

What is Digital Security?



In a nutshell, digital security means protecting your computer, mobile devices, tablets, any other Internet connected devices intruders, which could be in the form of hacking, phishing, and more.

Digital security, also known as information security, is the practice of protecting digital information from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing use of technology in every aspect of our lives, digital security has become a top priority for organizations of all sizes.

Digital security can be broken down into several different types, each with its specific purpose and application. The most common types of digital security include:

Network security: This type of digital security is focused on protecting an organization's networks from unauthorized access or attack. It includes firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs).

Application Security: This type of digital security is focused on protecting an organization's applications and systems from unauthorized access or attack. It includes web application firewalls, security testing, and secure coding practices.

Endpoint Security: This type of digital security is focused on protecting an organization's endpoints, such as laptops, smartphones, and tablets, from unauthorized access or attack. It includes antivirus software, endpoint protection platforms, and mobile device management (MDM) solutions.

Cloud security: This type of digital security is focused on protecting an organization's cloud-based systems and data from unauthorized access or attack. It includes security-as-a-service, cloud access security brokers, and cloud-based intrusion detection and prevention.

Identity and access management (IAM): This type of digital security is focused on controlling and managing access to an organization's systems and data. It includes multi-factor authentication, single sign-on, and identity and access management platforms.

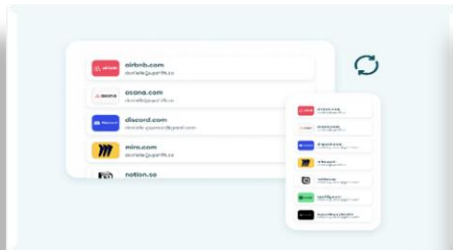


Dashlane is a web and mobile app that simplifies password management for people and organizations across all platforms & devices.

On a typical day, you might log in to email, work, social media, shopping, and banking accounts. You might enter dozens of logins and provide personal data, such as your address and credit card numbers.

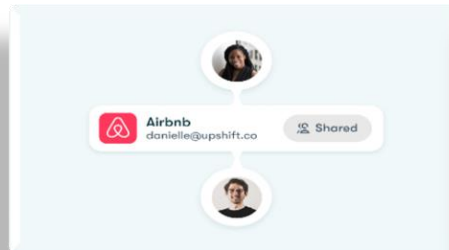
The more logins you have, the higher your security risk and your need for password management best practices. If you share logins, reuse passwords, and fail to change passwords regularly, you may increase your chances of being hacked.

WHAT DO YOU GET WITH DASHLANE?



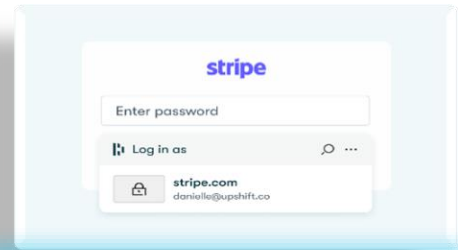
Unlimited secure password sharing

Share passwords without revealing them and revoke access at any time.



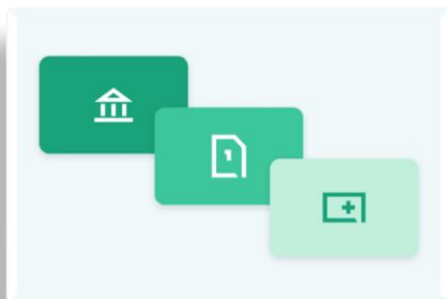
One-click passwords and forms

Dashlane all your passwords, payments and personal details where ever you need them.



Access and manage passwords everywhere

Use Passwords Manager across any device or platform.



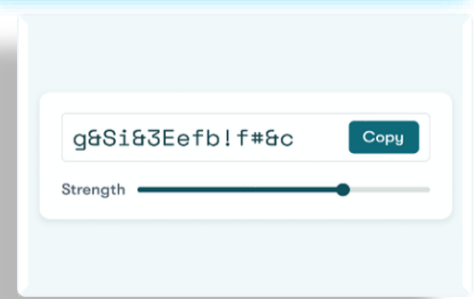
Financial, medical and private info

Secure financial, medical and private info attach encrypted files like passport scan.



Dark web monitoring and alerts

Receive automatic alerts if any of your stored personal data is compromised.



Password Generator

Automatically generate passwords based on guidelines you set and create strong and

Why Does Your Digital Security Matter?

As you go about your daily life, you leave a trail of online activity behind. You actively contribute to your digital footprint each time you use online banking, sign in to loyalty accounts, or message friends on Facebook. And you passively contribute to this trace in ways that you may not be aware of — exposing browsing history, IP addresses, device information, and online purchases. You may rarely give these mundane activities a second thought, but they could needle your identity in many ways.