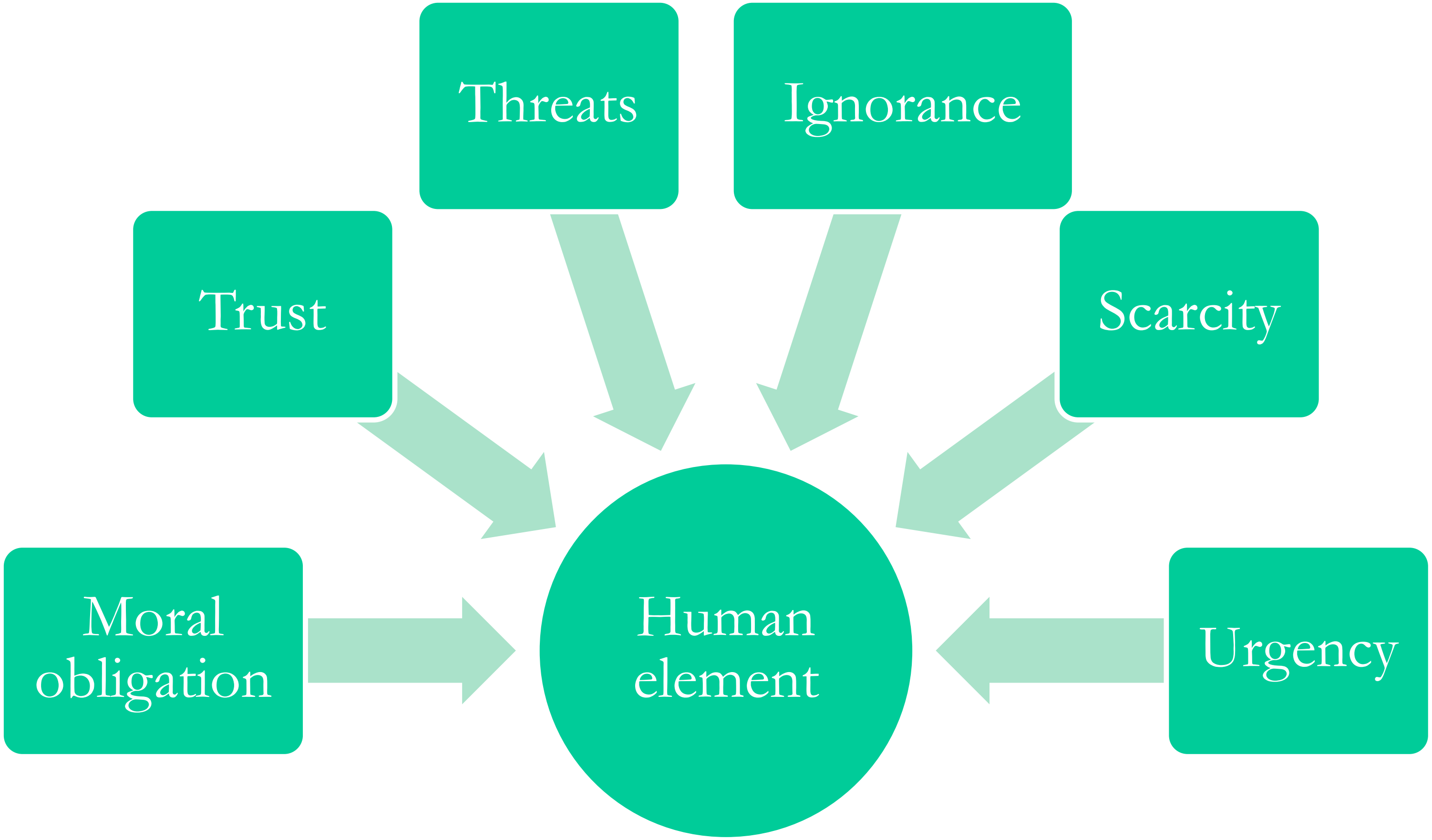
Social Engineering

Chapter 10

How Do Social Engineers Work?



Threats

Ignorance

Trust

Scarcity

Moral obligation

Human element

Urgency

Why Social Engineering Works

Social engineering is effective for a number of reasons, each of which can be remedied or exploited depending on whether you are the defender or the attacker.

