UNIT – V
Privacy Issues

Contents

1. Basic Data Privacy Concepts: Fundamental Concepts,
2. Data Privacy Attacks
3. Data linking and profiling
4. Privacy policies and their specifications
5. Privacy policy languages
6. Privacy in different domains- medical, financial, etc.

1. Fundamental Concepts - What is Data Privacy?

- Data privacy is a **part of the data protection area** that deals with the proper handling of data.

- **Data privacy relates** to how a piece of information—or data—**should be handled based on its relative importance**.

- Organizations need to learn how to process personal data while protecting privacy preferences of individuals.

1. Fundamental Concepts - What is Data Privacy? (contd..)

Why is Data Privacy Important?

1. When data that should be kept private gets in the wrong hands, bad things can happen.

2. A data breach at a government agency can, for example, put top secret information in the hands of an enemy state.

3. A breach at a corporation can put proprietary data in the hands of a competitor.

1. Fundamental Concepts - What is Data Privacy? (contd..)

Why is Data Privacy Important?

4. A breach at a school could put students’ PII in the hands of criminals who could commit identity theft.

5. A breach at a hospital or doctor’s office can put PHI in the hands of those who might misuse it.

2. Fundamental Concepts - What is PII?

Personally Identifiable Information is defined by the US Office of Privacy and Open Government as:

Information which can be used to distinguish or trace an individual's identity, such as

- their name,
- social security number,
- biometric records, etc. alone, or
- when combined with other personal or identifying information which is linked or linkable to a specific individual, such as
- date and place of birth,
- mother's maiden name, etc.

