FOR KIDS AND TEENS, STRONG ENCRYPTION PROTECTS...

PRODUCED BY
FUTURE OF PRIVACY FORUM
FPF.ORG

ENCRYPTION KEEPS YOUNG PEOPLE SAFE

Today's young people have lived their entire lives in the age of the commercial internet, social media, electronic health records, and a growing range of internet-connected devices, from insulin pumps to vehicles. Encryption is the first, best protection to ensure that communications, transactions, personal data, and digital devices are safe and secure.

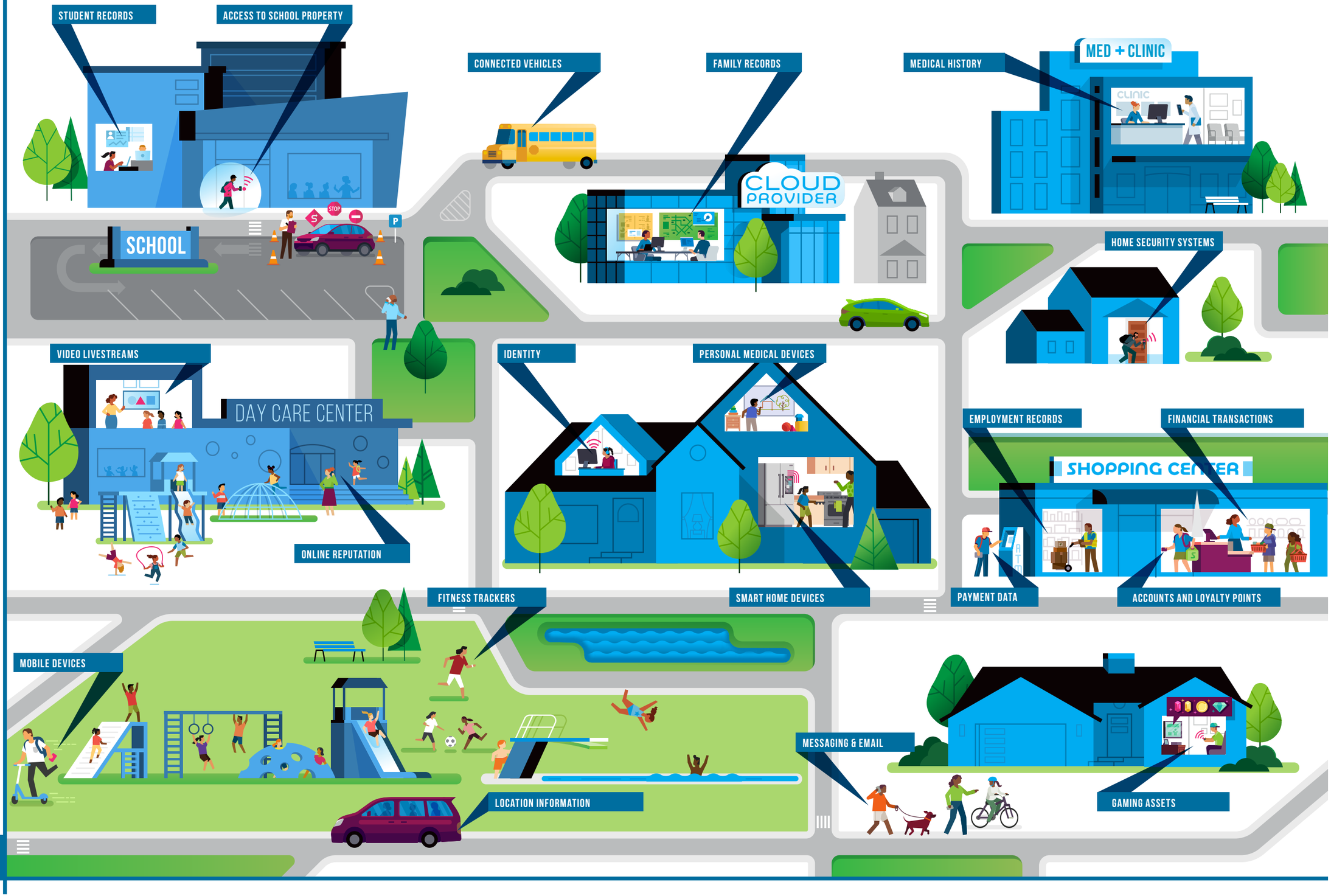
Encryption protects the digital lives of young people and keeps them safe in the physical world as well, whether it's preventing malicious actors from gaining control of kids' internet-connected health tools and teens' messaging accounts or authenticating identities to keep unwanted people out of protected spaces like schools.

HOW ENCRYPTION WORKS

Encryption is a mathematical process that encodes information; it can be used to keep information **confidential** from unintended viewers, to ensure the **integrity** of data against tampering, and to **authenticate** individuals for account access or building entry.

Encryption applies a mathematical formula to information, which obfuscates plaintext information into unreadable ciphertext. Each use of encryption generates a "key" - a long number that is the mathematical solution to the formula and can authenticate and unscramble the protected sensitive information. Encryption strength can depend on the particular formula used for obfuscation or the length of the key - not all encryption is equal, and cryptographers working to keep data and systems safe must constantly respond to any discovered flaws or vulnerabilities. If a private key is not kept secret, anyone with the key can access the private data or impersonate the authenticated person or organization.

