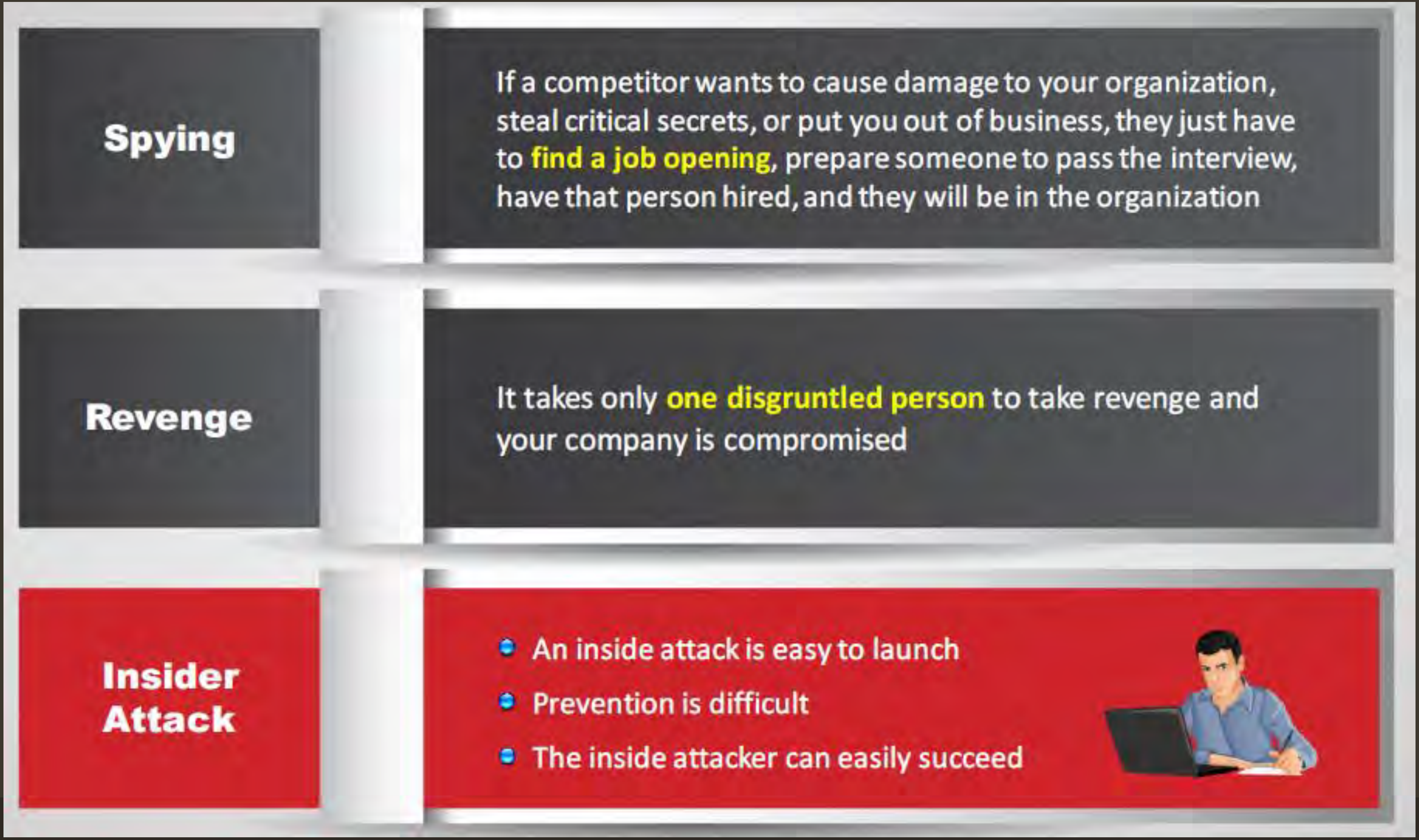
Your online banking is blocked
We are recently reviewed your account, and suspect that your Natwest
Bank online Banking account may have been accessed by an unauthorized third party.
Protecting the security of your account is our primary concern. Therefore, as a preventative
measure, we have temporarily limited access to sensitive account features.
To restore your account access, we need you to confirm your identity, to do so we need you to
follow the link below and proceed to confirm your information
https://www.natwest.co.uk
Thanks for your patience as we work together to protect your account.
Sincerely,
Natwest Bank Online Bank Customer Service
Important
Please update your records on or before 48 hours, a failure to update your records will result in a
temporal hold on your funds.



