Data Privacy:
A Guide for Individuals and Families

Protect your online information and safeguard your digital footprint.

panda

Table of Contents

01.
Data Privacy Basics

In the digital age, data privacy has become an unsung protagonist. It's the mysterious figure lurking behind every email sent, every transaction made and every site visited. Yet, for many, data privacy is a foreign concept often overlooked until it's too late.

Data privacy is about keeping your personal information secure. Companies, governments and cybercriminals all seek this information for various reasons, making it vital to understand how to keep data protected. Luckily, this comprehensive e-book on data privacy provides the information you need to claim control of your digital footprint.

What Is Data Privacy?

Data privacy is the control an individual or organization has over sensitive information stored or collected about them. It is the ability to determine who has access to this data, how it's used and the safeguards in place to protect it from unauthorized exposure.

Personal data associated with data privacy includes sensitive information like names, addresses, Social Security numbers and financial data. It also extends to less overtly personal data like browsing history, location data, IP addresses and online purchases. Further, it may encompass biometric data, health care records and employment details.

The concept of data privacy traces its roots to the early days of computing, where personal information was stored electronically for various purposes. As the digital landscape expanded, concerns regarding data misuse and privacy breaches rapidly increased.

The evolution of social media further compounded these concerns. With users freely sharing personal information on platforms like Facebook and Twitter, the amount of data being generated has reached unprecedented levels.

Why Data Privacy Matters

With technology advancing at breakneck speed, the importance of data protection and privacy is no longer optional — it's a requirement. Data privacy hinges on allowing individuals to control their digital footprint.

Every time we connect to the internet, we generate an extensive amount of data. From simple social media likes to our shopping habits, this seemingly innocuous data paints a vivid picture of who we are.

When this private data ends up in the wrong hands, repercussions can include:

Identity theft

Personal data could fall into the wrong hands, leading to identity fraud, where individuals could face unauthorized transactions or criminal activity conducted under their name.

Financial fraud

With access to sensitive financial information, cybercriminals could carry out fraudulent transactions, leading to serious monetary loss.

Legal repercussions

Without adherence to data privacy laws and regulations, companies could face heavy fines and legal actions, damaging their reputation and finances.

Lack of trust

Companies could lose their customers' trust, impacting customer loyalty and leading to business loss.

Increased cybercrime

The risk of cyberattacks could increase as more valuable data becomes easily accessible to hackers.