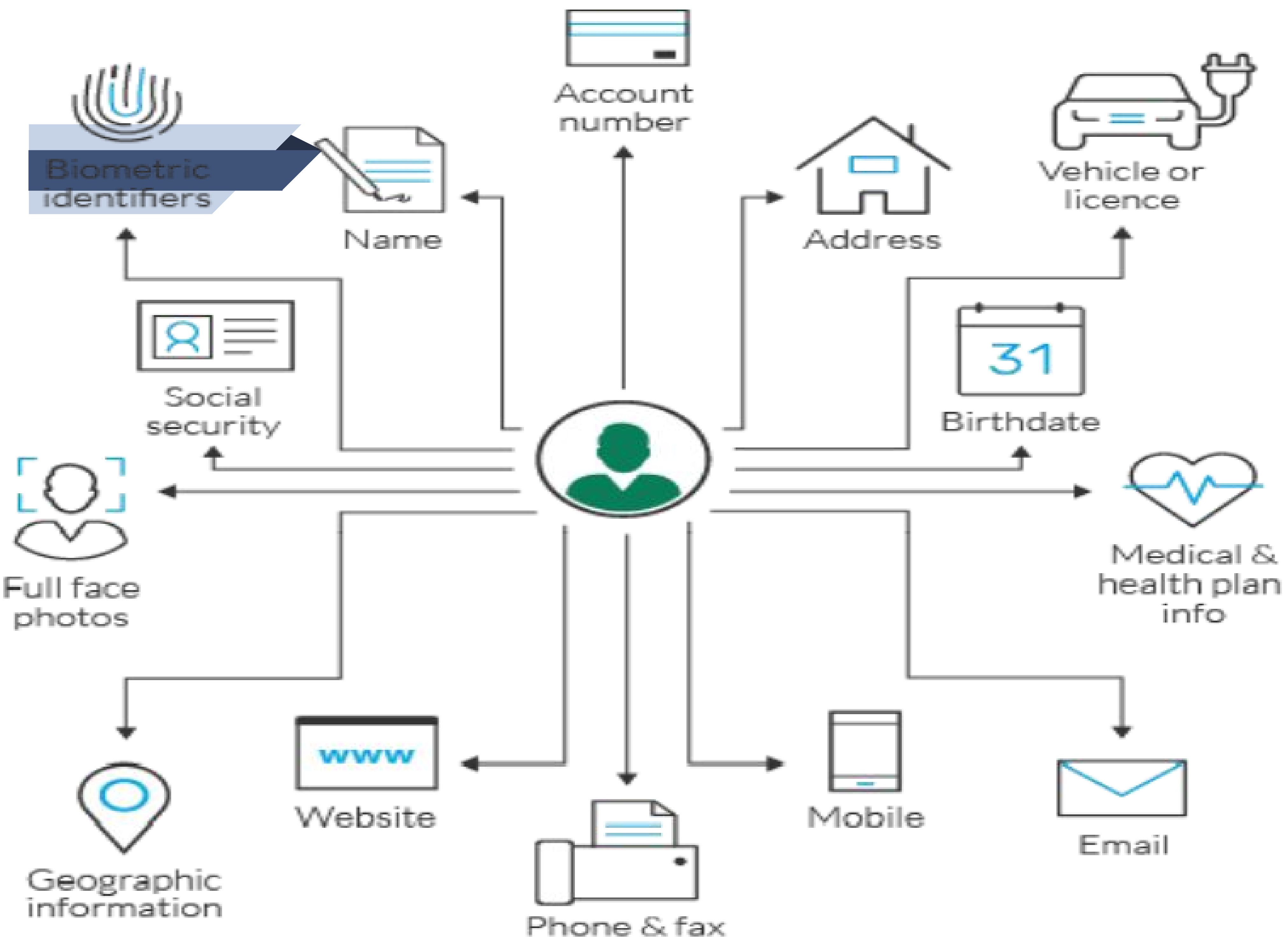
Some Important Aspects of Data Privacy

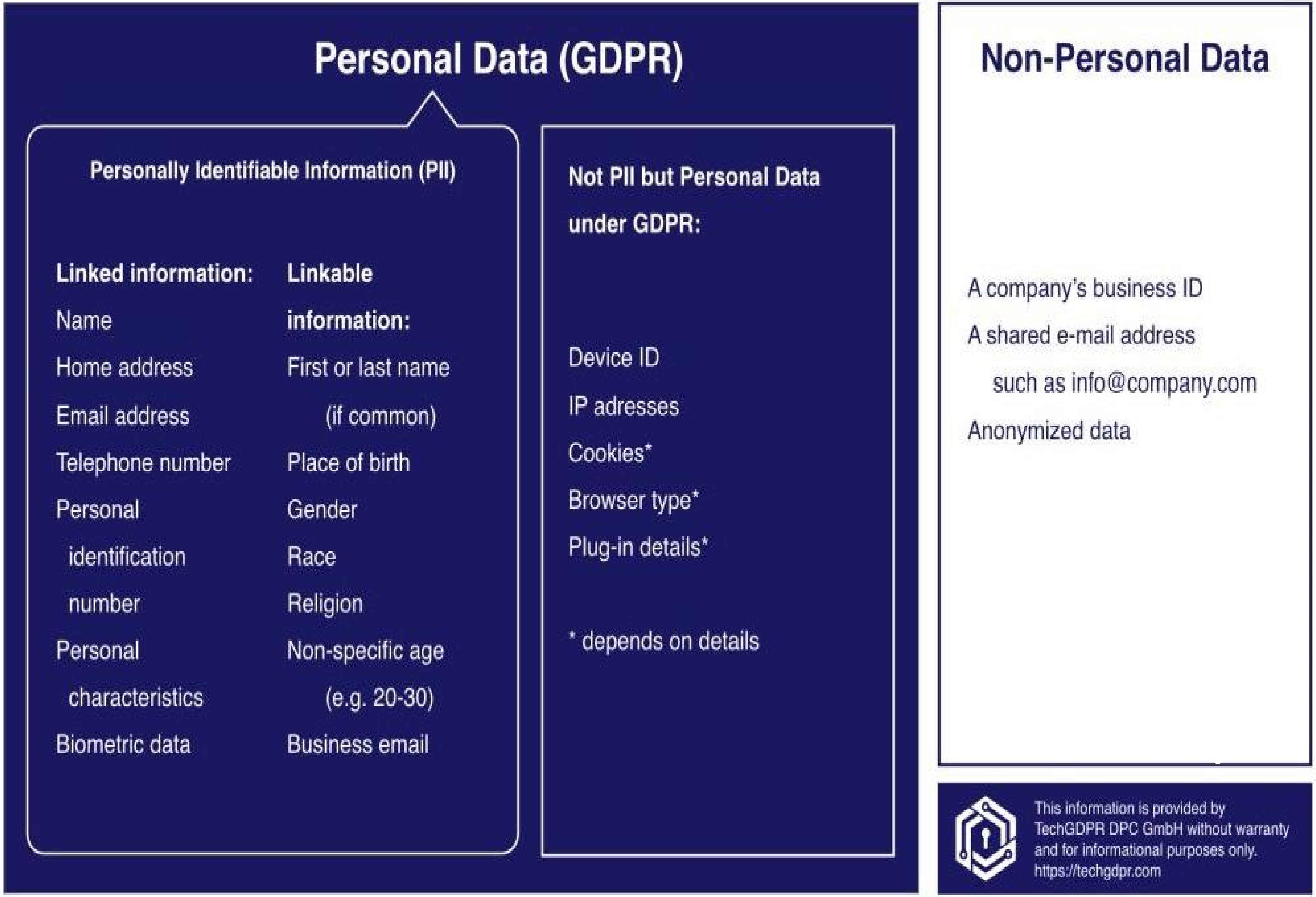
- Data Privacy is not the same as Data Security
- Privacy is the right to be left alone

Consequences of non-compliance:

More and more privacy regulations

worldwide are coming up


Biometric identifiers
Name
Account number
Address
Vehicle or licence
Social security
Birthdate
31
Full face photos
Medical & health plan info
Geographic information
www
Website
Phone & fax
Mobile
Email



Personal Data (GDPR)

Personally Identifiable Information (PII)

Linked information:

Name
Home address
Email address
Telephone number
Personal identification number
Personal characteristics
Biometric data

Linkable information:

First or last name (if common)
Place of birth
Gender
Race
Religion
Non-specific age (e.g. 20-30)
Business email

Not PII but Personal Data under GDPR:

Device ID
IP adresses
Cookies*
Browser type*
Plug-in details*

* depends on details

Non-Personal Data

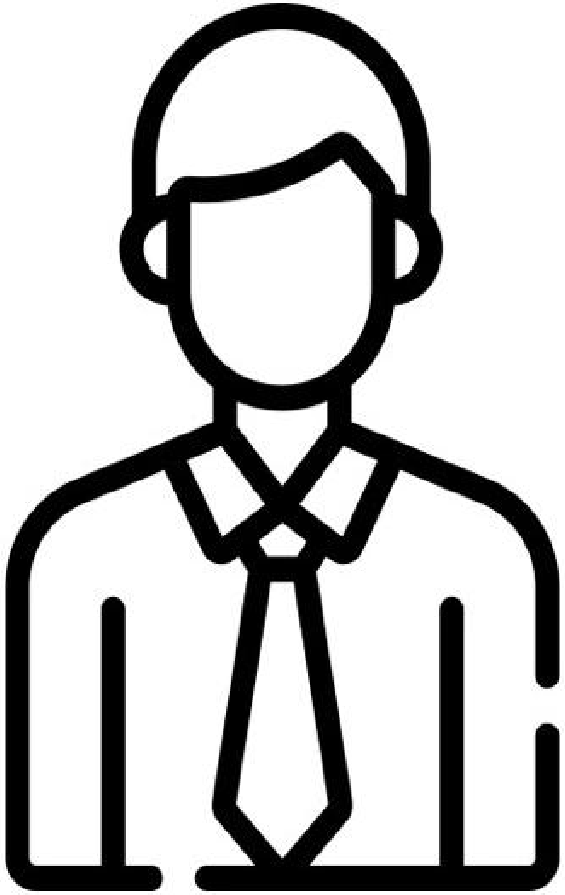
A company's business ID
A shared e-mail address such as info@company.com
Anonymized data

This information is provided by TechGDPR DPC GmbH without warranty and for informational purposes only.
https://techgdpr.com

General Data Protection Regulation (GDPR) in European Union (EU)

Special categories of personal data :

Data



- Philosophical beliefs
- Trade union membership
- Genetic data
- Medical data
- Religion
- Sexual orientation

Some Common Standards of Data Privacy

Personal Data Protection Bill (PDPB) India

- **Introduced in December of 2019**
- **Approved by Cabinet Ministry through Voice Vote.**
- **Applicable to whole India**

Companies all over India are already beginning to prepare. PDPB is modeled after GDPR although some of its policies aren't laid out as clearly and more discretion is given to India's Central Government to decide how it is enforced and when exceptions can be made.

