



# E-COMMERCE SECURITY

---

Presented by

**ANDY YU**

**yu z hu**

**web development**

# INTRODUCTION

Andy Yu

Owner, YUZHU Web Development

Web Architect, City of Timmins

# SUMMARY

- What is E-Commerce
- Retail vs E-Tail
- Other “Transactions”
- Security Considerations – What, Why, How
- Practical Scenarios
- SSL & Certificates

# WHAT IS E-COMMERCE?

amazon.com

 **Canada Trust**



*itravel2000*

**WESTERN**  
*Auto Sales*

 **Ontario**  
ServiceOntario

  
**AIR CANADA**



 **ePost**<sup>TM</sup>



# TYPICAL RETAIL TRANSACTION

- Customer is ready to check out!
- Gets to cashier, provides payment – cash, debit, credit
- Obtains receipt, product
- See you next time!

# TYPICAL E-COMMERCE TRANSACTION

- Customer is ready to checkout!
- Credit card details provided by customer
- Credit card details passed on for processing (payment gateway or to business!?)
- Order and customer details supplied to merchant (business)
- What's the major difference from the traditional retail transaction!

# OTHER ONLINE “TRANSACTIONS”?

- Exchange of confidential documents
- Access to sensitive data
- Consider business end as well – viewing, processing submitted information

## EXAMPLES

- Medical histories
- Credit applications
- Order forms
- Marketing sign up forms
- Contest entries
- What are you collecting?

# WHAT ARE WE PROTECTING?

- **INFORMATION!**
- Retail store vs Online
- Credit card information
- Personal Customer information
- Transaction information
- Accounting information
- Data integrity
- Trust
  
- What policies are in place at your physical business to deal with this?

# WHAT ARE WE PROTECTING AGAINST?

- Server attacks
- Web Application Attacks
- Data manipulation
- Compromised passwords
- Social engineering attacks
- Theft of identity and credit details

# WHY DO WE PROTECT IT?

- Maintaining trust – public, customers
- Legislative requirements – PIPEDA - the right to personal privacy and the need of organizations to collect information
- Imposed industry compliance – PCI DSS
- Alignment with organizational priorities
- Risk management – prepare now or pay later!

# IN THE NEWS

- April 2011 Sony PlayStation Network
- January 2009 Heartland Payment Systems
- January 2008 GE Money
- 2007 TJ Maxx
- 2007 TD Ameritrade
- Hacker attacks against retailers up 43% (Oct. 13, 2011 - Dell SecureWorks)
- So if THEY can get compromised...

# CONSEQUENCES

- Loss of business
- Loss of credibility
- Gain of liability
- Fines
- Lawsuits
- Negative media attention

# SECURITY MEASURES

- Physical security – buildings, servers, authorized users
- Data storage – protect electronically stored data!
- Data transmission – encrypt for transmission – no email!!!
- Application development – reliable code, protect access to code
- System administration – security, updates, log files, access accounts

# ESSENTIAL REQUIREMENTS FOR E-COMMERCE SECURITY

- Privacy
- Integrity
- Authentication
- Non-repudiation

# HOW DO WE PROTECT

- Privacy – Encryption, SSL
- Integrity – Firewalls, backups, Digital Signatures, Certificates
- Authentication – VPN, Digital Signatures, Certificates
- Non-Repudiation – Digital Signatures, confirmation services, digital receipts, timestamps

# SMB: TOO MUCH TECH!!!

Let's simplify:

- E-commerce site is not a “website”, it is an application for online sales through a website.
- Choose experienced e-commerce web developers, application providers or SaaS
- Ensure secure, reliable, scalable hosting environment
- Do not store, retrieve or accept credit cards directly
- Protect sensitive information
- **SSL certificates**
- Ask questions!

