



---

# E-COMMERCE SECURITY

Securing E-commerce Websites  
with  
Digital Certificates

---





# Cyber Risks and Threats



## Identity Theft

Stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, usually as a method to gain access to resources or obtain credit and other benefits in that person's name



## Malware Invasion

Short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.



## Phishing Scams

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details masquerading as a trustworthy entity in an electronic communication.



# Philippines: Phishing Sites Statistics

Malicious website statistics for Philippines

Metric	3Q12	4Q12	1Q13	2Q13
Phishing sites per 1,000 hosts (Worldwide)	11.23 (5.41)	8.43 (5.10)	3.22 (4.56)	5.76 (4.24)

Resource: Microsoft Intelligence Report Volume 15 January- June 2013

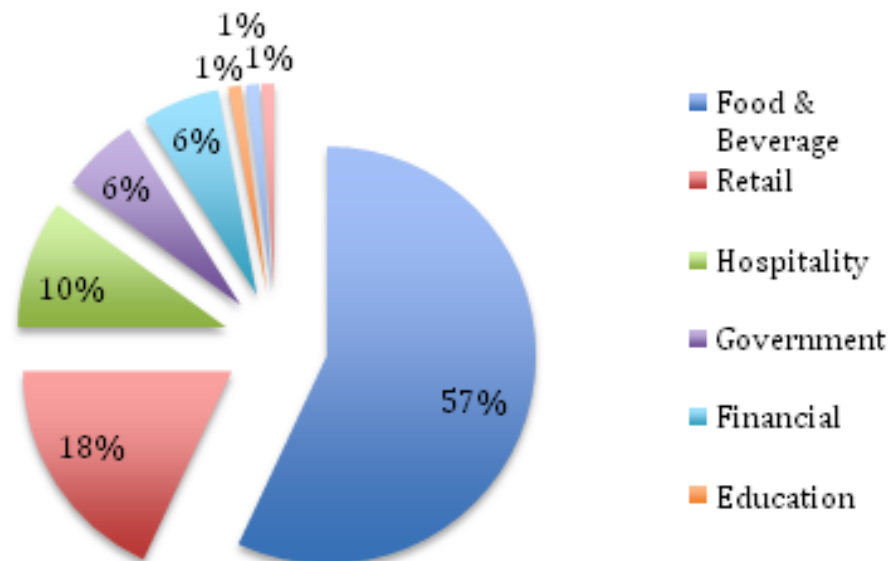
**Phishing Attacks** are prolific in the Philippine Websites.