Some Common Standards of Data Privacy

California Consumer Privacy Act (CCPA) USA

While there is currently no data privacy law applicable to all industries on the federal level, **every state in the Union has their own data privacy laws**.

These regulations vary significantly in terms of scope, applicability, and penalties, but the **strictest** among them **is** the recent **California Consumer Privacy Act (CCPA)**

Some Common Standards of Data Privacy

General Data Protection Regulation (GDPR) EU

- **It is the toughest privacy and security law in the world.**
- Though it was drafted and passed by the European Union (EU), it **imposes obligations onto organizations anywhere**, so long as they target or **collect data related to people in the EU**. The regulation was **put into effect on May 25, 2018.**
- The **GDPR will levy harsh fines against** those who **violate** its privacy and security standards, with penalties reaching into the tens of millions of euros.

Introduction to ISO 27701:2019

International Standards:

- **ISO 27701:2019: Privacy Information Management**
- **ISO 27001:2013: Information security management systems**

ISO 27701:2019 – Security Techniques - serves as a privacy extension to the ISO 27001:2013 and ISO/IEC 27002.

Specifies the requirements for – and provides guidance for the **establishment, implementation, maintenance and improvement of PIMS** (Privacy Information Management System) in an organization

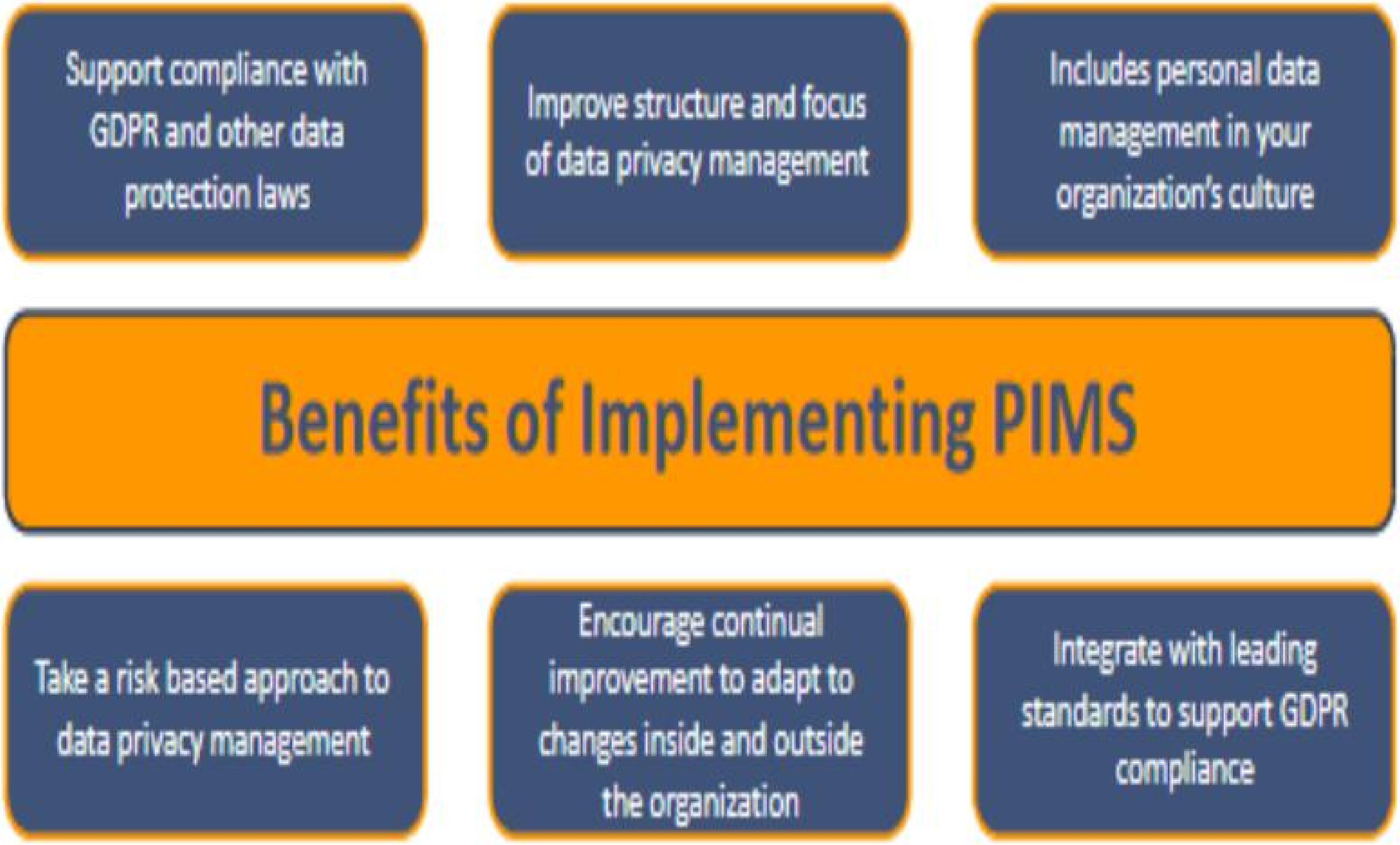
Introduction to ISO 27701:2019

The International Standard for Privacy Information Management

Based on the requirements, control objectives and controls of ISO 27001 **and includes a set of privacy-specific requirements, controls and controls objectives**