Loss of privacy

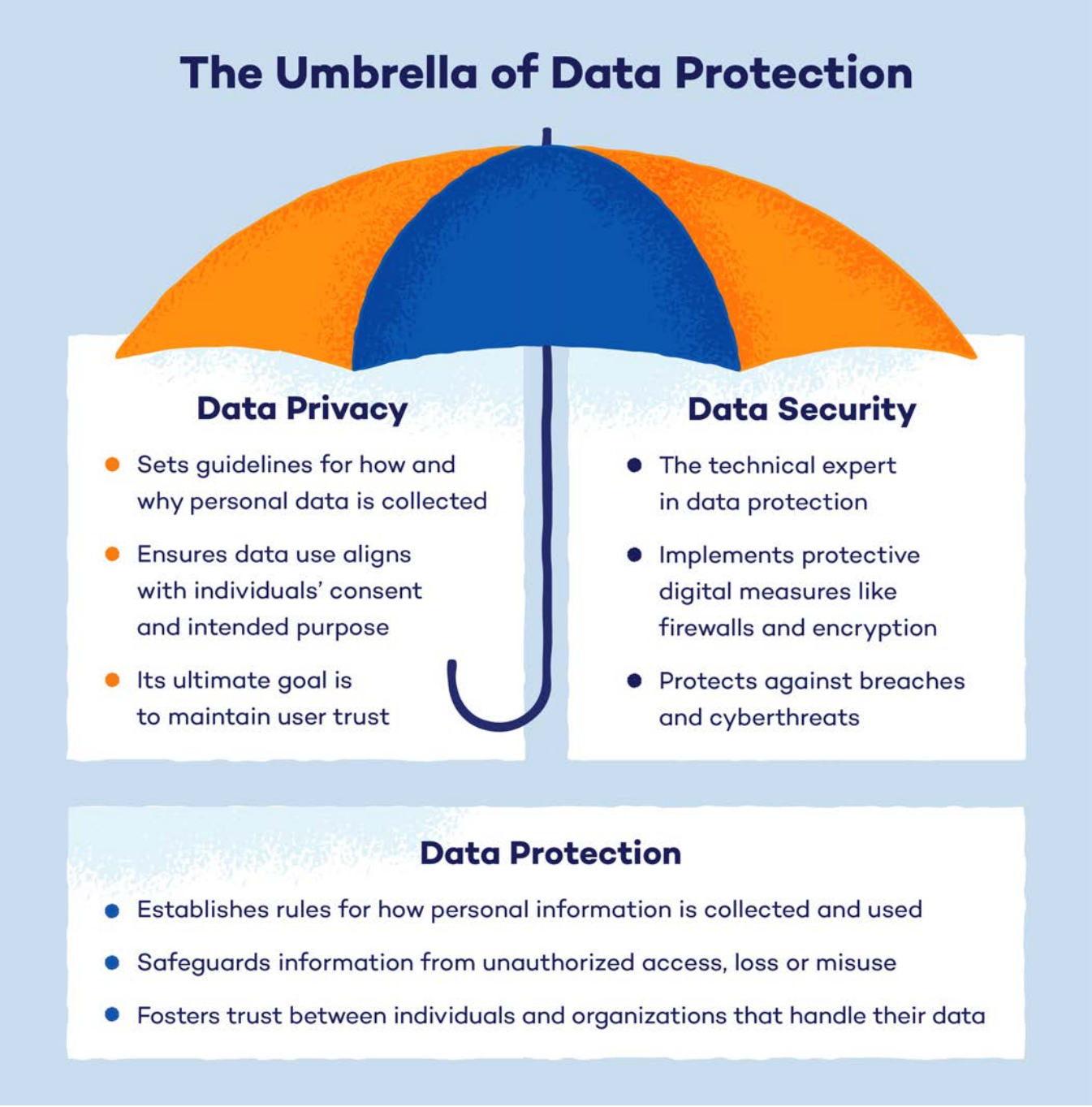
Without data privacy, our personal lives could become an open book accessible to anyone.

Manipulation and exploitation

Data could be used to manipulate behavior and decisions, often without an individual's knowledge or consent.

Data Protection vs. Data Privacy vs. Data Security

Data protection, data privacy and data security are three intertwined yet distinct concepts in the world of digital data.



In short, data protection, data privacy and data security work in harmony. Each has a distinct role, but together, they create a secure digital environment.

02.
Personal and Sensitive Personal Information

In the vast landscape of data privacy, understanding the distinction between personal and sensitive personal information is crucial for legal compliance, risk management and ethical considerations. It informs data handling practices, guides security measures and helps minimize potential harm to individuals if data is compromised.

This section unravels the layers of data classification with insights on how to safeguard the most intimate details of your digital identity.

What Is Personal Information?

Personal information, often called personal data, is any information that can be used to identify a specific individual. It encompasses a wide range of data that could be linked to a particular person. Depending on the context, it can contain names, addresses, phone numbers and more.

How to Control Your Personal Information

To effectively control your personal information, it's essential to adopt proactive measures that enhance your online privacy and security. Let's look at some important tips to keep in mind.

Limit social media exposure

Review and adjust your privacy settings on social media platforms to control who can see your posts and personal information.

Think before you post

Before sharing personal details online, consider the potential consequences and whether disclosing that information is necessary.

Read privacy policies

Take the time to read and understand the privacy policies of websites and apps you use to know how your data is collected, stored and shared.

Opt out of data collection

Opt out of data collection whenever possible and choose services that only ask for essential information.

What Is Sensitive Personal Information?

Sensitive personal information is a category of personal information that is considered more critical and requires higher levels of protection. It includes details that, if exposed, could lead to serious consequences such as identity theft, cyberstalking or discrimination.

How to Control Your Sensitive Personal Information

These days, controlling your sensitive personal information is more crucial than ever. With the rise of data breaches and other cyberthreats, it's essential to take proactive steps to safeguard this valuable data.