# Small Merchants and Ecommerce: Big Targets for Card Information Thieves

## Percent of Compromised Merchants by Industry



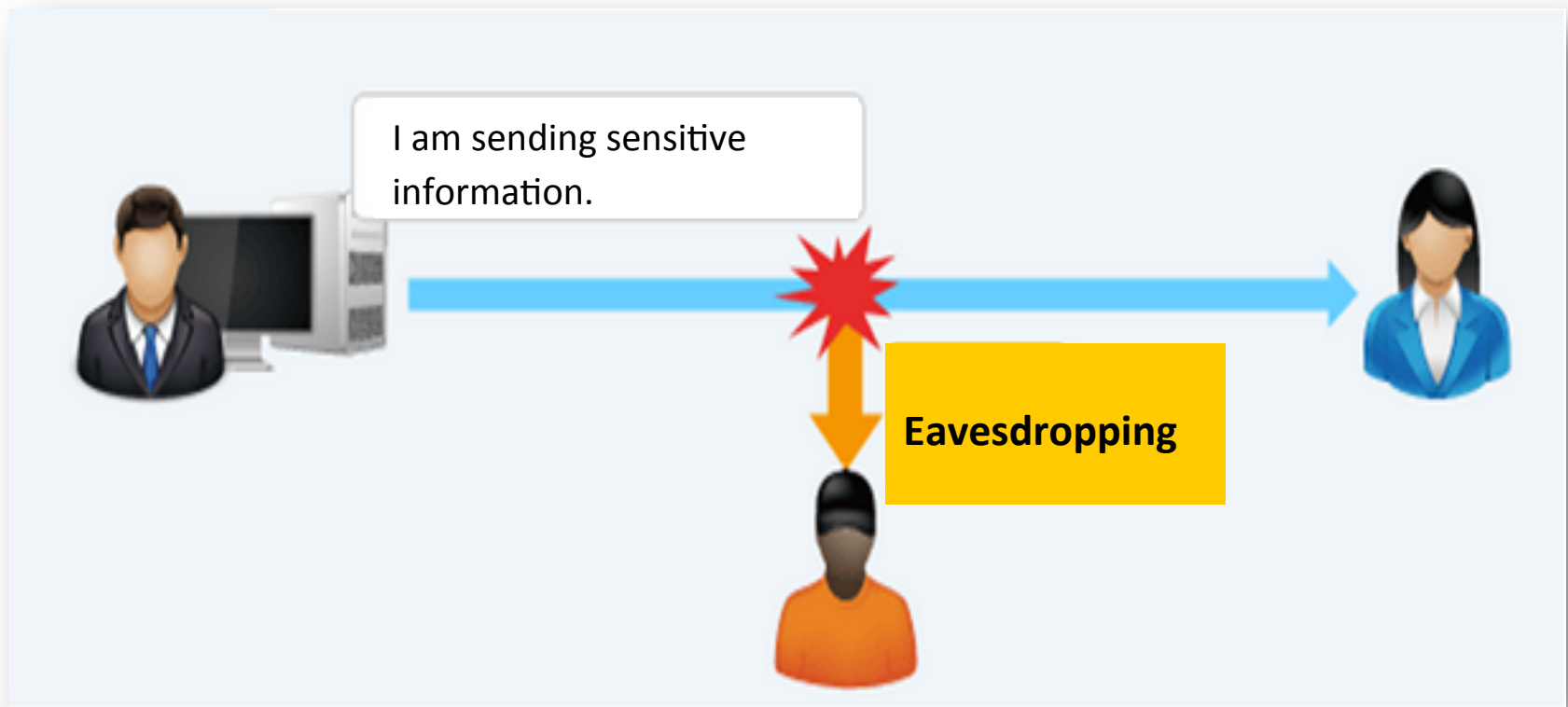


**Some of the security issues that need to be addressed by E-commerce merchants**

**The use of