E-Commerce I

Tom Kelliher, CS 102

Nov. 22, 2004

1 Administrivia

Announcements

Web sites due in two weeks.

Assignment

Read 10.4–10.5 and Chapter 10 Above & Beyond. Questions on pg. 600: 17, 18, 21. Questions on pg. 607: A3, A4.

From Last Time

JavaScript lab.

Outline

1. Introduction and discussion.

Coming Up

E-commerce II — lab.

2 Introduction and Discussion

2.1 Advantages and Discussion

The advantages of e-commerce:

1. To start, ask students.
2. Use search engines to find best prices. froogle.com, bizrate.com, shopper.com, priceline.com
3. Can find almost anything.
4. Great prices on used items through online auctions.
5. No sales tax. (Sometimes; for now!)

The disadvantages of e-commerce:

1. To start, ask students.
2. Can't see items (important for clothes).
3. Concern over eavesdropping on connection, e-commerce site being hacked, marketing of customer data.
4. Shipping costs.
5. Have to wait for package to arrive.

   But: package tracking; typical delivery times.

Personal experience:

1. Credit card information hacked (McGlen).
2. Item advertised was not item delivered (video card).

3. SPAM.

4. Phishing expeditions.

2.2 Safeguards

1. Shop with merchants whom you know and trust.

2. Look for and read each merchant's delivery, return, and privacy policies.

3. Never transmit sensitive data over a page which does not have an address beginning with `https://` and a locked padlock icon.

4. Make online purchases with a credit card, not a debit card.

5. Don't hit the "BUY" button more than once — be patient.

6. Never send credit card info via e-mail.

7. Print and save all online receipts at least until you receive all ordered items in good condition.

8. Search for the best prices before buying.

Background:

1. Digital Certificates: sent by Web site; used to encrypt session data.

   But still, how do you know the site is legitimate?

2. Certificate authorities: organizations which vouch for e-commerce sites.

   Web browsers have a list of them. Sometimes, the list must be updated.

2.3 Potential Problems

1. Site spoofing: Counterfeit Web sites (`www.whitehouse.gov` vs. `www.whitehouse.com`).

2. Unauthorized disclosure: Sending sensitive data in the clear.

   Why would they do that?

3. Unauthorized action: Unauthorized alteration of Web pages.

4. Data alteration: Intercept and modification of data being transmitted to a Web site.

Encryption via SSL guards against all of these. 128-bit encryption is best (no one can break). Don't accept anything below 64-bit (only NSA can break) — 56 or 40.