Submit a Data Subject Access Request (DSAR) Form

- **Know your rights:** Under the General Data Protection Regulation (GDPR), you have the right to ask an organization whether or not it is processing your data.
- **Access information:** A data subject access request (DSAR) allows you to gain access to stored information about you and understand its usage.
- **Demand rectification:** Demand rectification of incorrect data or its deletion; companies are required to comply within one calendar month for GDPR and 45 days for the California Consumer Privacy Act (CCPA).

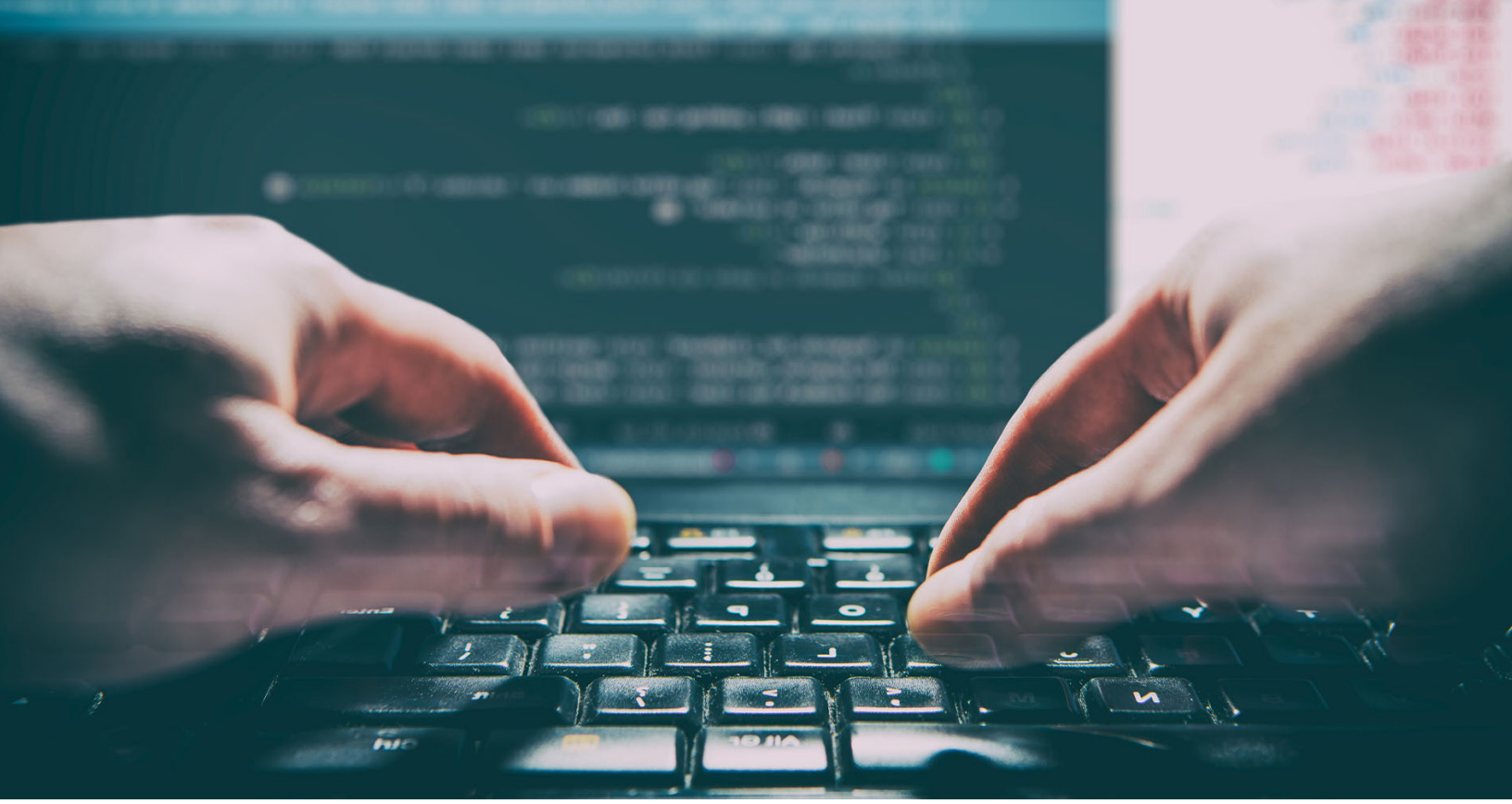
Use "Do Not Sell or Share My Personal Information" Links