Digital Certificates**

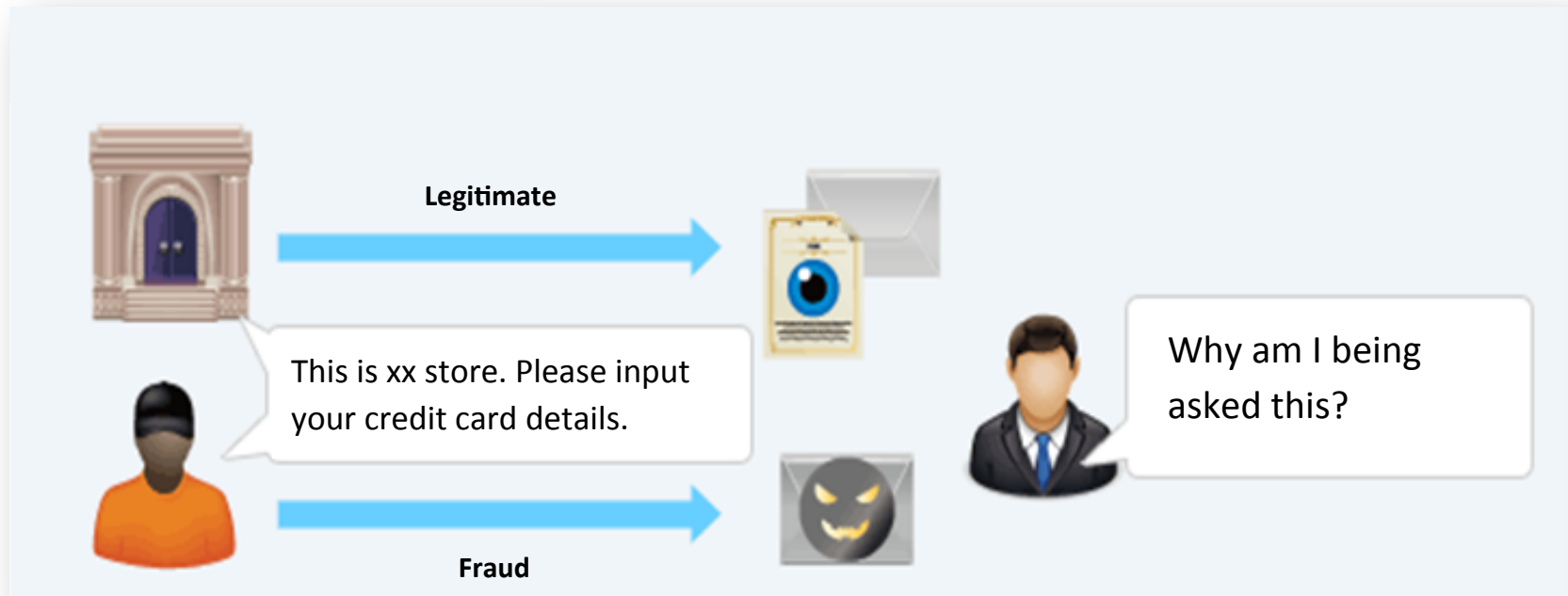


# Data Integrity over the Network





# Strong Authentication of the Website







# HOW DO YOU ADDRESS THESE ISSUES?





1

**SSL  
CERTIFICATES  
SECURE THE DATA  
BETWEEN THE  
WEBSITE AND THE  