Dear Sir/Madam,
Barclays Bank PLC always looks forward for the high security of our clients.
Some customers have been receiving an email claiming to be from Barclays advising them to follow a link
to what appear to be a Barclays web site, where they are prompted to enter their personal Online
Banking details. Barclays is in no way involved with this email and the web site does not belong to us.
Barclays is proud to announce about their new updated secure system. We updated our new SSL servers
to give our customer better fast and secure online banking service.
Due to the recent update of the server, you are requested to please update your account into at the
following link.
https://update.barclays.co.uk/olb/p/loginMember.do
Important
We have asked few additional information which is going to be the part of secure login process. These
additional information will be asked during your future login security so, please provide all these info
completely and correctly otherwise due to security reasons we may have to close your account
temporarily.

http://www.banksafeonline.org.uk

Insider Attack



Spying

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to **find a job opening**, prepare someone to pass the interview, have that person hired, and they will be in the organization

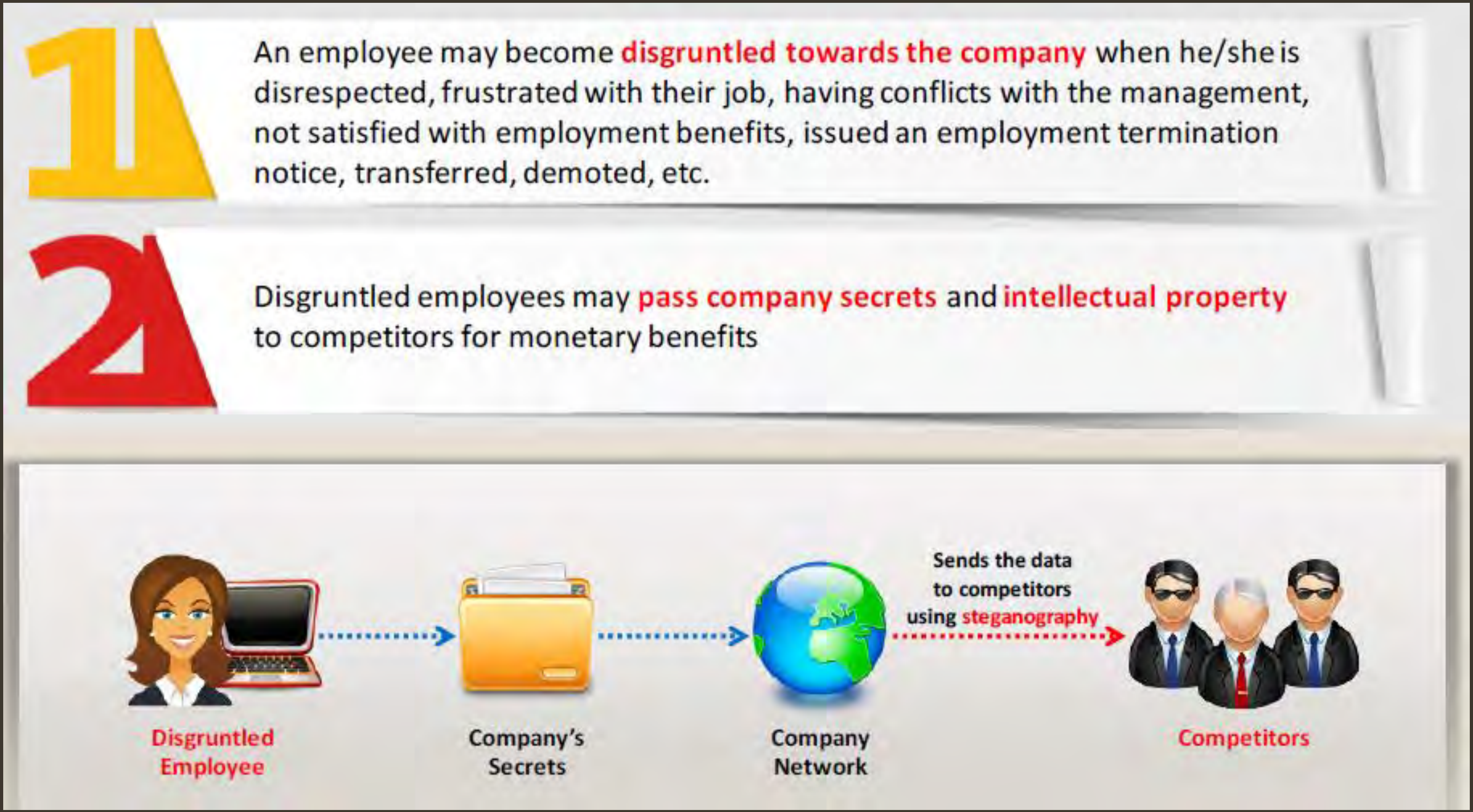
Revenge

It takes only **one disgruntled person** to take revenge and your company is compromised