Published in August 2019

Benefits of Implementing PIMS



Support compliance with GDPR and other data protection laws

Improve structure and focus of data privacy management

Includes personal data management in your organization's culture

Benefits of Implementing PIMS

Take a risk based approach to data privacy management

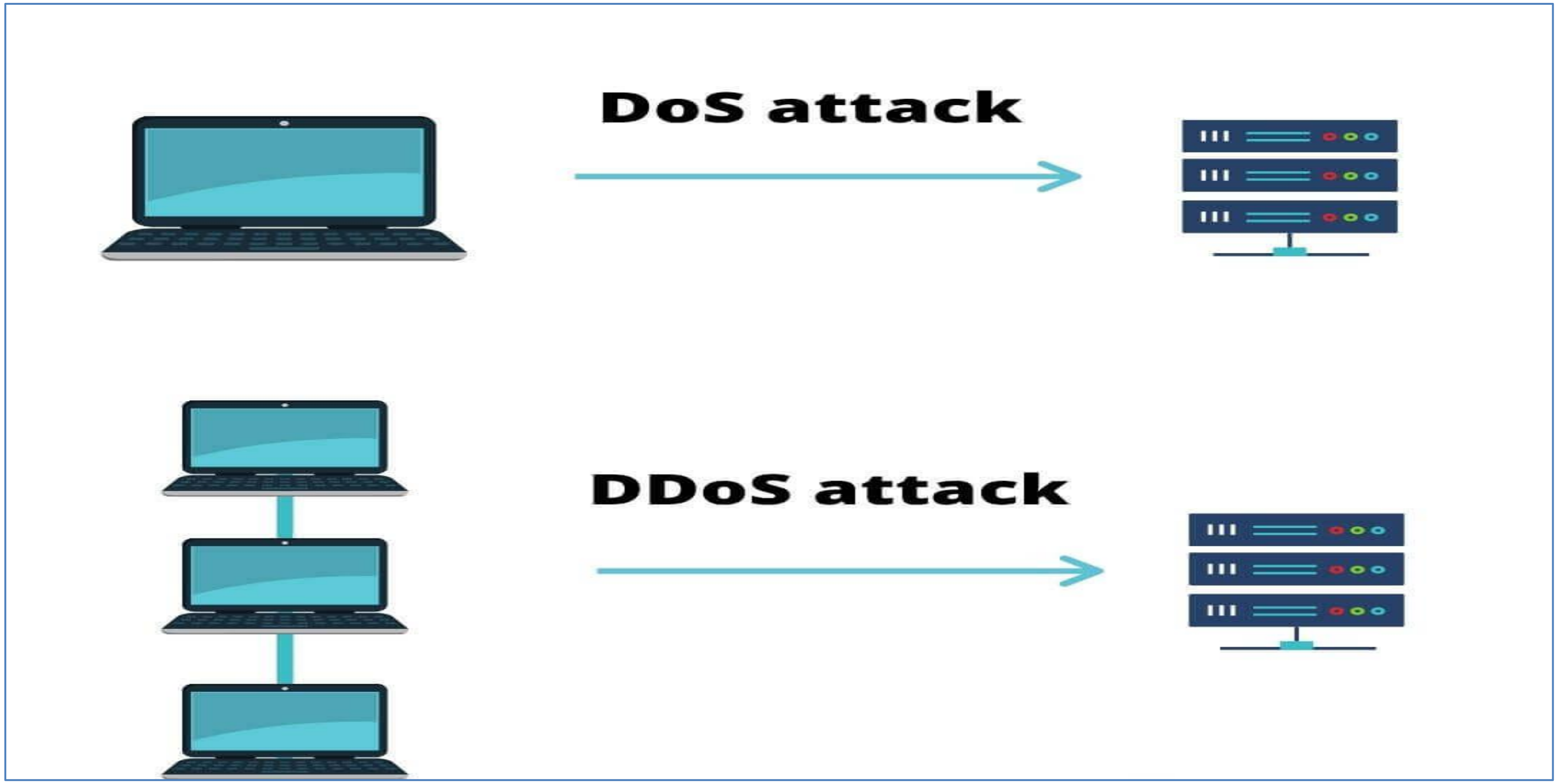
Encourage continual improvement to adapt to changes inside and outside the organization

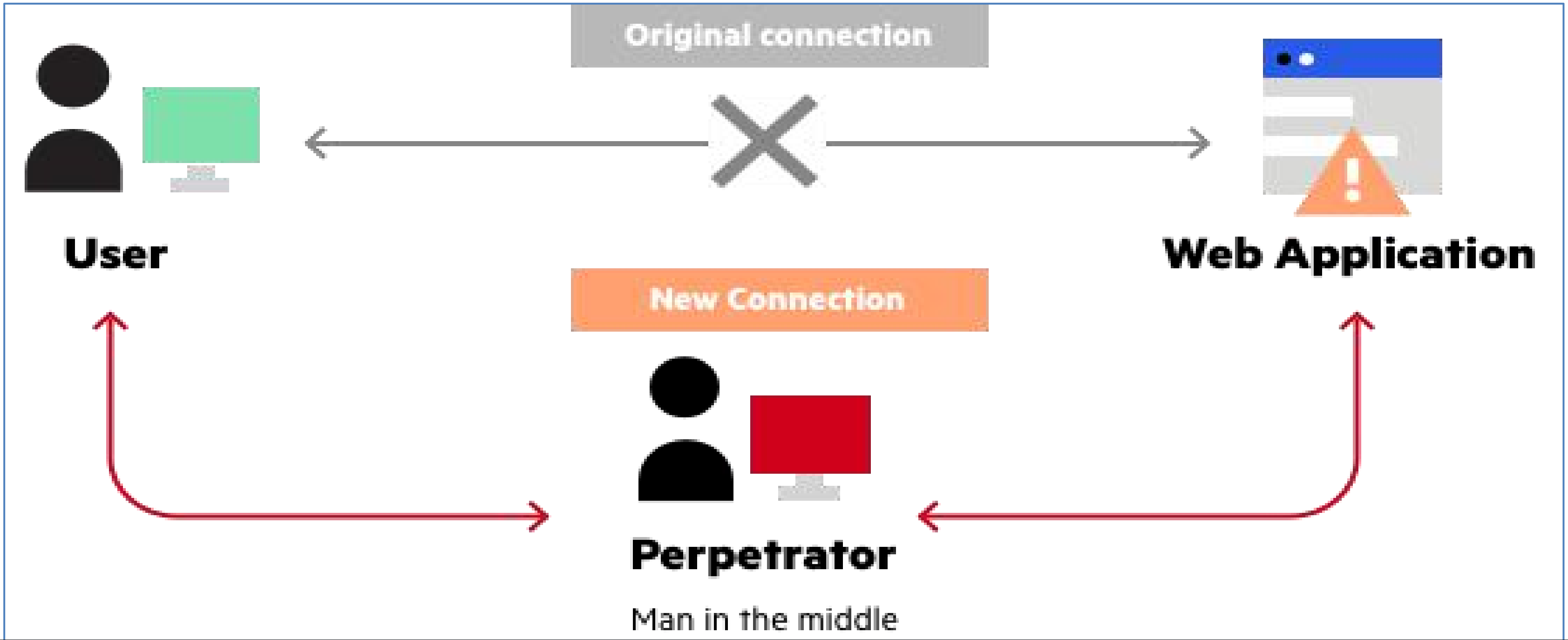
Integrate with leading standards to support GDPR compliance