- **Lack of a technological fix**
- **Insufficient security policies**
- **Difficult detection**
- **Lack of training**

Example of Social Engineering

- An unexpected phone call from your Internet service provider (ISP) or Microsoft
- Tells you you’re either in danger (a virus or outdated software) or missing something valuable

- **Why it works:**
  - Exploits trust
  - Exploits buzzwords
  - Exploits scarcity

Example of Social Engineering

In the next phase, the attacker gains the user's trust, convinces the user a technical service is being provided, and requires payment via credit card.

- **Exploits lack of technical know-how**
- **Interacts with victim to build trust**
- **Acts as if providing a legitimate service**
- **Uses charade to obtain financial information**

Example of Social Engineering

Exploit fear

Leverages target's ignorance

Stresses urgency to force reaction

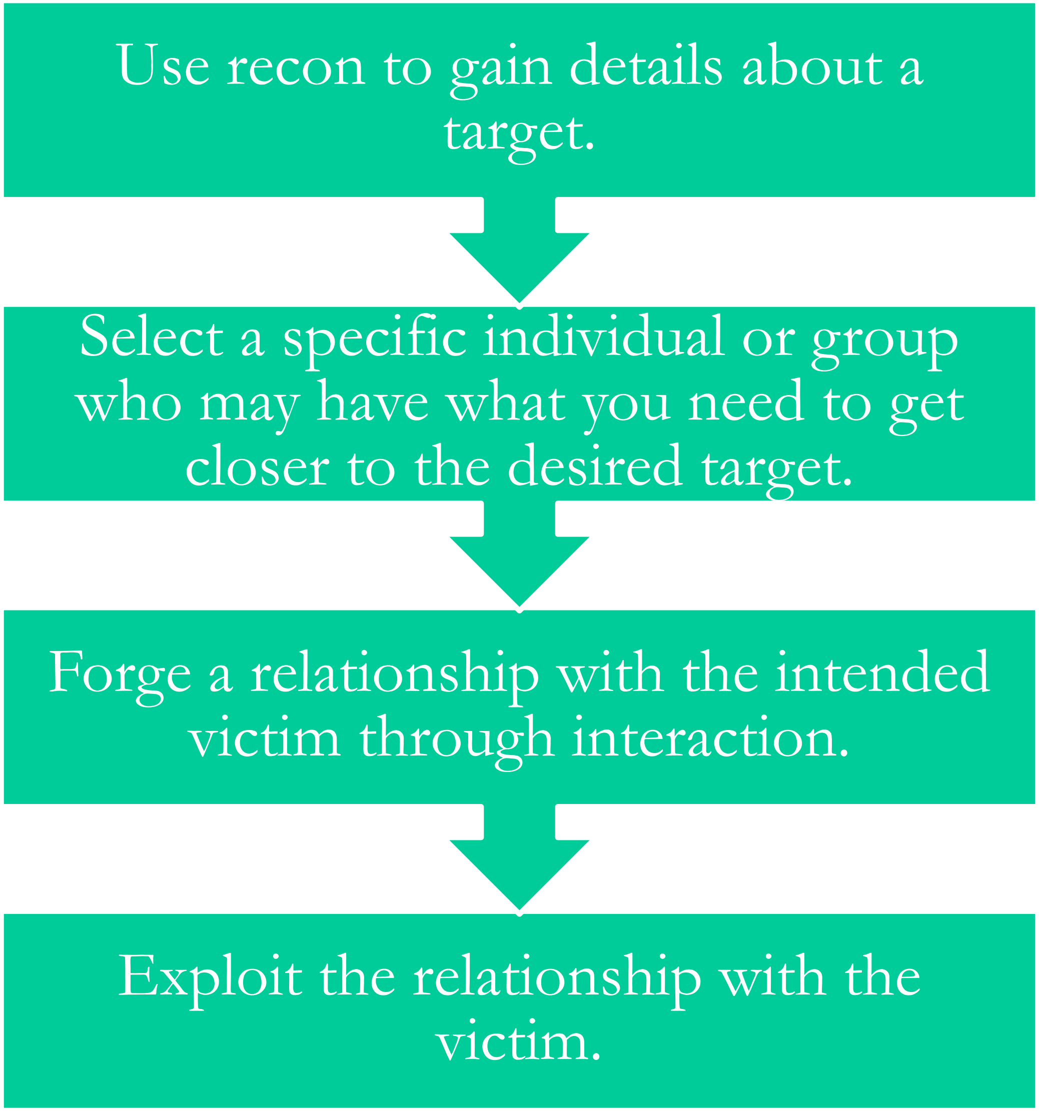
Presents image of authority

Signs of an Attack

- Use (or abuse) of authority
- Inability to provide contact information
- Making informal requests
- Excessive name dropping
- Excessive use of praise
- Discomfort when questioned

Social Engineering Phases

Social engineering, like the other attacks we have explored, consists of multiple phases, each designed to move the attacker one step closer to the ultimate goal.