Insider Attack

- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed

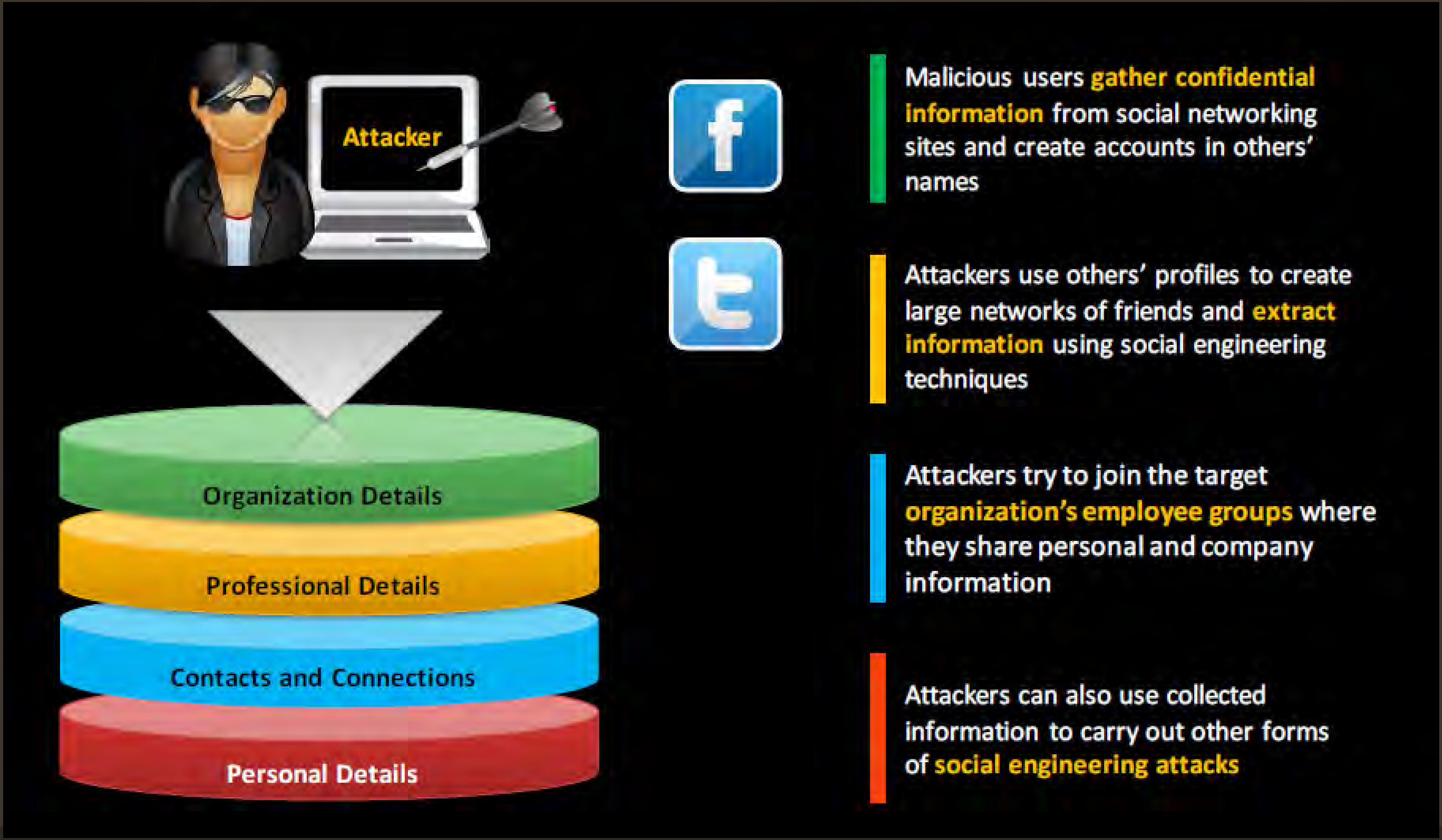
Disgruntled Employee



1 An employee may become **disgruntled towards the company** when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.