3. Data Privacy Attacks

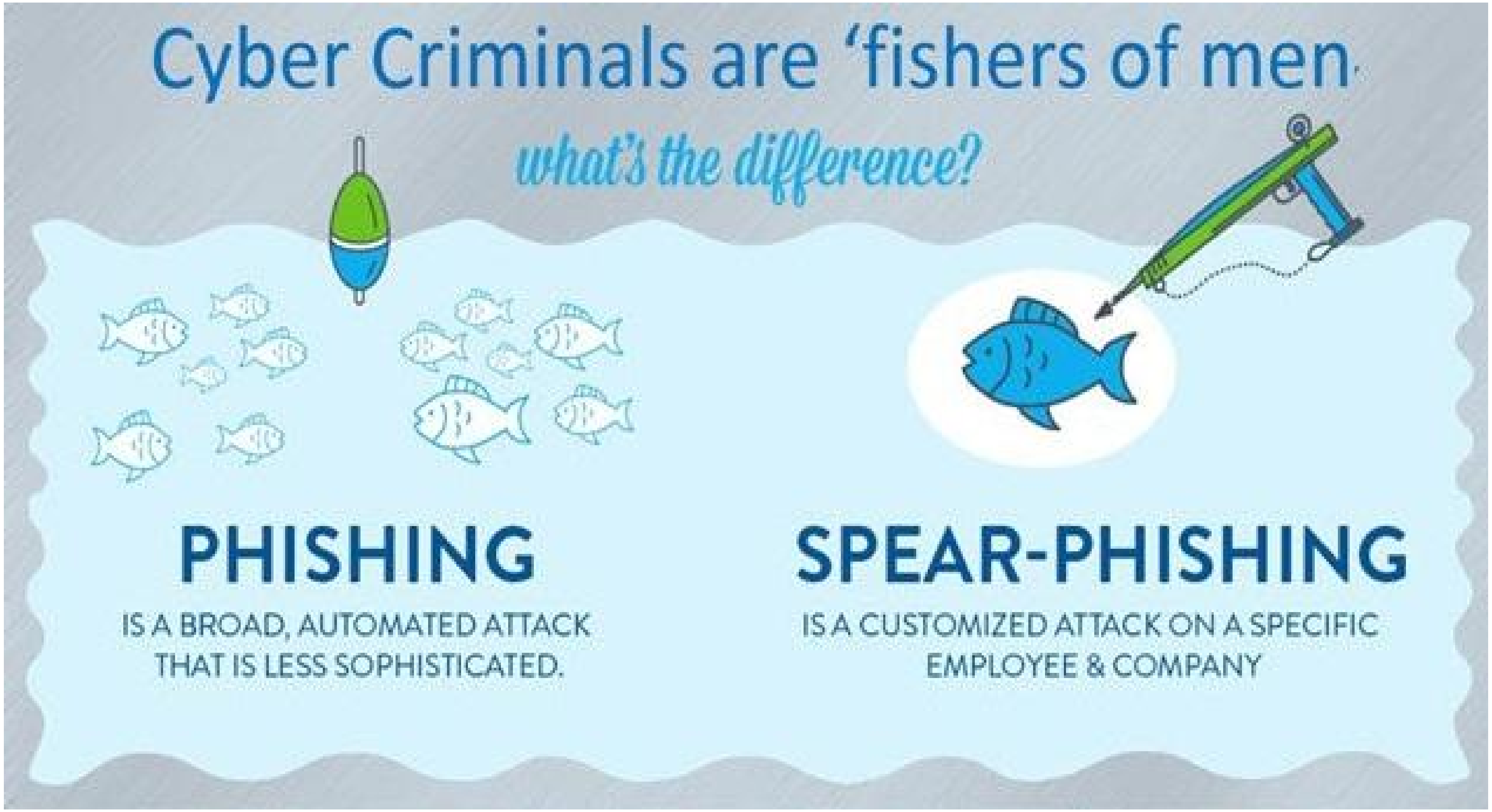
1. Denial of service (DOS) and distributed denial of service (DDoS) attacks
2. Man in the middle (MITM) attack
3. Phishing and spear phishing attacks

   Drive by attack
4. SQL injection attack
5. Cross-site scripting (XSS) attack


DoS attack
DDoS attack


Original connection
User
Web Application
New Connection
Perpetrator
Man in the middle

Phishing and Spear Phishing



Cyber Criminals are 'fishers of men'

what's the difference?