END-USER.**

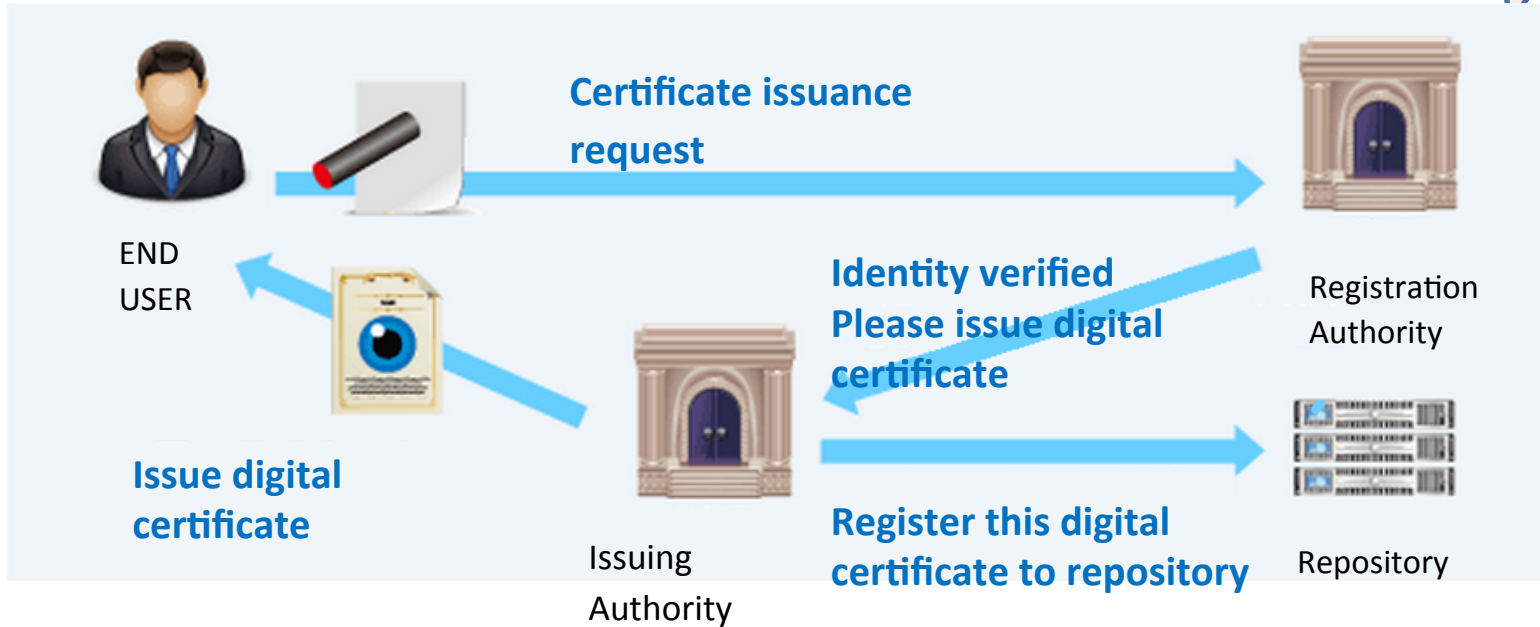




# How SSL certificates are obtained?

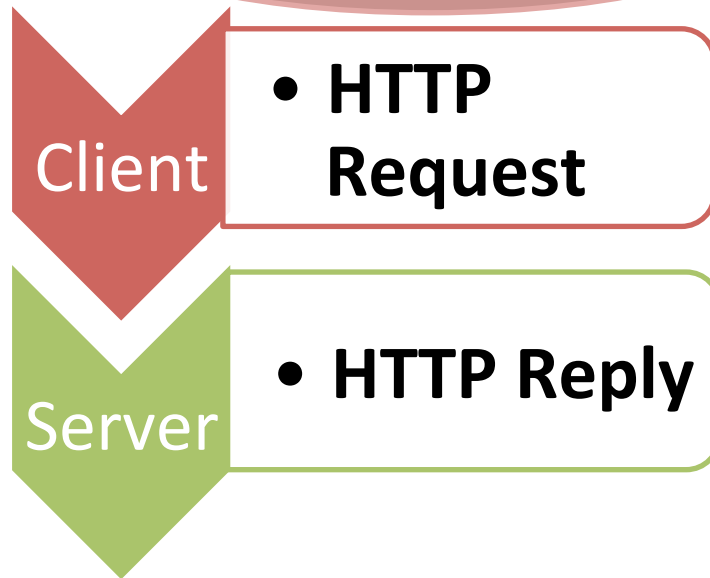


## Certificate Authorities



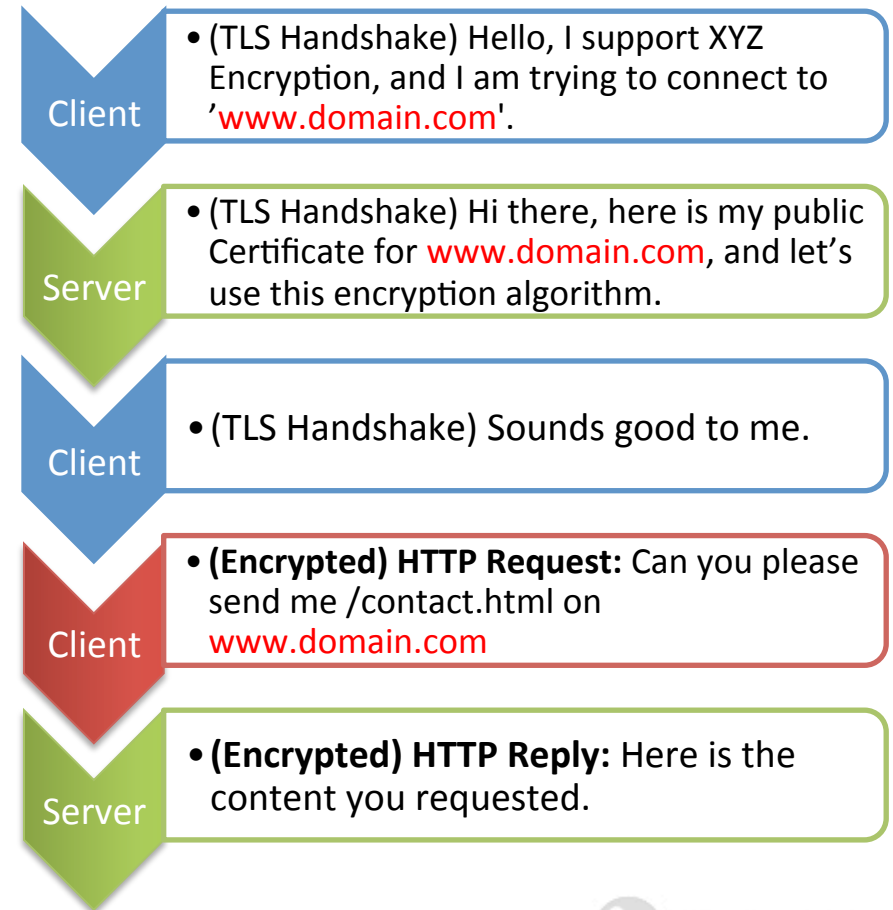


## Regular Website HTTP



How SSL connection works