Remember:

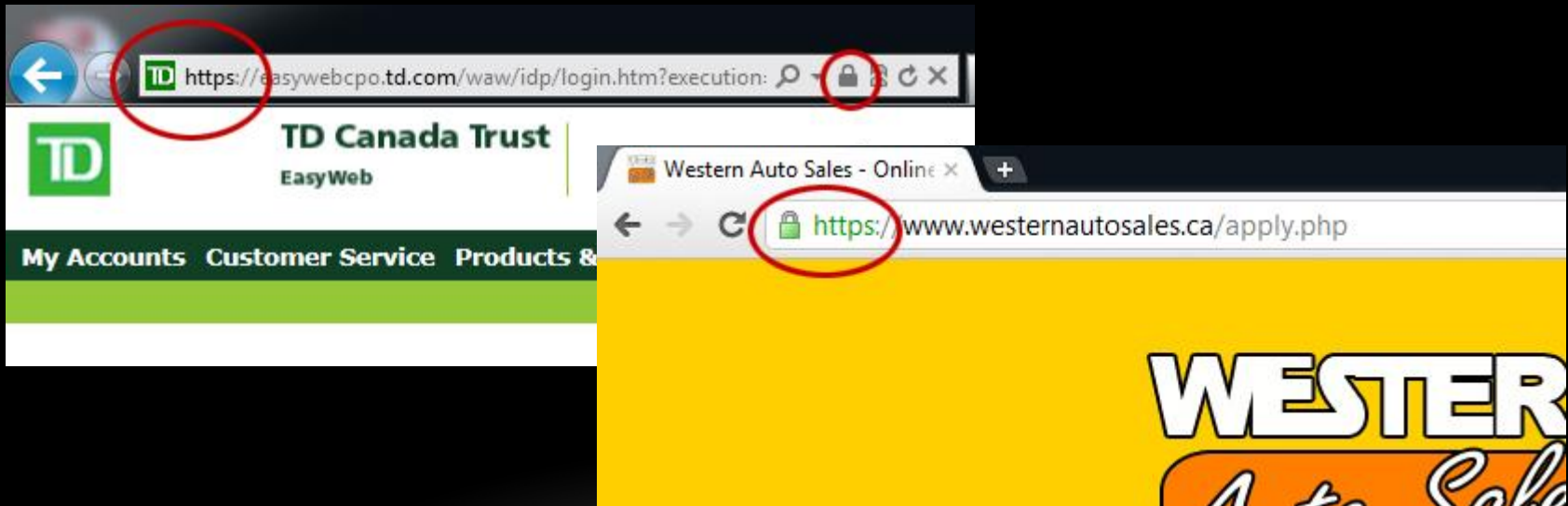
- You get what you pay for!
- E-Commerce is a business decision, not a technology decision!

# PCI DSS

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a <b>firewall</b> configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system <b>passwords</b> and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

# SSL – SECURE SOCKETS LAYER

- Most visible component to e-commerce security for customers
- Provides encryption of data during **transmission** over networks
- Look for the HTTPS and the Lock



# NAMES IN SSL

- VeriSign
- Entrust
- GeoTrust
- Thawte
- Comodo
- GoDaddy
- And more!

# DIFFERENT TYPES OF SSL PRODUCTS

- Free, low-cost, hundreds, thousands
- Shared Certificates – not appropriate for public access sites \$0
- Domain Validated – tied to your domain name - ok for e-commerce \$
- Company Validated – validates domain, business and domain ownership. \$\$
- Extended Validation – additional thorough checks and validation. \$\$\$
- Others: wildcard, multi-domain \$\$\$\$+
  
- Best value: Company Validated SSL Certificates. Encryption and customer assurance.

# EXAMPLES

- Who's using them, and how.
- Our examples:
  - Western Auto Sales – Online Credit Applications
  - Attitudes for Education – Secure scholarship applications
  - Millson Forestry Service – Online Store

# DATA PROTECTION

- What about information that is stored?
- Encrypt for storage too!
- Password protect
- Backups

# TAKEAWAYS

- Plan and research
- Make information security a priority
- Choose the right people to work with
- SMB has same responsibility with the same information as Big Corp
- Ask questions
- Build a business not a website

# QUESTIONS



[www.yuzhu.ca](http://www.yuzhu.ca)