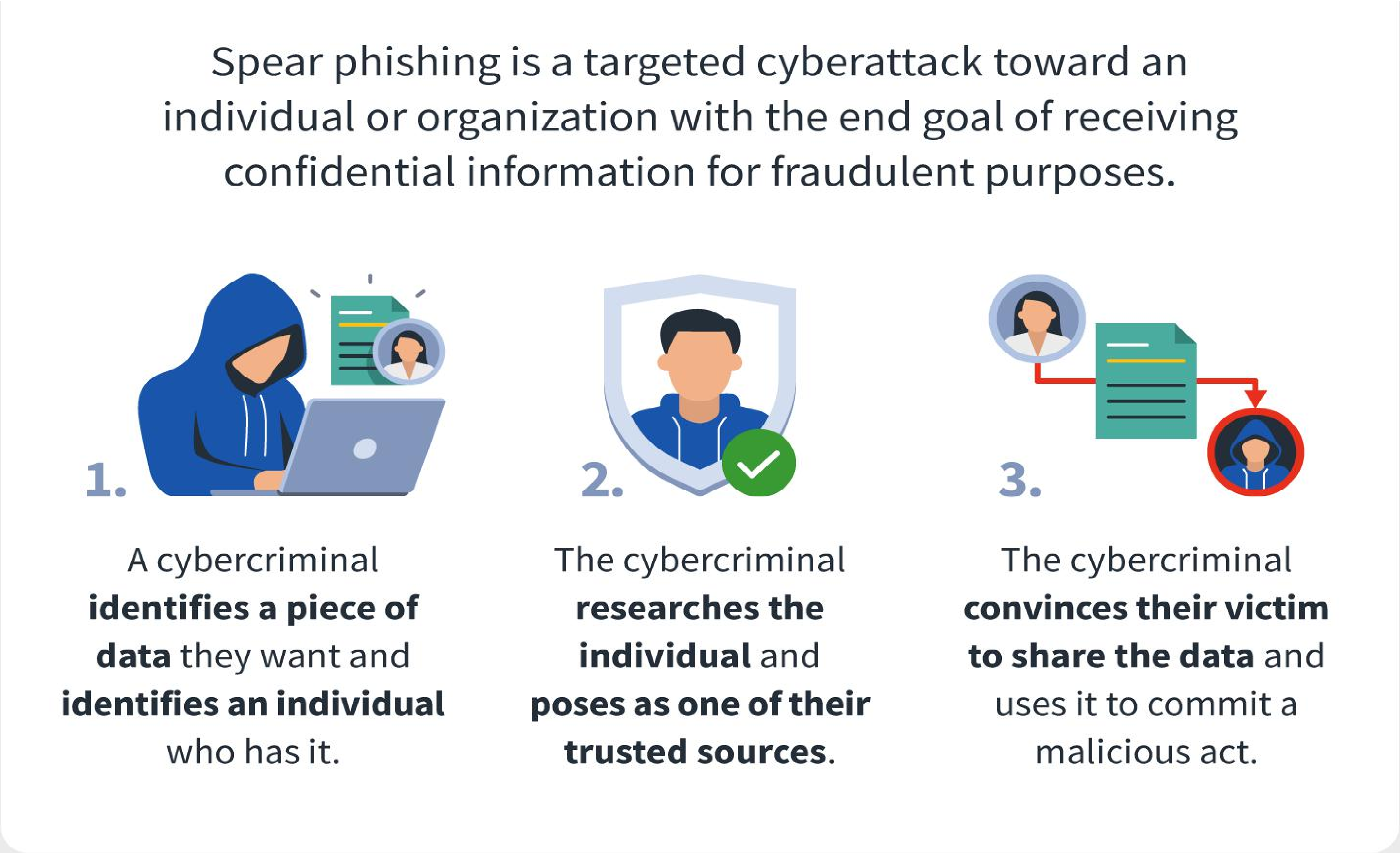
PHISHING

IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.

SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

Spear Phishing



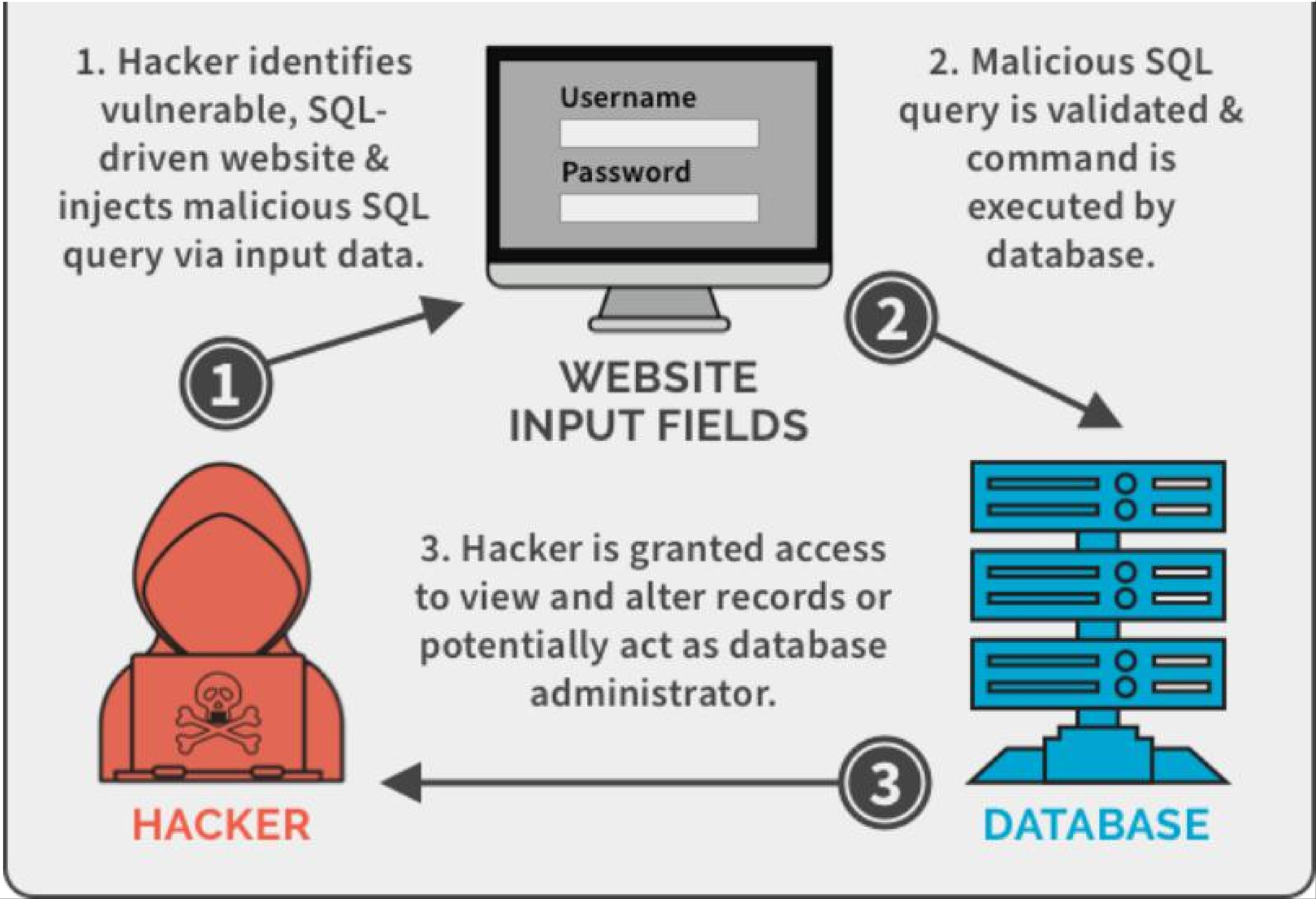
Spear phishing is a targeted cyberattack toward an individual or organization with the end goal of receiving confidential information for fraudulent purposes.