Use recon to gain details about a target.

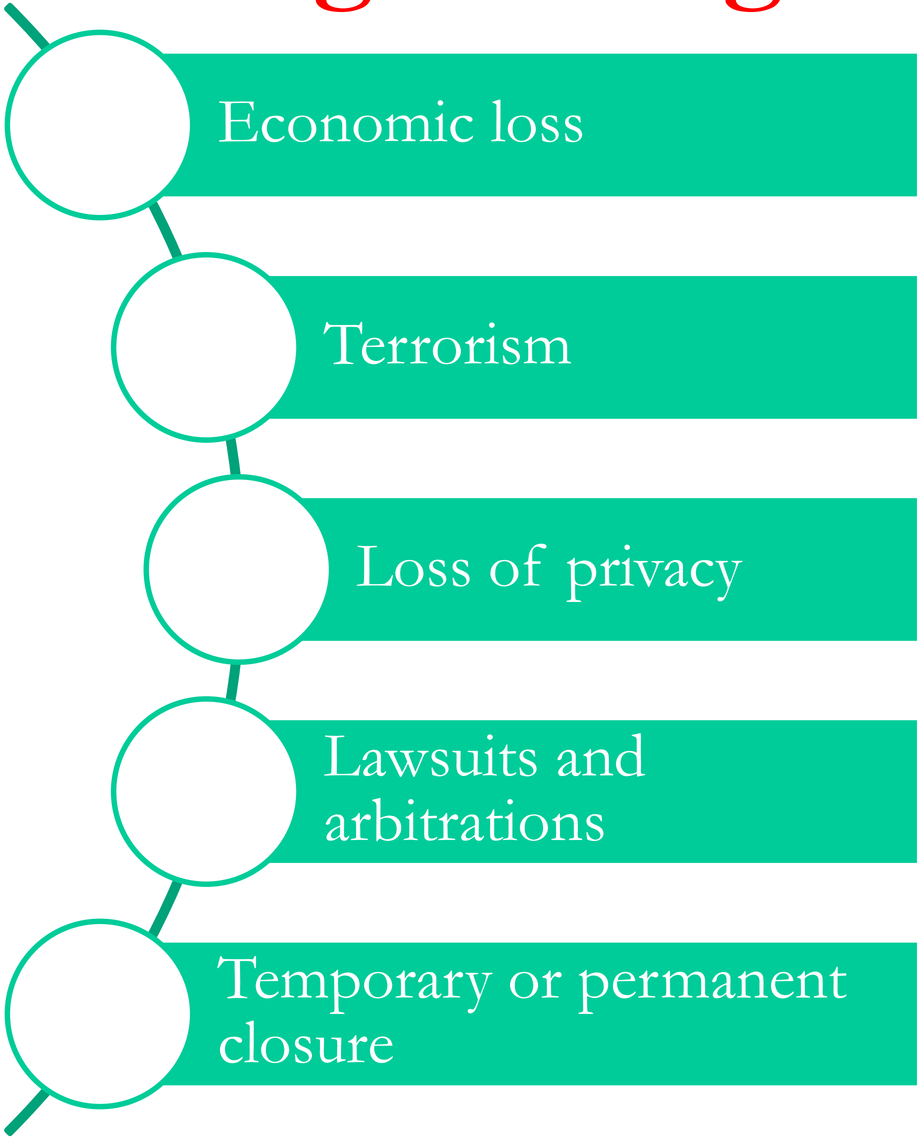
Select a specific individual or group who may have what you need to get closer to the desired target.

Forge a relationship with the intended victim through interaction.

Exploit the relationship with the victim.

Impact of Social Engineering

After experiencing a successful social engineering attack, businesses say they suffer from business disruption, lost productivity, and lost revenue and need to undo damage or conduct a forensic analysis.



