

# HTTPS and Website Security



Office of the Government  
Chief Information Officer

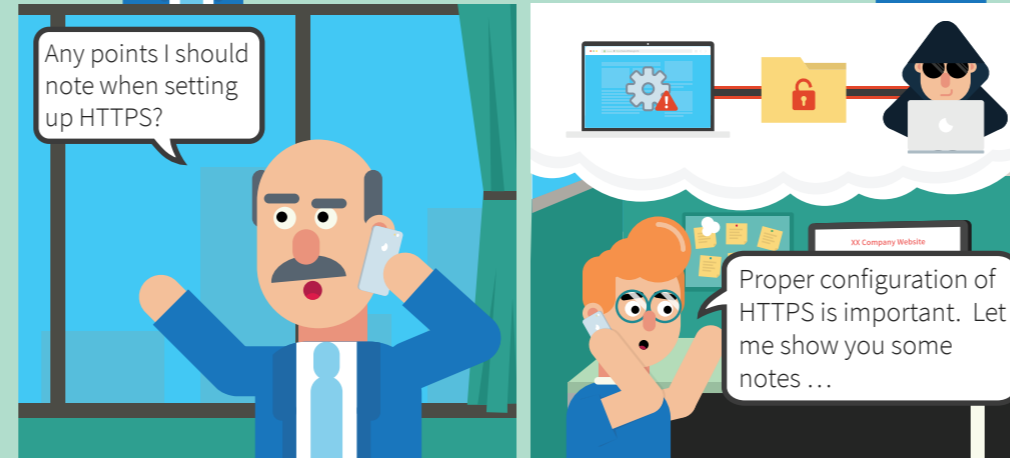
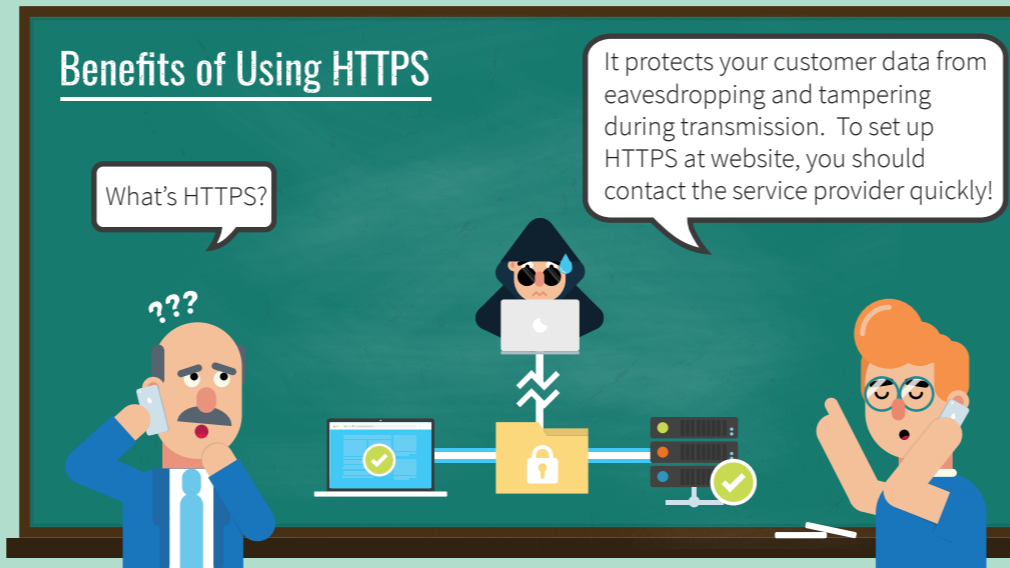
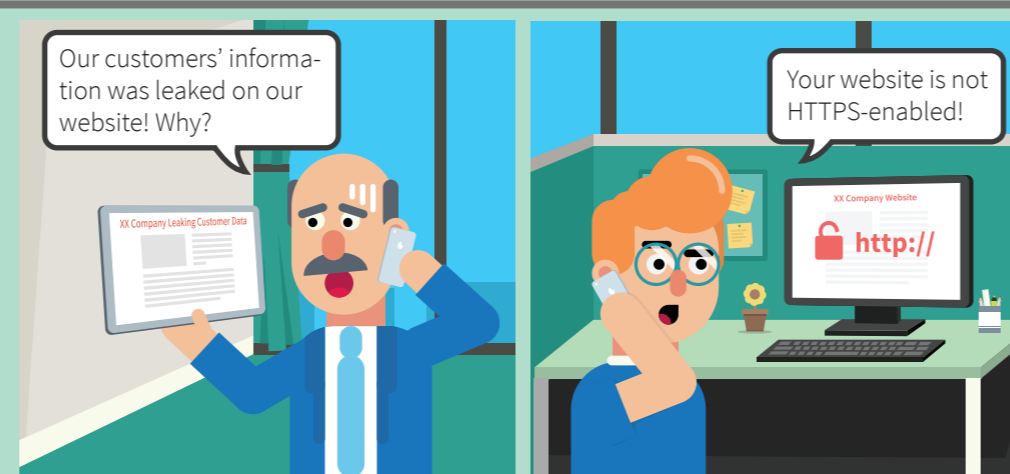


Hong Kong Computer  
Emergency Response  
Team Coordination Centre



Hong Kong Police Force

For details, please visit the InfoSec website at:  
[www.infosec.gov.hk](http://www.infosec.gov.hk)



InfoSec Website ×  
Secure | <https://www.infosec.gov.hk>

## Points to note about HTTPS and Website Security

- Use server certificate issued by a recognised certificate authority and keep the certificate in “Trusted” condition
- Employ secure protocols only (e.g. TLS 1.2)
- Automatically redirect web traffic to HTTPS site (e.g. enable HTTP Strict Transport Security (HSTS) support)
- Use strong cipher suites (e.g. SHA-256, AES 256-bit, etc.) and disable those functions with security risks (e.g. TLS compression, etc.)
- Update operating systems, applications, framework libraries and cipher suites periodically
- Store sensitive data in the backend server with proper protection
- Do not include sensitive information in the URL