1. A cybercriminal **identifies a piece of data** they want and **identifies an individual** who has it.

2. The cybercriminal **researches the individual** and **poses as one of their trusted sources**.

3. The cybercriminal **convinces their victim to share the data** and uses it to commit a malicious act.

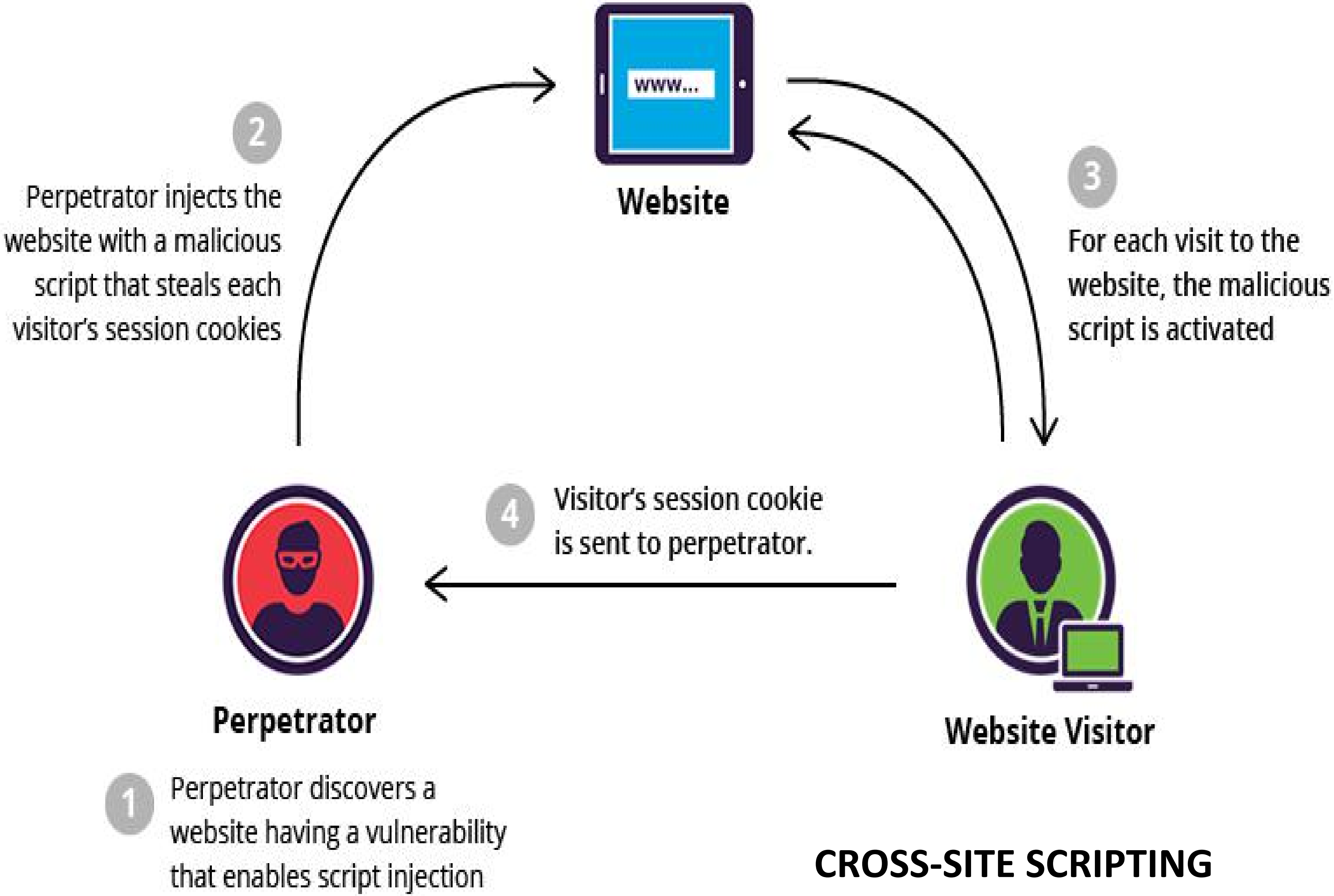
SQL Injection Attack



1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.

