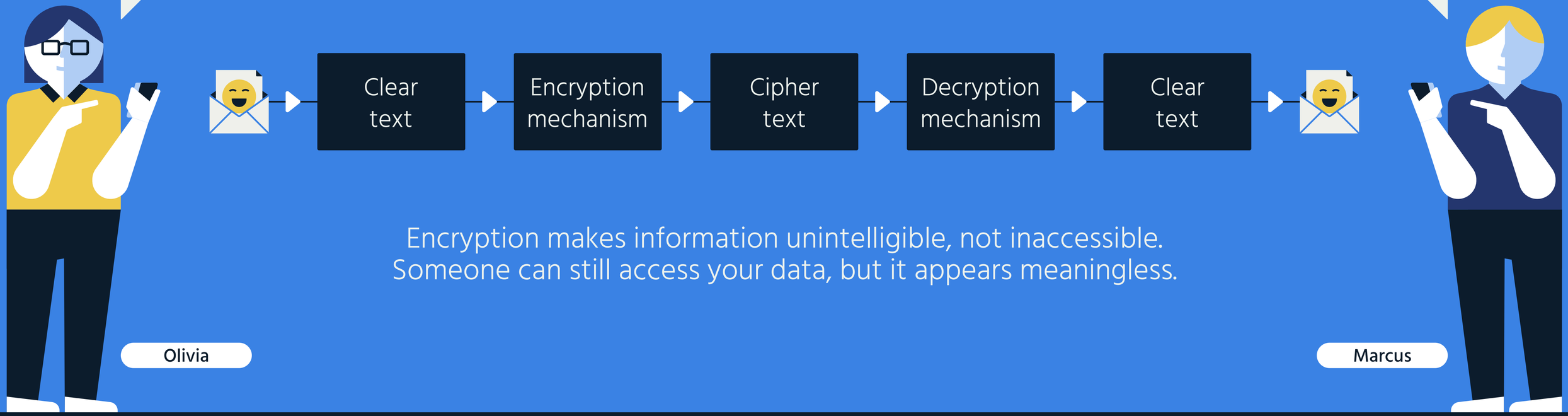
01 What is encryption?

Internet Society

I want to keep all my messages confidential!

Encryption is a way to scramble information so that only those with ‘keys’ can understand what is being shared.

I don’t expect anyone to read my messages, other than who I send them to!



Encryption makes information unintelligible, not inaccessible.
Someone can still access your data, but it appears meaningless.

The importance of encryption

In our increasingly digital lives, the role of encryption has never been more essential.

Encryption is a crucial feature of a safe Internet. It ensures your private messages stay private.

From video calls to air traffic control and e-voting, encryption is vital for securing all aspects of our lives.

It keeps your identity safe and stops people from impersonating you, or the people that you trust.

It is critical to national security, protecting society from terrorists, criminals, and hostile governments.

Personal security depends on encryption. It keeps your confidential data out of the hands of criminals.

02 How does encryption work?

Internet Society

Each user has two keys: a public one and private one.
Olivia finds Marcus' public key and copies it to her device.

Olivia generates a secret, symmetrical key, encrypts a copy of it using Marcus' public key, and sends it to him. He decrypts it with his private key.

Olivia and Marcus now have a shared, secret key which they can use for fast, efficient symmetric encryption.

The initial key exchange uses asymmetric encryption.
The data itself is transferred using symmetric encryption.

Different types of encryption

Not all encryption is equal. The best systems balance safety and efficiency.

Symmetric encryption is like a cash box, where all users have the same secret key to see what's inside.

- ✓ Fast and efficient
- ✗ Vulnerable to interception

With asymmetric encryption each user has their own public and private keys, providing additional security.

- ✓ Safe and secure
- ✗ Complexity means less efficiency

In hybrid systems, a mixture of encryption processes provides the best of both worlds. Asymmetric encryption is used for a secure key exchange, with the more efficient system of symmetric encryption used to transfer the data itself.

