STRONG ENCRYPTION PROTECTS...

EVERYONE USES ENCRYPTION

Strong encryption protects sensitive communications and stored data. Strong crypto protects you when you use a smartphone, browse the web, bank online, or send electronic messages to your family and colleagues.

Crypto can also help authenticate your credentials, preventing criminals from impersonating you, viewing your email and photos, or accessing your bank accounts and health data.

HOW ENCRYPTION WORKS

Encryption is a mathematical process that scrambles information; it is often used to secure or authenticate sensitive documents. Encryption protects information by applying a mathematical formula, which obfuscates plaintext information and transforms the plaintext into unreadable ciphertext. Each use of encryption generates a very long number that is the mathematical solution to the formula and can unscramble the protected sensitive information. This "key" must be kept a secret or anyone who has it will be able to access the information.

LEGEND

- ENTERPRISES
- INDIVIDUALS
- GOVERNMENT

STRONG CRYPTO

SEE PAGE 2 FOR THE RISKS OF WEAKENED CRYPTO

Labels within the illustration:
- CLOUD STORAGE
- CLOUD STORAGE CO.
- MEDICAL RECORDS
- TIME INTEGRITY
- STUDENT RECORDS
- SCHOOL
- SECURITY CLEARANCE DATA
- NATIONAL DEFENSE
- MILITARY COMMS
- OFFICE BUILDING
- LOCATION DATA
- ELECTION INTEGRITY
- GOV'T OFFICIALS' COMMS
- VOTER INFO
- CONNECTED CARS
- FINANCIAL INFORMATION
- DELIVERIES
- CORPORATE COMMS
- MESSAGES
- PUBLIC TRANSIT
- POWER PLANTS
- GUARANTEED LEVELS
- POWER PLANT
- GAS
- SMART SCALES
- CREDIT CARDS
- MOBILE DEVICES
- ONLINE REPUTATION
- HEALTH INFO
- CONSUMER IDENTITY
- INDUSTRY SECRETS
- NUCLEAR FACILITIES
- PERSONAL MEDICAL DEVICES
- WELLNESS TRACKERS
- CREDIT & FINANCE
- NUCLEAR FACILITY

STRONG ENCRYPTION PROTECTS...

SAFEGUARDS FOR INDIVIDUALS, COMPANIES & GOVERNMENT

Every day, consumers, companies, government agencies, and elected officials benefit from strong crypto. Cryptographic technologies protect personal data, corporate confidentiality, and critical infrastructure. Many uses of encryption impact a combination of individuals, enterprises, and government. This graphic illustrates how crypto protects stakeholders and highlights risks posed by weakened crypto.

Weakened crypto creates risks to health, safety, and privacy, and increases the possibility that criminals will infiltrate systems or intercept data. Crypto can be weakened by unintentional software flaws or by intentional decisions to provide some entities with exceptional access.

Government officials typically use commercial software and hardware; there is no practical way to distinguish between public sector vs. private sector crypto.

LEGEND

- ENTERPRISES
- INDIVIDUALS
- GOVERNMENT

WEAKENED CRYPTO
SEE PAGE 1 FOR THE BENEFITS OF STRONG CRYPTO

CLOUD STORAGE CO.

CLOUD STORAGE
Protecting documents and photos stored in the cloud from access and publication.

MEDICAL RECORDS
Preventing blackmailers from cryptowalling medical systems.

TIME INTEGRITY
Ensuring that criminals cannot modify clocks to manipulate financial transactions or security measures.

OFFICE BUILDING

FUNDS

STUDENT RECORDS
Preventing criminals from breaching school systems, imperiling school funding, and exposing children's data.

SCHOOL

SECURITY CLEARANCE DATA
Protecting sensitive government personnel data about trusted officials.

NATIONAL DEFENSE
Preventing foreign adversaries from stealing sensitive military technologies.

MILITARY COMMS
Protecting overseas troops from foreign surveillance and targeted assaults.

ELECTION INTEGRITY
Preventing criminals from modifying voter registrations and votes.

VOTER INFO

LOCATION DATA
Protecting location data about delivery companies' customers and workers.

DELIVERIES

CORPORATE COMMS
Preventing criminals from intercepting and leaking company communications.

CONNECTED CARS
Preventing hackers from remotely controlling or stalling cars.

FINANCIAL INFORMATION
Preventing malware from stealing banking app credentials.

GOV'T OFFICIALS' COMMS
Protecting lawmakers' and candidates' emails from leaks and forgery.

PUBLIC TRANSIT
Protecting SCADA systems from unauthorized control and preventing service disruptions and injuries.

POWER PLANTS
Preventing foreign adversaries from accessing and mapping critical infrastructure.

GAS

MESSAGES
Preventing thieves from breaching cell networks and accessing private messages.

SMART SCALES
Preventing interception of sensitive health information.

CREDIT CARDS
Preventing thieves from skimming credit card information.

POWER PLANT

ONLINE REPUTATION
Protecting social media accounts from impersonation, blackmail, and ransom schemes.

HEALTH INFO

CONSUMER IDENTITY
Protecting SSNs and credit profiles from identity thieves.

MOBILE DEVICES
Protecting misplaced laptops from unauthorized access by identity thieves.

NUCLEAR FACILITIES
Protecting nuclear centrifuge equipment from computer viruses and foreign control.

INDUSTRY SECRETS
Preventing hackers from stealing trade secrets and selling info to competing companies and nations.

PERSONAL MEDICAL DEVICES
Preventing attackers from commanding insulin pumps to administer an overdose.

WELLNESS TRACKERS
Preventing apps from leaking personal health information.

CREDIT & FINANCE

DATA

NUCLEAR FACILITY