2 Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monetary benefits

Social Engineering through Social Networking



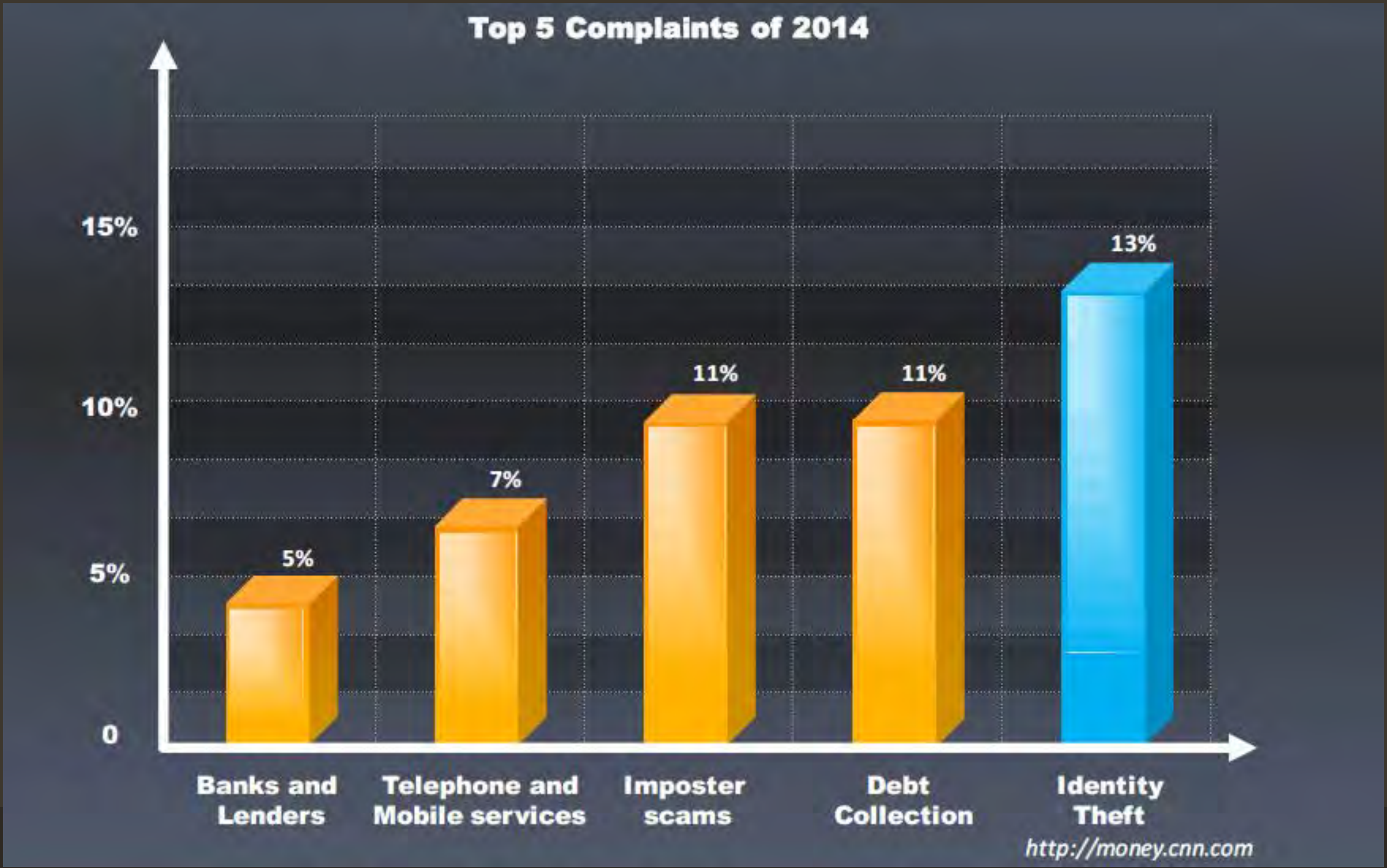
Malicious users **gather confidential information** from social networking sites and create accounts in others' names