- **Check business websites:** Look for expanded options like "Do Not Sell or Share My Information" under the California Privacy Rights Act (CPRA) on business websites' homepages and privacy policy pages.
- **Opt out:** Opt out of having your personal or sensitive personal information sold or shared with third parties; businesses are legally obligated to comply.

Opt Out of Collection on Websites or Browsers

- **Perform an online search:** Conduct an online search for your name to find data broker websites like Radaris, Pipl, Spokeo and Whitepages listing your information.
- **Request data removal:** Visit the opt-out pages of these platforms or send an email request to have your data removed.
- **Utilize resources:** Utilize resources like the Privacy Rights Clearinghouse for a comprehensive directory of websites and their opt-out options.
- **Review privacy policies:** Review the privacy policies of your financial institutions to opt out of data sharing with brokers.

03.
Understanding Data Breaches



You've probably heard of companies having massive data breaches and thought, **"How did that happen?"** or **"What if I had been affected?"** A data breach can be scary, and can also have serious outcomes like payment card fraud or even identity theft.

Here's a deeper look into how data breaches can affect you, how they happen and how to prevent them.

What Is a Data Breach?

A data breach is a security incident where private, confidential or sensitive information is exposed or stolen by someone without authorization. They happen for various reasons, from human error to malicious attacks, and the consequences can be significant. Anyone is at risk of a data breach, especially if their accounts aren't protected.

Data breaches can result in:

Stolen credentials
Example: Hackers gained unauthorized access to a database containing the usernames and passwords of a social media platform's users, leading to widespread account takeovers and misuse of personal information.

Identity theft
Example: A cybercriminal used stolen personal information, such as Social Security numbers and addresses, to fraudulently apply for loans and credit cards in the victims' names, causing financial damage and identity-related issues.

Compromised assets
Example: Malware infected a company's network, allowing attackers to control critical systems and sensitive data, disrupting operations and causing significant financial losses.

Third-party access to accounts
Example: A cloud service provider experienced a data breach, allowing unauthorized third parties to access sensitive files and information stored by its clients, leading to potential data leakage and privacy violations.

Payment card fraud
Example: A cyberattack targeted an online retailer's payment processing system, resulting in the theft of customers' credit card information, which was then used to make unauthorized purchases.

How Do They Happen?

Data breaches can be a type of cybercrime if done maliciously, but they can also be an unintentional error from someone with authorized access to the data.

The causes of data breaches include:

Malicious insiders

People with access to the database intentionally misuse their access privileges to steal or leak sensitive information.

Malicious outsiders

Someone from outside the organization attacks a database via phishing, malware, vulnerability attacks or denial of service (DoS) attacks.

Accidental insiders

Individuals with authorized access accidentally expose data due to mistakes or lack of security measures. This is technically classified as a data leak since it's an internal mistake; however, it still has the same consequences for those affected, and the company may still face legal ramifications.

Phases of a Data Breach

Unlike what your imagination may suggest, a malicious data breach looks less like someone dressed in all black sneaking into a building with a flash drive and more like people in a remote location scheming about how to hack into a database.

However, not every data breach is malicious. Some result from human error or negligence, but we'll go over that more in the next section.

Here are the three stages of an intentional data breach.

1. Research

At the very beginning of a data breach, an attacker picks a target — usually a company or organization with access to personal data — and researches how they can infiltrate their target's database.

The attacker gathers details like employee information, financial records and security budgets. They also look for vulnerabilities like weak passwords, outdated software or unprotected network connections.

2. Attack

Taking what they've learned from their research, the attacker can now attack the data system. Here are some common ways attackers gain access to company systems or networks:

- **Stolen credentials:**
  They can collect compromised usernames and passwords through the dark web, phishing, brute force attacks or even physical theft of devices to impersonate legitimate users and gain access to systems.