compared to regular network connection .

## Secured Website HTTPS







## Benefits of SSL Certificates to E-commerce



### Secures:

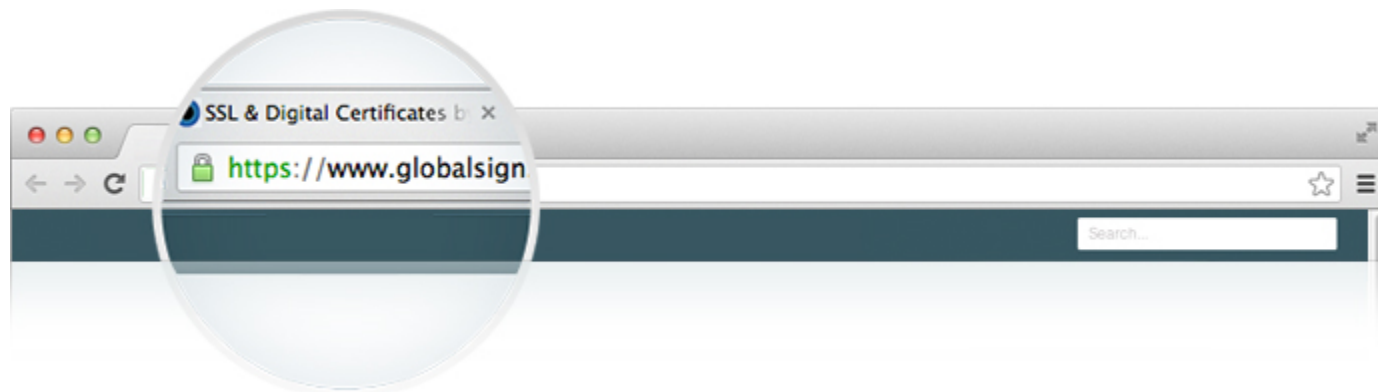
- Confidential Financial Information
- Log-in Information
- Personal Information