Attackers use others' profiles to create large networks of friends and **extract information** using social engineering techniques

Attackers try to join the target **organization's employee groups** where they share personal and company information

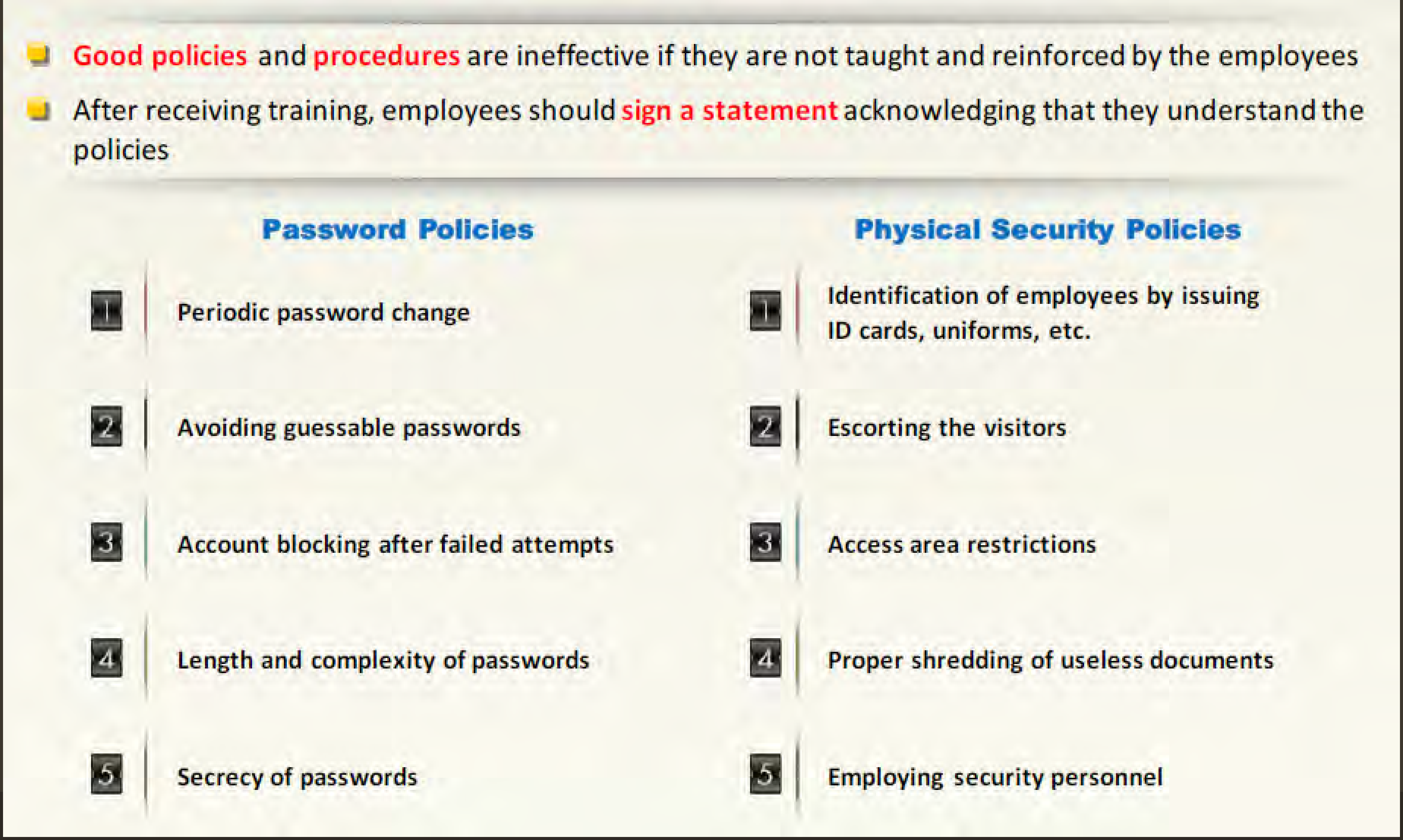
Attackers can also use collected information to carry out other forms of **social engineering attacks**