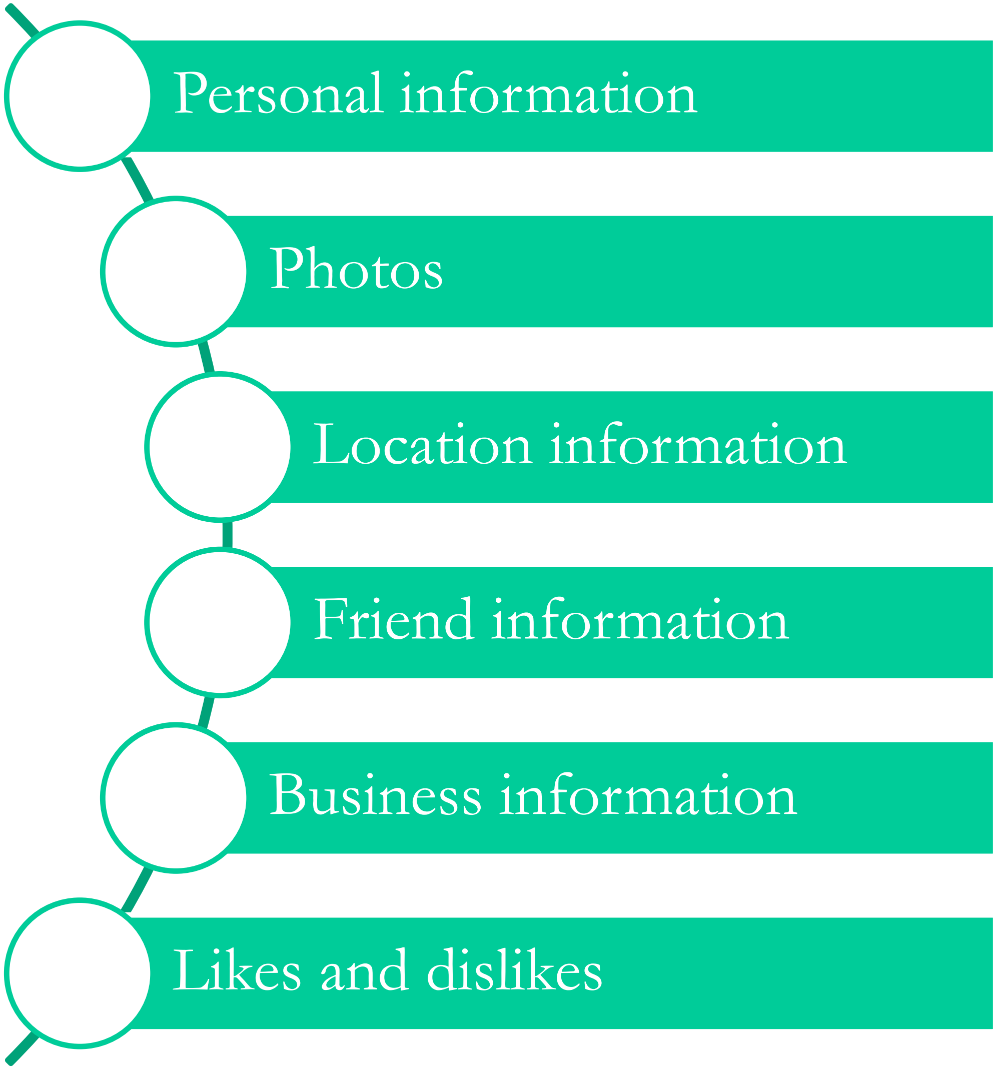
- Economic loss
- Terrorism
- Loss of privacy
- Lawsuits and arbitrations
- Temporary or permanent closure

Targets of Social Engineering

An attacker will look for targets of opportunity or potential victims who have the most to offer.