- **Phishing emails**
  Attackers also use personal information from their research, like job titles or coworkers' names, to trick their targets into providing credentials or clicking a malicious link that downloads malware onto their computer.

- **Malware**
  Hackers use malicious software to secretly infect and take control of a victim's computer or network to steal data.

- **Vulnerability exploitation**
  The attacker uses vulnerabilities like weak passwords, misconfigurations or unpatched systems found within a company's computer system to gain access.

- **Denial of service (DoS) attacks**
  This attack overwhelms a website with excessive fake traffic until it's unavailable to actual users. It's a distraction from other security weaknesses so attackers can carry out data breaches.

3. Extract Data

Once the attackers have gained access to the target's system or network, they can locate and extract valuable or sensitive data, including personal information, financial records or any other data they can sell on the dark web.

The extracted data is then copied or transferred to the attacker's own servers, where they can control and exploit it. Oftentimes, a company won't know its data has been stolen until a third party, like law enforcement, service providers or customers, reports the breach.

04.
Protecting Yourself and Your Information

There are some simple ways to stay safe online. Panda Dome has a protection plan for any lifestyle, so you can browse without worry.

Network Security

Network security involves implementing measures to protect computer networks from unauthorized access, cyberattacks and data breaches. This includes securing network infrastructure, monitoring traffic and implementing robust encryption protocols.

Use public Wi-Fi safely

Employ caution when connecting to public Wi-Fi networks to prevent unauthorized access to sensitive data.

Use a VPN

Enhance online privacy and security by encrypting internet traffic when accessing public networks.