SEE PAGE 2 FOR THE RISKS OF WEAKENED ENCRYPTION



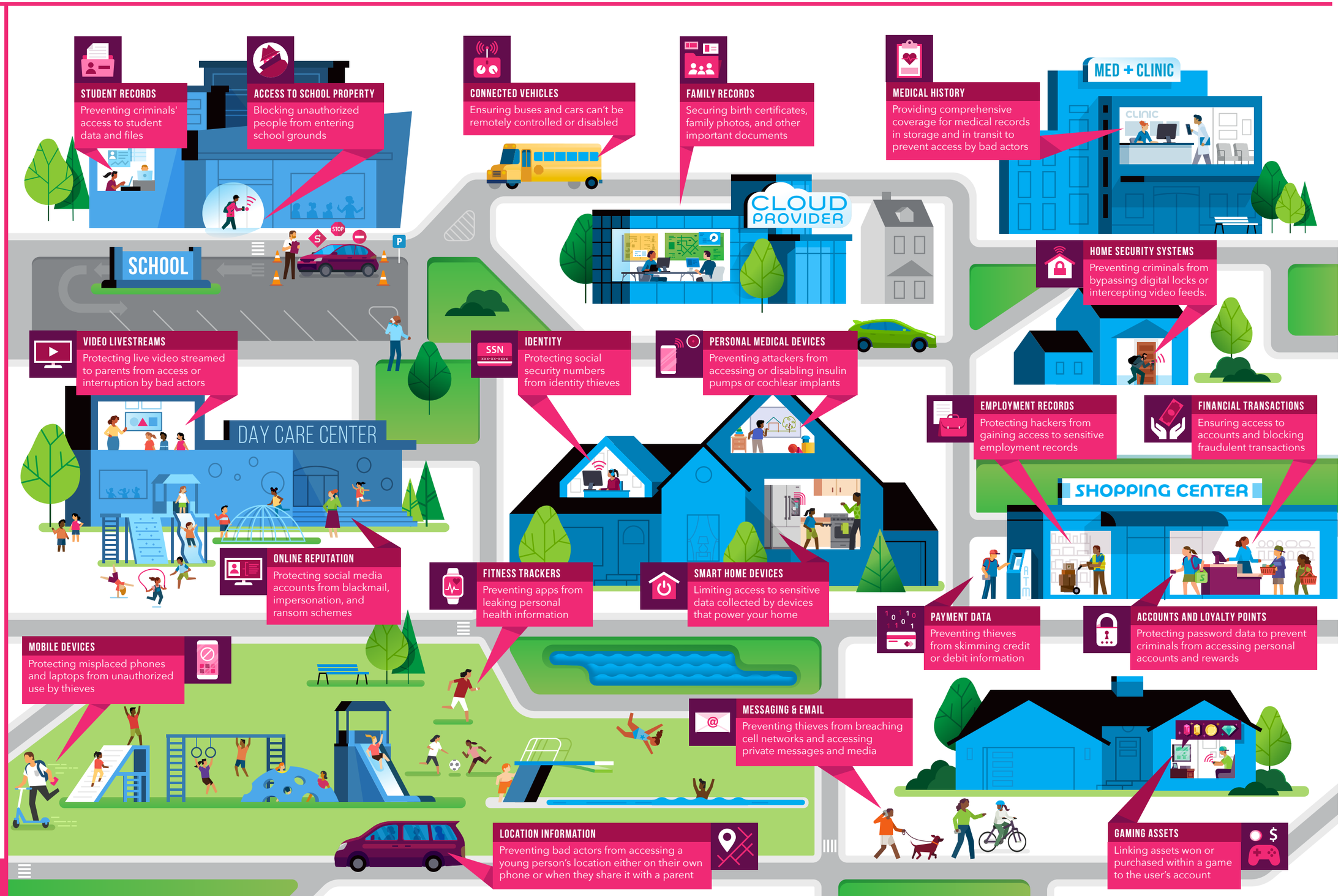
FOR KIDS AND TEENS, STRONG ENCRYPTION PROTECTS...

PRODUCED BY
FUTURE OF PRIVACY FORUM
FPF.ORG

THREATS TO ENCRYPTION

This graphic illustrates how encryption protects young people's data and devices, highlighting some risks posed by weakened encryption. Encryption can be weakened by unintentional software flaws or by intentional decisions to provide some entities with exceptional access. When encryption is absent, or when it is not strong enough, bad actors may be able to gain access to an asset or area and use it to cause harm to an individual or community. For example, a criminal may be able to access teens' communications, bank records, or identification numbers, facilitating identity theft or blackmail. Alternatively, a malicious individual could alter health records to modify medicine dosage, surreptitiously track a child's location, or take control of a school bus or family car and cause it to speed through a school zone.

To mitigate these risks it is imperative that individuals, government, and industry work together to promote the development and deployment of strong encryption, resilient to both known and future threats.



SEE PAGE 1 FOR THE BENEFITS OF STRONG ENCRYPTION