- **Receptionists**
- **Help desk personnel**
- **System administrators**
- **Executives**
- **Users**

Dangers of Social Networking



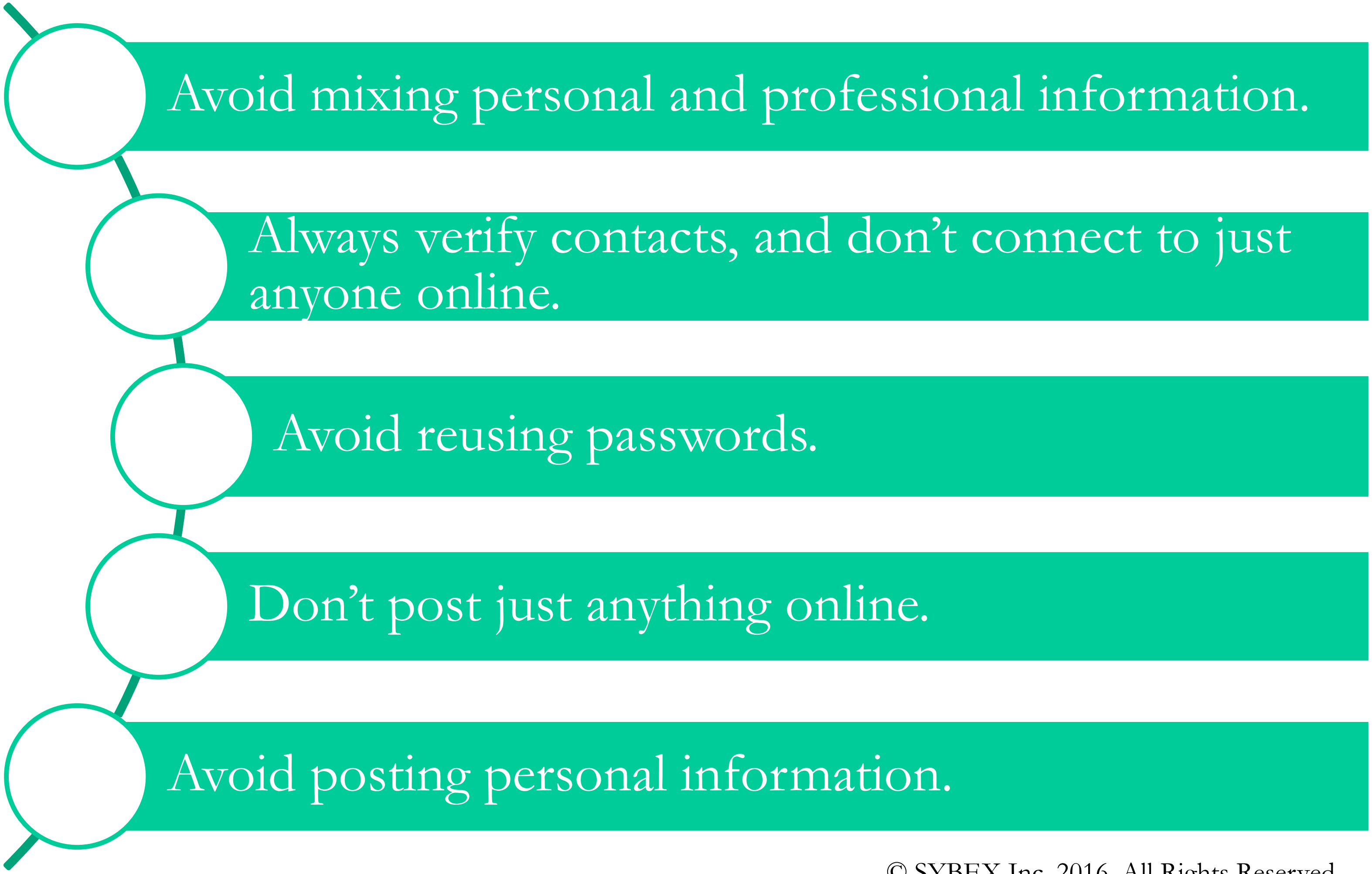
- Personal information
- Photos
- Location information
- Friend information
- Business information
- Likes and dislikes

Information Found on Social Networking

Social networking has made the attacker's job easier because of the volume of data and personal information available.

- Location information
- Personal data
- Company information
- Photos of private or secure facilities
- Information on co-workers
- Event or vacation information

Countermeasures Against Social Engineering



Avoid mixing personal and professional information.

Always verify contacts, and don’t connect to just anyone online.

Avoid reusing passwords.

Don’t post just anything online.

Avoid posting personal information.

Countermeasures and Recommendations

To avoid problems with social networking, a company should exercise many different countermeasures.