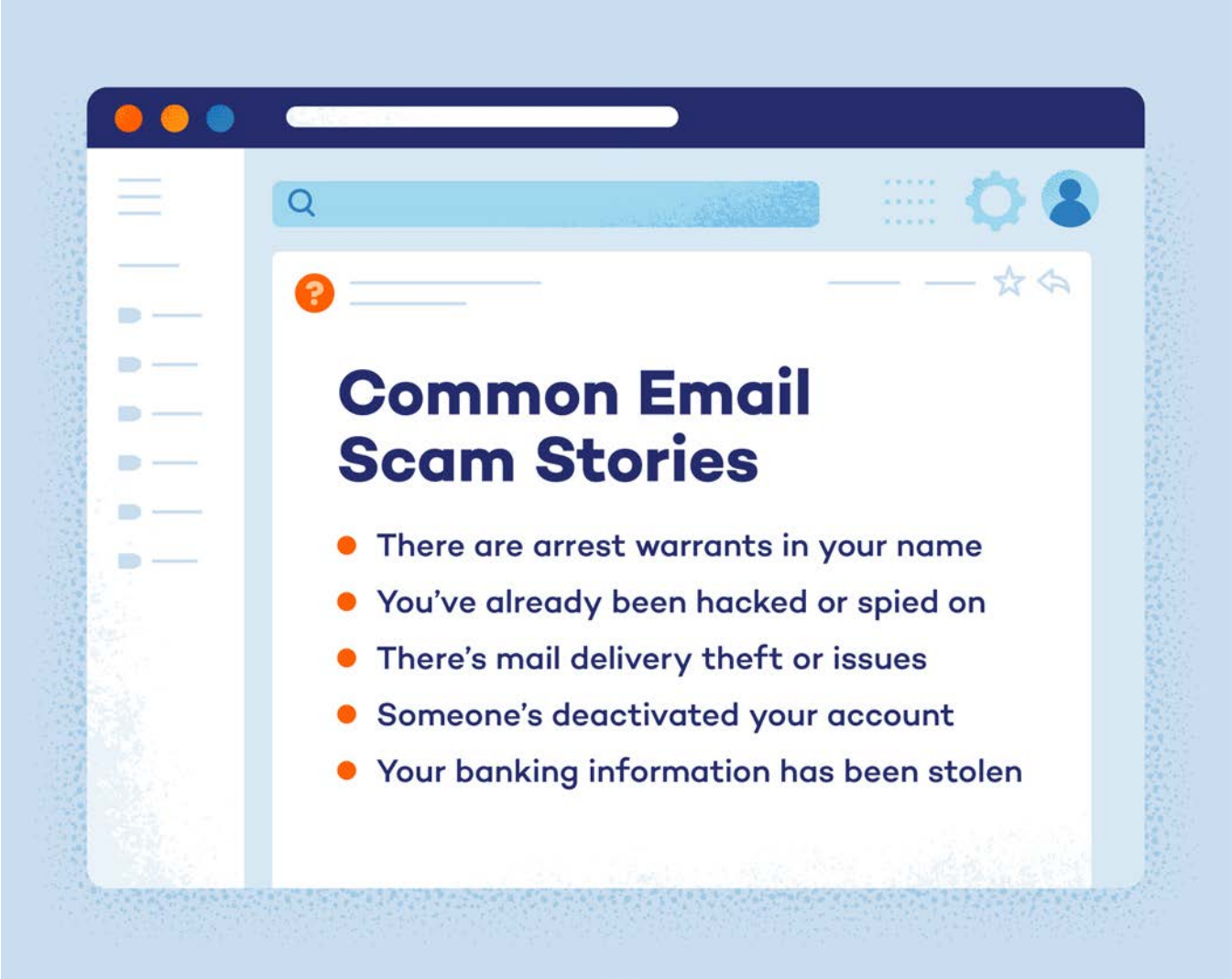
Install a firewall

Implement a barrier against unauthorized access to your network, providing an additional layer of defense against cyberthreats.

Authentication and Access Control

Authentication and access control are essential components of data privacy, ensuring only authorized individuals or systems can access sensitive data or resources. These measures verify the identity of users and enforce restrictions on their actions within a network or system.

- **Choose secure and unique passwords**
  Strengthen account security by creating complex passwords that are unique for each account to mitigate the risk of unauthorized access.
- **Set up two-factor authentication**
  Add an extra layer of security by requiring a secondary form of verification, such as a code sent to a trusted device, in addition to a password.
- **Monitor account information**
  Regularly review account activity to detect suspicious behavior or unauthorized access attempts. Promptly report any suspicious activity or unauthorized access attempts to relevant authorities or service providers.
- **Never share codes you receive via text or email**
  Avoid sharing verification codes received through text or email, as they could be intercepted by attackers attempting unauthorized access.