2

## SSL Certificate

**provides strong authentication to websites in which it represents.**





# EV SSL

Clear security indicator that increases USER TRUST



 **GMO GlobalSign Inc [US]** <https://www.globalsign.com>



 <https://www.globalsign.com> 



 **GMO Globalsign Inc (US)** <https://www.globalsign.com>



**GMO GlobalSign Inc**  [www.globalsign.com](http://www.globalsign.com)



Extended Validation is the highest class of SSL available



Activates the green address bar



Prevents Phishing attacks







# CAs offer SITE SEAL to provide Assurance and Authentication



## Secure Site Seal Benefits

- Increases recognition of trust
- Encourages consumer to complete call to action
- Provides a Click to Verify function, enabling the user to view details of SSL Certificate used
- Decreases abandoned shopping baskets and other purchases
- Shows the website owner cares about user online privacy and security



# RECAP

- Provides **strong Authentication** of the website.
- Increase **Trust** through **prevention** of Phishing Attacks
- Data **Security** through **SSL Certificates** over the network.



---

# E-COMMERCE SECURITY

Securing E-commerce Websites  
with  
Digital Certificates

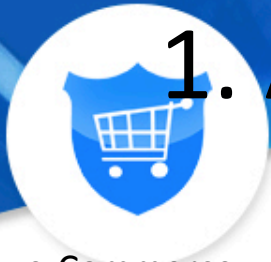
---



# About the Speaker

Moises Merin is the Country Manager for GMO GlobalSign Inc. – a Certificate Authority securing online identities, data and transactions. In 2010, he joined GlobalSign and has travelled to Asia Pacific territories of GlobalSign to understand the different consumer behaviors, security status and maturity level of his markets.



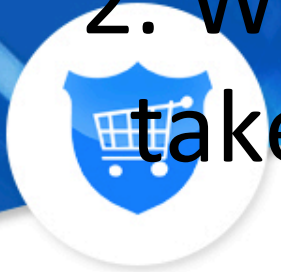


# 1. Are Philippine E-Commerce Sites today secure?

e-Commerce websites in the Philippines are *not secure* because:

- **The existing Electronic Commerce Act of the Philippines has weak provisions.**
  - While **RA 8792** mentions the use of electronic signature on documents issued by ecommerce owners, it does not have strong implementing guidelines to ensure the security of the Electronic Signatures used.
  - The law does not impose the use of Server Certificates (SSL Certificates) on ecommerce sites to protect online buyers' financial information.
  - The Government does not run active campaigns to ensure every online retailer is aware of the existing law. More so, it does not mandate these ecommerce sites to enforce security measures.
    - The Government itself is yet to adopt high assurance online security protocols.
    - The DTI, the agency assigned to lead the adoption of security measures in ecommerce sites, may not be actively tracking ecommerce sites.
- **Majority of online retailers in the Philippines use free hosting platforms and Social Networking Sites as online point of sales.**
  - Most often, international brands extending market in the Philippines are those who have their own domains and SSL certificates. Since their sites are hosted and managed in other country where SSL is more popular and encouraged.
- **Online retailers do not see Digital Certificates, SSL certificates particularly, as wise investments.**
  - Most Filipinos are still not comfortable with online purchases. Ordering of product is online, but payment still happens over the counter or COD.

## 2. What security measures should be taken to ensure the security of our websites?



- Implement strict IT security policy in the webserver and the website.
- Secure sensitive information over the network by implementing security protocol such as SSL.
- Install Anti-Virus or Anti-Malware applications on the end user's computer.



### 3. What are the cost investment in relation to it?

Implementing SSL as a security protocol will cost around Php 11,000.00 to Php 40,000.00 annually depending on the type of SSL Certificate that will be implemented.



# E-Commerce Strategy Blueprint suggestion

- In connection to securing e-Commerce websites using SSL, I suggest that major organizations supporting E-Commerce in the Philippines **endorse** in a memorandum the need for e-Commerce websites to get the appropriate level of SSL protection from Certificate Authorities.
- These organizations should recognize their members' achievements around securing their own e-Commerce operations in view of the business case and moral responsibility of securing online identities, data and transactions.