- Educate employees against publishing any identifying personal information online.
- Encourage or the use of nonwork accounts for use with social media.
- Educate employees on the use of strong passwords.
- Avoid the use of public profiles that anyone can view.
- Remind users that once something is put online, it never goes away.
- Educate employees on the use of privacy.
- Instruct employees on the presence of phishing scams.

Internet-Based Social Networking

Many threats will continue to pose problems for those using the Internet, and unless you opt to stop using this resource, you must address the threats.

Malware is used as an all-inclusive term for viruses, spyware, keyloggers, and worms.

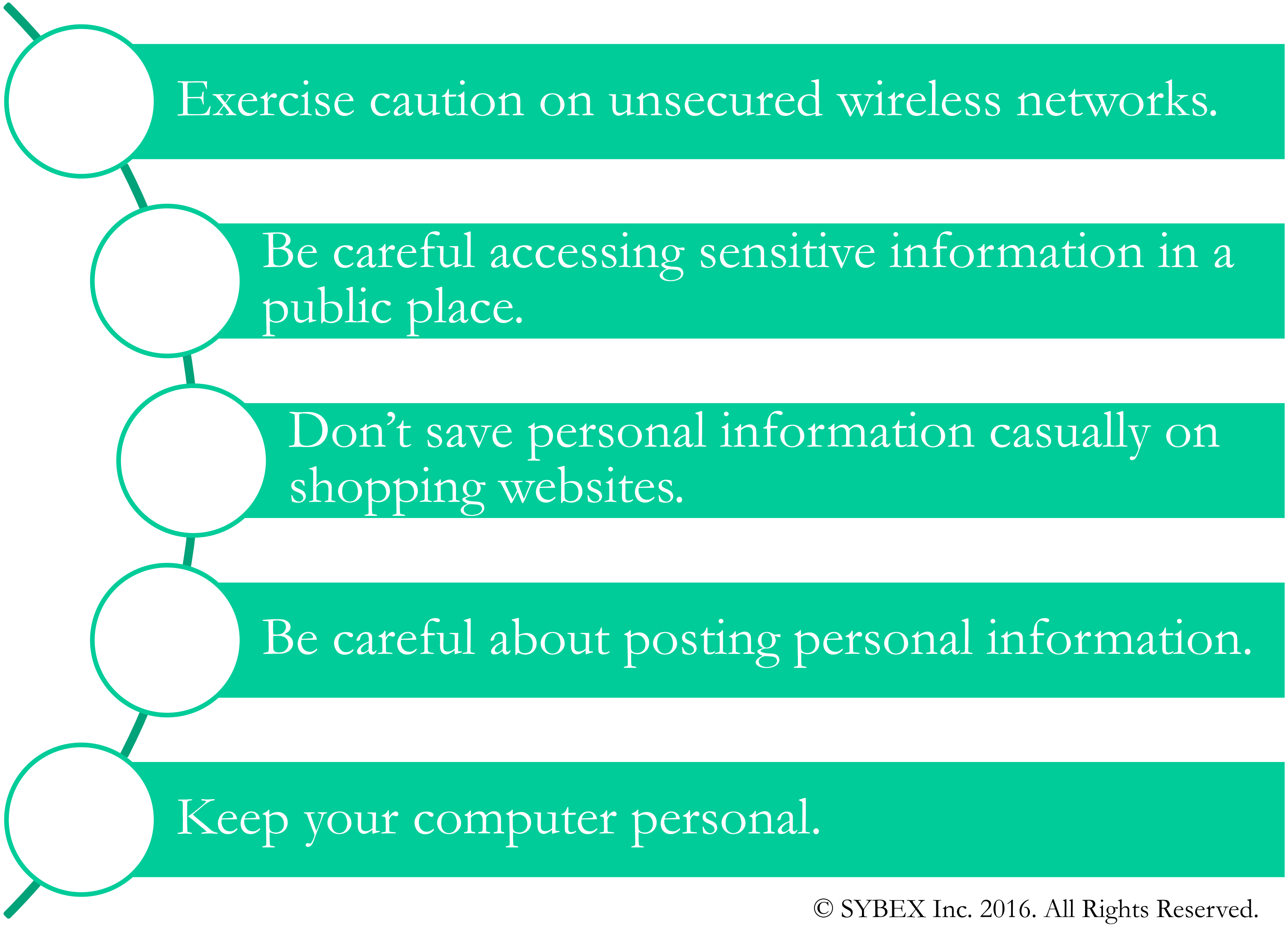
Shoulder surfing is when one party is able to look over another's shoulder, also called *spying*.