Data Protection and Recovery

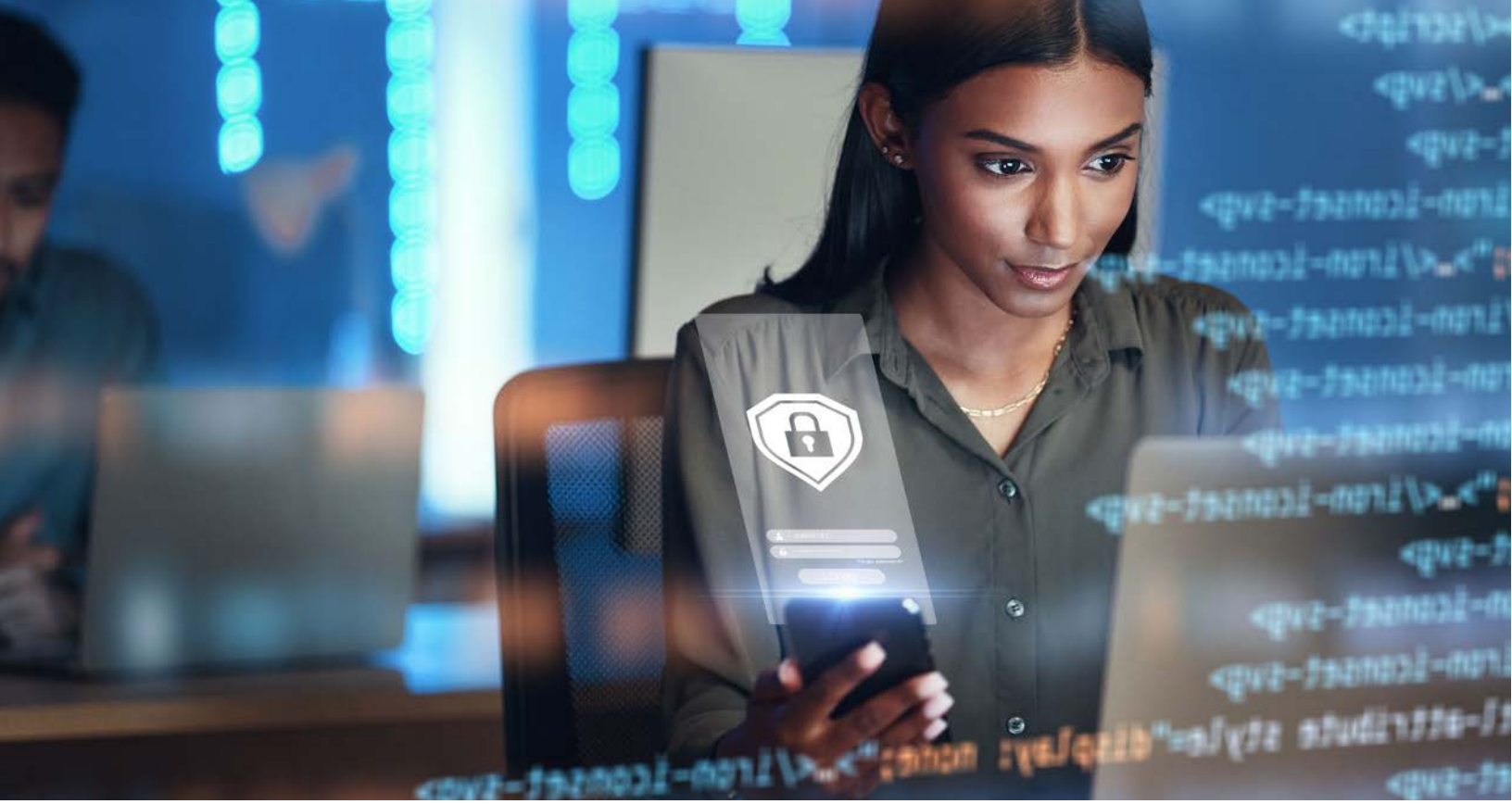
Data protection and recovery refers to the strategies and technologies used to safeguard and restore data in the event of accidental deletion, corruption or cyberattacks. It involves implementing backup solutions, encryption and disaster recovery plans to ensure data integrity and availability.

Backup your data

Safeguard against data loss due to cyberattacks or hardware failures by regularly backing up important files and documents.

Install antivirus software

Protect against malware and other cyberthreats by installing reputable antivirus software to detect and remove malicious software from your devices.



General Cybersecurity Knowledge

It's important to know common signs of hacking so you can take action as soon as possible and recover your accounts.

Here are some warning signs that you may have been hacked:

- Device internet usage increases dramatically
- Device operating speed slows
- Battery depletes rapidly without explanation
- You receive unauthorized requests to change passwords
- New software or applications are downloaded automatically

05.
Data Privacy FAQ

In this section, we answer some common questions about data privacy.

What Is the Purpose of the Data Privacy Act?

The purpose of the Data Privacy Act is to safeguard individuals' personal information by regulating its collection, processing and storage — thereby promoting transparency and data protection.

What Are the 4 Types of Data Privacy?

The four types of data privacy correspond to different levels of access and sensitivity:

Public data privacy

Pertains to information intended for public consumption such as general company contact information and generally does not require strict privacy protections.

Internal-only data privacy

Involves data accessible only within the organization and typically requires safeguards to prevent unauthorized access by external parties.

Confidential data privacy

Relates to sensitive information that requires heightened privacy measures to restrict access to authorized individuals within the organization.

Restricted data privacy

Refers to highly sensitive data subject to stringent privacy controls, often requiring special permissions for access and handling to minimize the risk of unauthorized exposure or misuse.

What Is Considered Privacy Data?

Privacy data, also known as personally identifiable information (PII), encompasses any information that can directly or indirectly identify an individual. This includes basic identity details like name and date of birth, contact information such as email addresses and phone numbers, financial data like creditcard numbers and sensitive information like health records.