Identity Theft Statistics



http://money.cnn.com

Social Engineering Countermeasures



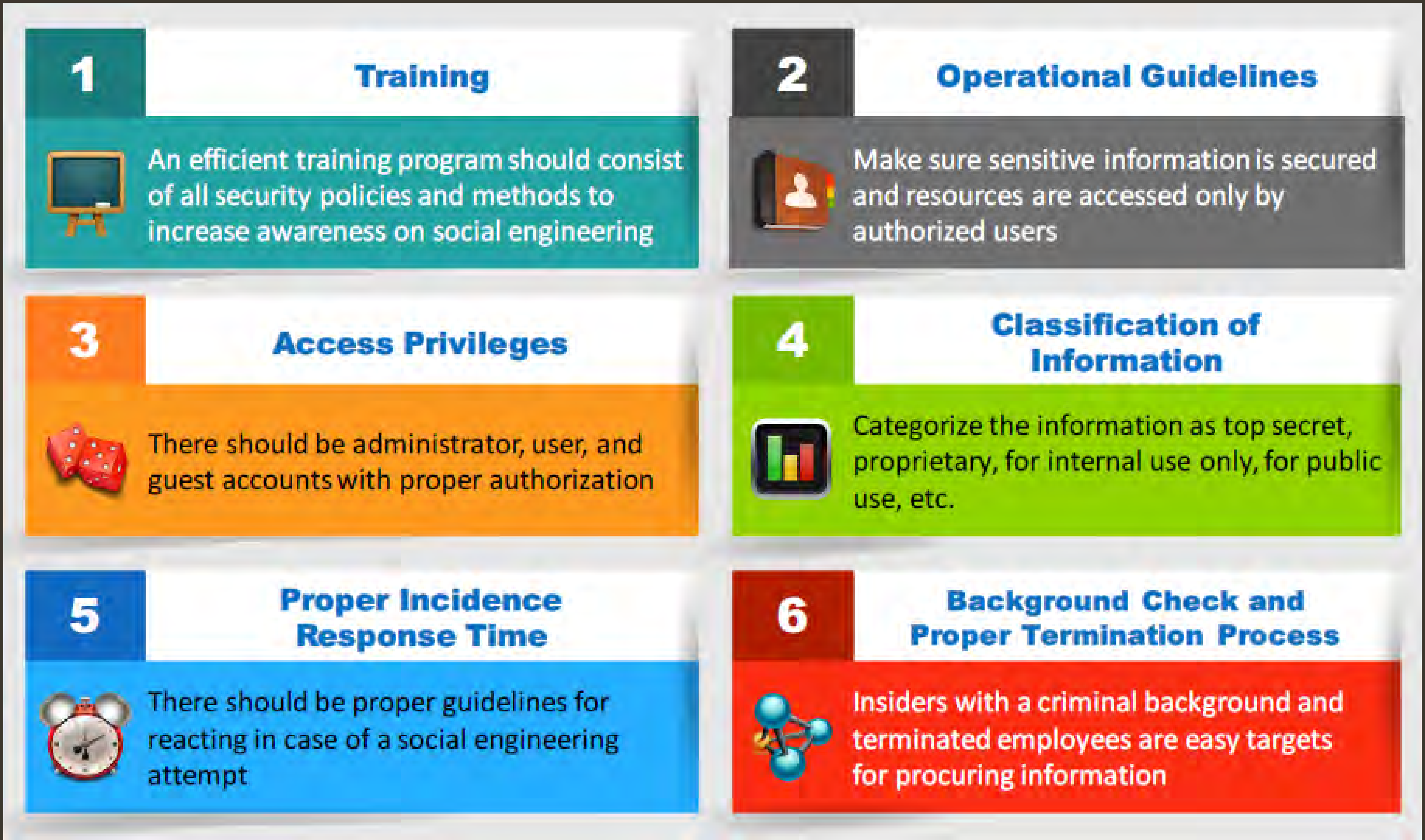
- Good policies and procedures are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies

Password Policies

1. Periodic password change
2. Avoiding guessable passwords
3. Account blocking after failed attempts
4. Length and complexity of passwords
5. Secrecy of passwords

Physical Security Policies

1. Identification of employees by issuing ID cards, uniforms, etc.
2. Escorting the visitors
3. Access area restrictions
4. Proper shredding of useless documents
5. Employing security personnel



1 Training

An efficient training program should consist of all security policies and methods to increase awareness on social engineering

2 Operational Guidelines

Make sure sensitive information is secured and resources are accessed only by authorized users

3 Access Privileges

There should be administrator, user, and guest accounts with proper authorization

4 Classification of Information

Categorize the information as top secret, proprietary, for internal use only, for public use, etc.

5 Proper Incidence Response Time

There should be proper guidelines for reacting in case of a social engineering attempt

6 Background Check and Proper Termination Process

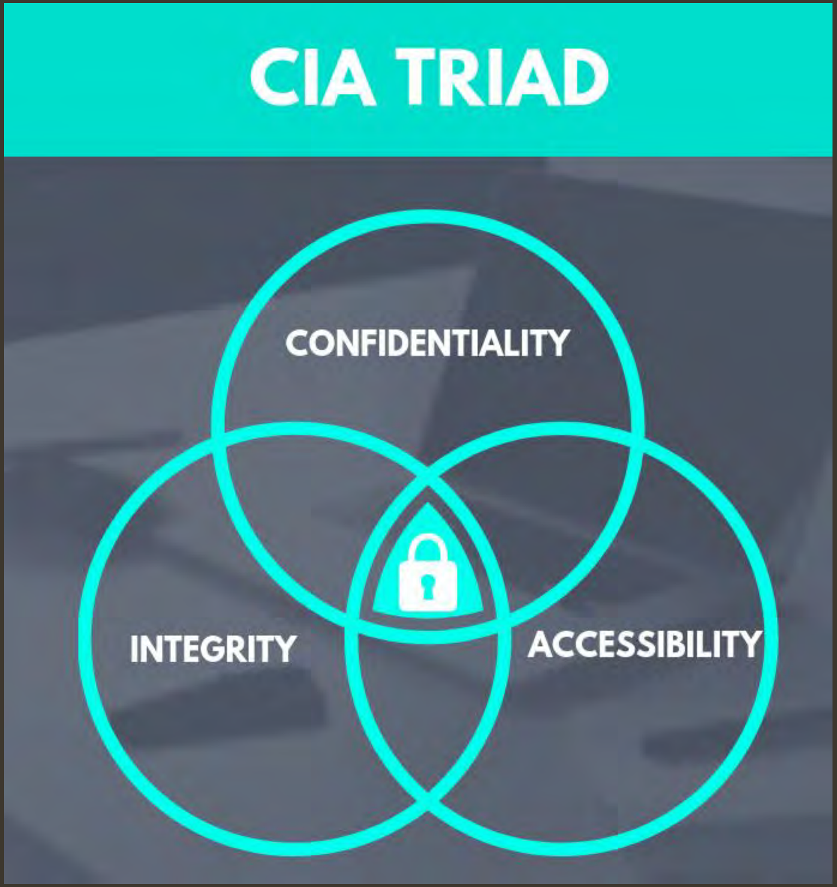
Insiders with a criminal background and terminated employees are easy targets for procuring information

Anti-Virus/Anti-Phishing Defenses > Use **multiple layers** of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks

Two-Factor Authentication > Instead of fixed passwords, use two-factor authentication for **high-risk network services** such as VPNs and modem pools

Change Management > A **documented change-management** process is more secure than the ad-hoc process

CIA Concept with AAA Model



Q & A

- END