Eavesdropping involves listening in on communications.

Dumpster diving seeks to collect information from disposal points.

Phishing uses a bogus email to bait you to click a link or visit a malicious website.

Internet Social Engineering Countermeasures



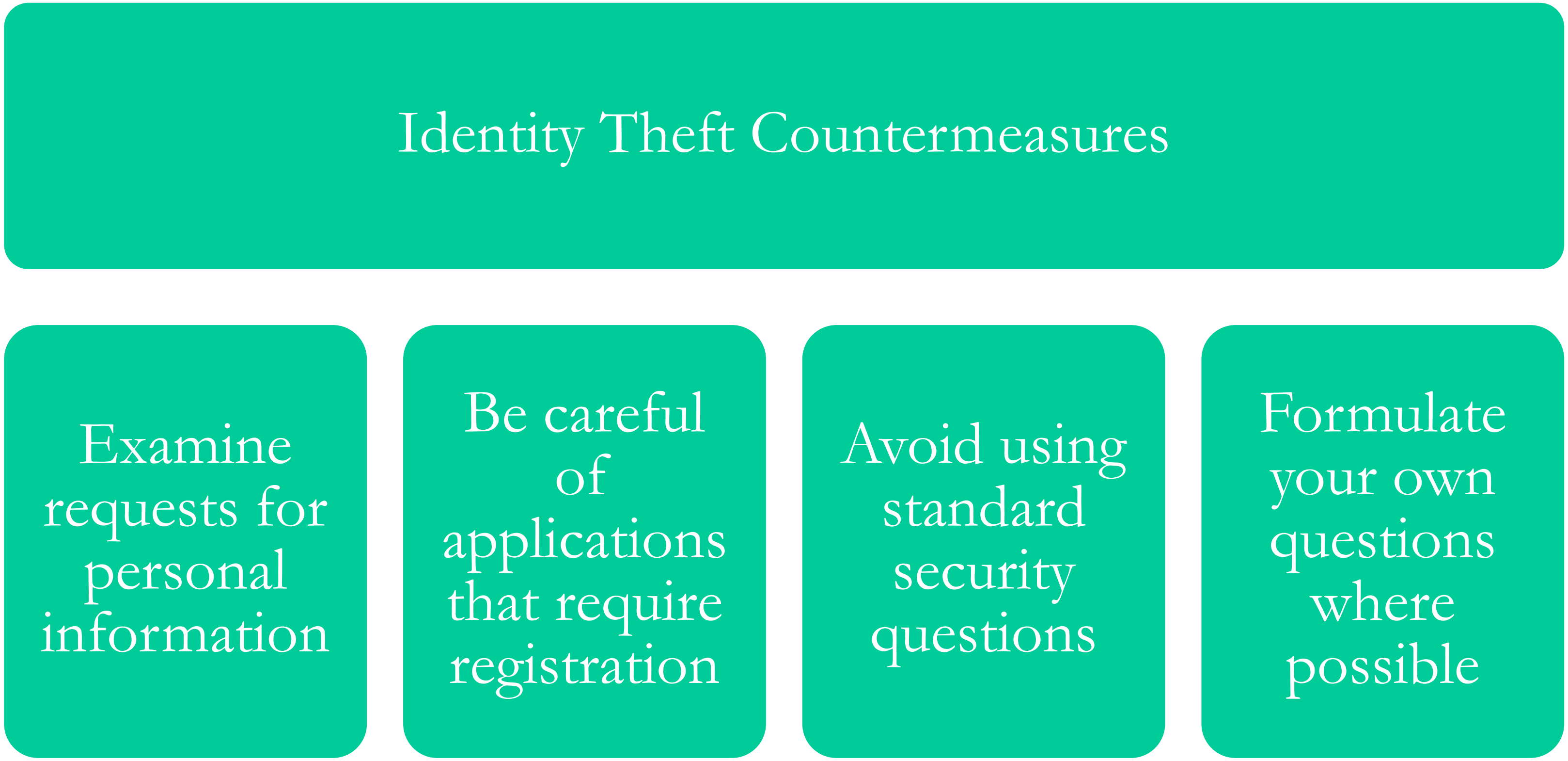
- Exercise caution on unsecured wireless networks.
- Be careful accessing sensitive information in a public place.
- Don’t save personal information casually on shopping websites.
- Be careful about posting personal information.
- Keep your computer personal.