- ✓ Safe and secure
- ✓ Fast and efficient

May 2021

03 What threatens encryption ?

Internet Society

Key escrow

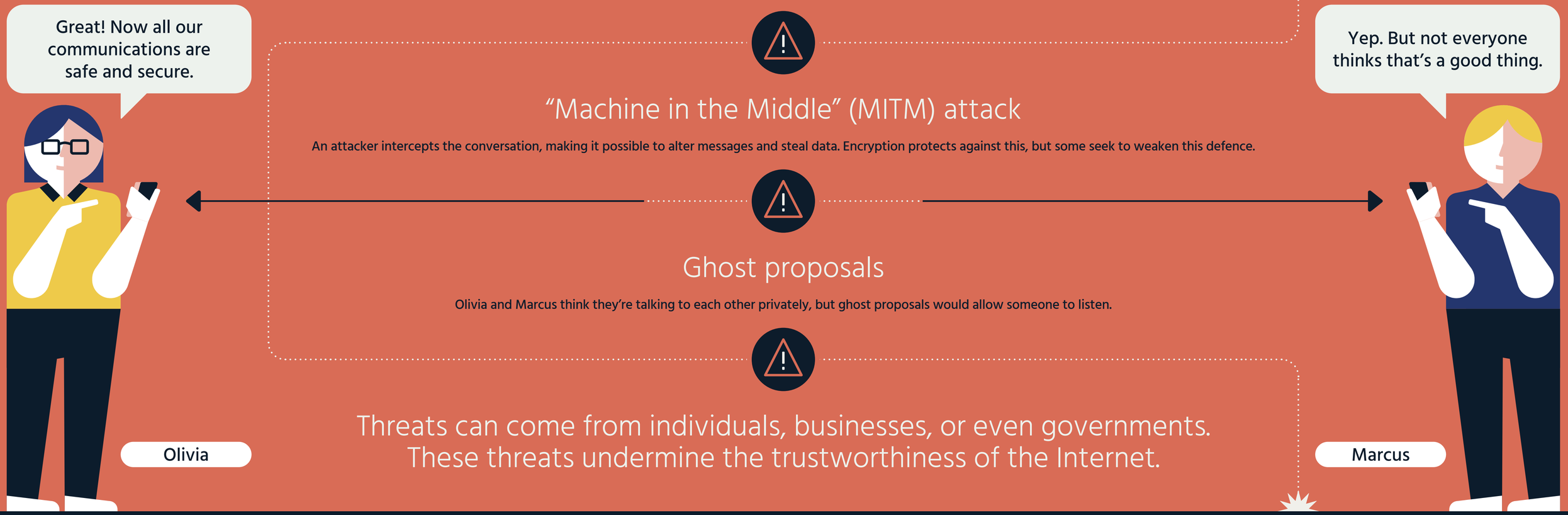
Olivia and Marcus may want a third party to look after their keys. If the third party can be trusted, this isn't a problem. But it's a potential weakness.

"Machine in the Middle" (MITM) attack

An attacker intercepts the conversation, making it possible to alter messages and steal data. Encryption protects against this, but some seek to weaken this defence.

Ghost proposals

Olivia and Marcus think they're talking to each other privately, but ghost proposals would allow someone to listen.



Threats can come from individuals, businesses, or even governments. These threats undermine the trustworthiness of the Internet.

Where threats come from

Knowing who wants to access your data highlights the importance of keeping it safe.

Some areas of law enforcement want backdoors to catch criminals. This creates access for bad actors, not just good ones.

Many governments think they should be able to break encryption in order to access their citizens' messages.

Blackmailers would like to break encryption to target people's private messages, photos and videos.

Personal banking and national economies rely on encryption. Vulnerabilities could lead to stolen money and financial data.

Criminals steal people's identities, to commit crimes and evade capture. Weak encryption would enable this.

May 2021