2. Malicious SQL query is validated & command is executed by database.

3. Hacker is granted access to view and alter records or potentially act as database administrator.



1 Perpetrator discovers a website having a vulnerability that enables script injection

2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies

3 For each visit to the website, the malicious script is activated

4 Visitor's session cookie is sent to perpetrator.

CROSS-SITE SCRIPTING ATTACK

4. Data Linking and Profiling

Data linking is used to bring together information from different sources in order to create a new, richer dataset. This involves identifying and combining information from corresponding records on each of the different source dataset.

Data linkage is done by assigning an identifying number to each person on a dataset and storing a set of links to all records for the person. The TDLU is responsible for creating and maintaining the links between the main state wide health **data** collections and other approved **data** sources in Tasmania.

4. Data Linking and Profiling (contd..)

- **Profile linking** - Important method used in link building.
- A tactic used by SEO professionals in order to gain do follow / no follow backlinks from reputed websites.
- In profile link, you simply add your website's URL to a personal, professional or any business profile, which you create on different sites.
- Getting profile links from such site provides quality backlinks and such links carries more weight and are more beneficial to your site.

NIST Privacy Framework

Overview of the Privacy Framework

Cybersecurity and Privacy Risk Management

Privacy Policies and Their Specifications

- A **Privacy Policy** is not only the legally required document to disclose your practices on protecting personal information, but it's also great way to show users that **you can be trusted**, and that you have procedures in place to handle their personal information with care.

- **Privacy Notice(or Privacy Statement)** A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.
- A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.

What to Include in Privacy Policy?

- Collection
- Use and Disclosure
- Information Quality
- Data Security
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Transborder Data Flows
- Sensitive Information

Privacy Policies and Their Specifications

1. **Collection**: Collection of personal information must be fair, lawful and not intrusive. A person must be told the following:
   1. organization's name,
   2. the purpose of collection,
   3. any laws requiring the collection,
   4. the main consequences if all or part of the information is not provided, and
   5. that the person can get access to their personal information.

2. **Use & Disclosure**: An organization should only use or disclose information for the purpose for which it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would expect such disclosure.

Privacy Policies and Their Specifications

3. **Information Quality :** An organization must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to date.

4. **Data Security:** An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.

Privacy Policies and Their Specifications

5. **Openness:** An organization must have a policy document outlining its information handling practices and make this available to anyone who requests it.

6. **Access and Correction:** An organization must give an individual access to personal information it holds about that individual.

7. **Identifiers:** An organization must not adopt, use or disclose an identifier that has been assigned by a Commonwealth government 'agency'. For example, a tax file number or Medicare number.

Privacy Policies and Their Specifications

8. **Anonymity:** Organizations must give people the option to interact anonymously whenever it is lawful and practicable to do.

9. **Transborder Data Flows:** An organization can only transfer personal information to a recipient in a foreign country in circumstances where it is necessary to do so to complete an agreement with a person, or where the information will have appropriate protection or the person has consented to the transfer.

10. **Sensitive Information:** An organization must not collect s information (for example, details of a person’s race, religion, sexual preferences or health) unless the individual has consented.

A few PII Security Controls

- Change Management
- Data Loss Prevention
- Data masking
- Privileged user monitoring
- User Rights Management
- Secure audit trail archiving

A few PII Security Controls (contd..)

1. **Change Management—**tracking and auditing changes to configuration on IT systems which might have security implications, such as adding/removing user accounts.

2. **Data Loss Prevention—**implementing systems that can track sensitive data transferred within the organization or outside it, and identify unnatural patterns that might suggest a breach.

3. **Data masking—**ensuring that data is stored or transmitted with the minimal required details for the specific transaction, with other details masked or omitted.

A few PII Security Controls (contd..)

4. **Privileged user monitoring—**monitoring all privileged access to files and databases, user creation and newly granted privileges, blocking and alerting when suspicious activity is detected.

5. **User rights management—**identifying excessive, inappropriate, or unused user privileges and taking corrective action, such as removing user accounts that have not been used for several months.

6. **Secure audit trail archiving—**ensuring that any activity conducted on or in relation to PII is audited and retained for a period of 1-7 years, for legal or compliance purposes.

Privacy in Different Domains

What is Domain Privacy?

- Domain privacy (often called Whois privacy) is **a service offered by a number of domain name registrars**.
- A user buys privacy from the company, who in turn replaces the user's information in the WHOIS with the information of a forwarding service (for email and sometimes postal mail, it is done by a proxy server).

Privacy in Different Domains (contd..)

- Every domain name has a WHOIS listing, which is a searchable database of registered domains. It is available to everyone on the Internet.
- Without domain privacy, or WHOIS privacy protection, all of your contact information (address, phone number, name, etc.) is available to the public.

Privacy in Different Domains (contd..)

What are the benefits of Domain Privacy and Protection?

- With Full Domain Privacy & Protection, your **domain is protected from domain hijacking and honest mistakes** like accidental transfer or an expired credit card. It also prevents spam with a private email address for domain inquiries.

- Full Domain Privacy & **Protection puts your domain on lockdown, making inadvertent, accidental or malicious transfers virtually impossible.**

- Plus, it will extend your domain's renewal period in case of an expired credit card and billing failure.

Privacy policy languages

- Most Privacy Policies are published in English.
- While this may not seem like the most considerate approach in non-English speaking countries, **it is not required for Privacy Policies to be available in a country's native language**.

Privacy in different domains- medical, financia

5 Industries with the Strictest Data Privacy Compliance Rules

1. Data Based Industries
2. Educational Institutions
3. Online Financial Services
4. Medical and healthcare
5. Utility Sector

Rules to be followed

First, they limited the use of both authorized and third-party data by introducing the following rules:

1. Consent-based data sharing and data selling
2. The right to opt-out from any data permission
3. Customer’s request to delete their whole history
4. Obligation to deliver customer data in an easily downloadable format

Rules to be followed (contd..)

5. Data breach notification period of 72 hours since the breach was detected
6. Use of plain language is required, meaning there is no more space for complex marketing and legal jargon