Signs of Identity Theft

One of the most prominent and rapidly evolving threats is identity theft, which falls under the heading of social engineering.

- You see withdrawals that are unexplained.
- You don’t get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren’t yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn’t use.
- You get notice that your information was compromised by a data breach.

Protection Against Identity Theft



Identity Theft Countermeasures

Examine requests for personal information

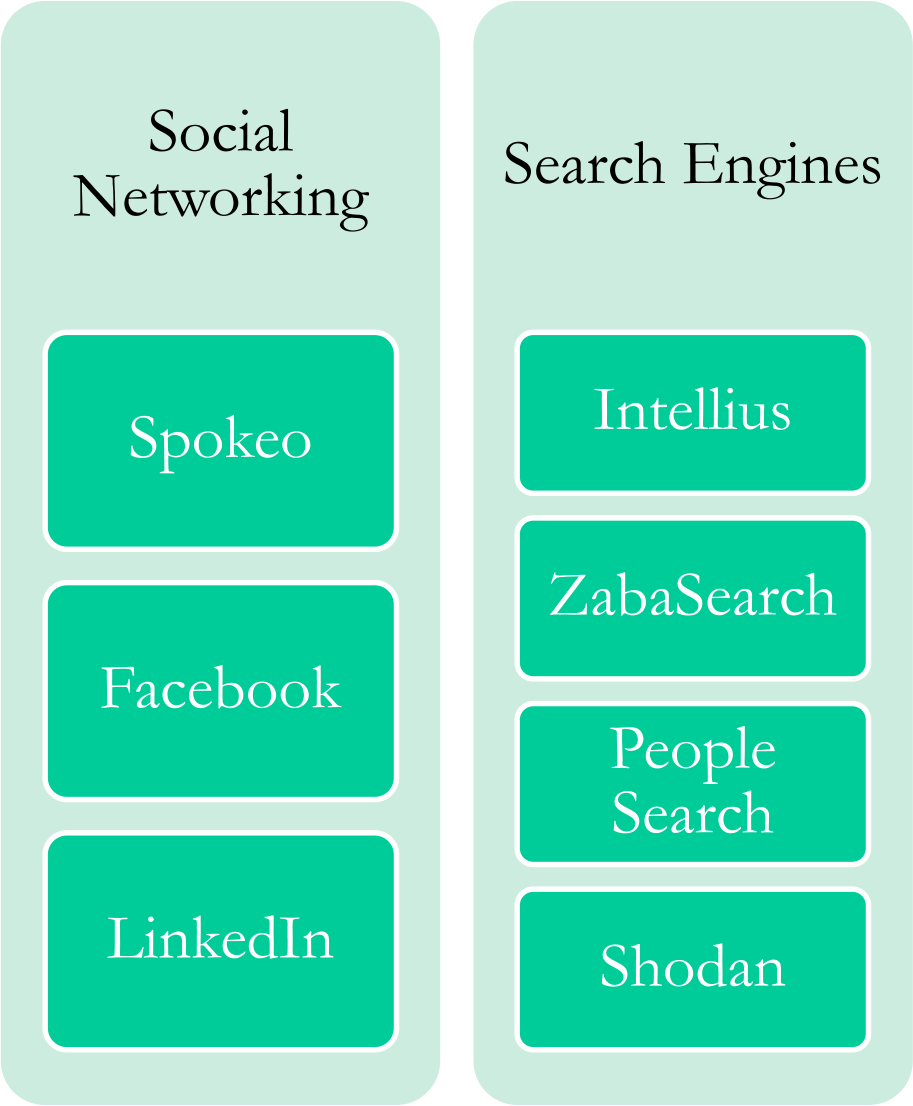
Be careful of applications that require registration

Avoid using standard security questions

Formulate your own questions where possible

In many cases, the only thing standing between someone and your money is a four- to six-digit number or a word or combination of words.

Finding Out About Yourself



Social Networking

- Spokeo
- Facebook
- LinkedIn

Search Engines

- Intellius
- ZabaSearch
- People Search
- Shodan

Summary

- What social engineering is
- How social engineering works
- Countermeasures