



Romel Cabiling ▾



[Home](#)

[Home](#) > [My courses](#) > [Seminars and Tours](#) > [O5 \[Enter Module Title Here\]](#) > [Lesson Proper for Week 5](#)

Lesson Proper for Week 5

Today, privacy and security are a noteworthy sympathy toward electronic advances. Business offers security worries with other innovations in the field. Advancement in installment framework empowers transactions to be carryout easily crosswise over outskirt and plastic cards are one of the essential methods for picking up to record regardless of where the client is living. In Africa, illustration, the connection of outskirts and the Euro' presentation have prompted a generous increment in cross outskirt transaction and related fraud.

The principal e-commerce in history was in 1886, when a broadcast administrator by the name of Richard Sears who subsequent getting a shipment of watches that was rejected by the neighborhood diamond setter, utilized the broadcast to offer the watches to kindred administrators and railroad utilizes with time, he had guarded up enough money to stop his job to begin his own business which later got to be Sears, Roebuck, and co. Advancement business its purest structure as indicated by Vladimir Zwass (Editor-in Chief of International Journal of Electronic Commerce) in vogue times can be followed to 1948 electronic transmission of messages amid the Berlin transport.

The following phase of e-commerce as per Turban et al (2008) was the improvement of (EDI) Electronic Data Interchange which start in the 1960s in the type of agreeable endeavors at creating typical electronic information organizations between industry bunches.

This configuration was utilized just for transportation, buying, and in intra-industry exchanges and it was not until the 1970's that work began on national (EDI) Electronic Data Interchange measures that in the long run made a stage for Electronic Funds Transfer (EFT). This was utilized by organizations to encourage online installment for business exchanges and additionally subsidizes exchange. Furthermore, to send business reports like buy requests, invoices.

In any case, was not without its particular difficulties at origin because of the way that there was no institutionalization and two organizations must have the same application programming or else, exchanges cannot occur between them. Had the capacity grown very much organized E-Commerce stages that made conformities for the impressive dangers and blunders.

In addendum, the verifiable advancement of ECommerce cannot be finished without making appropriate reference to Automated Teller Machines(ATM), Enterprise Resource Planning(ERP), acknowledgment and development, acknowledgment and improvement of phone managing an account in the 1980s, information mining, and information warehousing in the 1990s, charge cards, furthermore as of late,



advancements in Electronic Governance (administration), furthermore all the more e-Learning, all of which have come to be referred to and for the most part acknowledged as a feature of E-Commerce.

Web Security

Web Security is one of the principal and continuing concerns that restrict customers and organizations from engaging with e-commerce. This seminar aims to explore the perception of security in e-commerce B2C and C2C websites from both customer and organizational perspectives.

1. With the rapid development of E-commerce, security issues are arising from people's attention. The security of the transaction is the core and key issue of the development of E-commerce. This seminar about the security issues of Ecommerce activities put forward a solution strategy from two aspects that are technology and system, to improve the environment for the development of E-commerce and promote the further development of E-commerce.
2. Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet.
3. Each phase of an E-commerce transaction has a security measure.

E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry- ption	Secure Delivery Integrity Checks

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the e-commerce server wouldn't know the order was fake or real. Password protection, encrypted client-server communication, public-private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear text before it gets encrypted.

Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information.

Problem Statement



E-commerce security is the protection of e-business resources from an unapproved access use modification or obliteration and security risk consists of unapproved access, burglary, theft, and misrepresentation and Ebusiness issue includes not being able to offer items under the "long Tail", the client cannot touch and feel an item, dialect barrier, geographical Barrier.

Definition of Terms

→ **E-COMMERCE:** The term electronic commerce (e-commerce) refers to a business model that allows companies and individuals to buy and sell goods over the internet.

→ **SECURITY:** The state of being protected or safe from harm.

→ **Security Framework:** is a compilation of state-mandated and international cybersecurity policies and processes to protect critical infrastructure.

→ **ICT:** Information and Communication Technologies (ICTs) is a broader term for Information Technology (IT), which refers to all communication technologies, including the internet, wireless networks, cell phones, computers, software, middleware, video-conferencing, social networking, and other media applications and services enabling users to access, retrieve, store, transmit, and manipulate information in a digital form.

→ **EDI:** Electronic Data Interchange (EDI) is the electronic interchange of business information using a standardized format; a process that allows one company to send information to another company electronically rather than with paper. Business entities conducting business electronically are called trading partners.

→ **EFT:** Electronic funds transfer (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer-based systems, without the direct intervention of bank staff.

→ **ATM:** An automated teller machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access cash at most ATMs.

→ **ERP:** Enterprise resource planning (ERP) refers to a type of software that organizations use to manage day-to-day business activities such as accounting, procurement, project management, risk management and compliance, and supply chain operations.

Evolution of E-Commerce

E-commerce, that we all know of today has been existing for the past ten years. Be that as it may, its antecedents, for example, material requirement planning (MRP), enterprise resource planning. (ERP), electronic data interchange (EDI), has been existing for over forty years and is yet living. Electronic information interchanged is the electronic communication of business transaction, for example, confirmation and involves between organizations although interactive access may be part of it, electronic data interchange (EDI) implies computer to computer transaction into vendors database and ordering system. The detailed data of the Material requirement planning (MRP) and Enterprise resource planning (ERP) is covered. However, the predecessors cannot rival the exponential development and acknowledgment of transitioning business over the web. In the 1970s, developments like electronic fund transfer (EFT), funds routed electronically starting with one company and to the next (restricted to extensive cooperation). Create another method for working or doing business or making transactions.



In the 1990s, the web commercialized and the client ran to partake as dotcoms or web starts ups. 1997 saw the introduction of a fresh new stage in e-trade. It was seen as a stage on from e-trade by looking at the trends commence undoubtedly keep on moving and change.

Merits of E-Commerce Security Framework in Nigeria

Time sparing: Doing exchange online is quick which reduces stress and saves time for a specific client and in e-business, there is no driving in circles while looking and delving with expectations of discovering what you require. Stores online offer their full line and in addition use distribution centers rather than storefronts—items are anything but difficult to find and can be conveyed to your entryway not more than days.

Easy to discover surveys: Since the opposition is most extreme, firms online need you to take a gander at other shopper audits. Great and awful surveys are on each side, not just would you be able to check whether the item is enjoyed, you can likewise see the explanations for the thumbs up or down.

Options, choices, choices!: E-business online gives parcel of dialog boxes in which customers can pick their craving choice indoor to accomplish a particular errand as indicated by their suitable expert document. What is more, the buyer can without much stress thoroughly analyze items for another to see who offers the best value and have more choices to browse.

Easy to analyze: Items that are put online for attention are anything but difficult to contrast them and different things internet, knowing they have the best choices and can return for additional in other to accomplish a particular undertaking.

Easy to compare: E-commerce makes things simple for humanity separated from diminishing anxiety, it is a stage that enhances the nation's economy. Case Nigeria, instead of starting with one specific district then onto the next.

Coupons and bargains: With each online business, more coupons and arrangements can't be maintained which is a strategic distance that is awesome for clients. With significant destinations that go about as retail establishments, you may discover things up to 80% off! Exploit the opposition and locate the best cost accessible.

Demerits of E-Commerce Security Framework in Nigeria

Delay in getting products: This is one of the demerits of e-commerce that can bring about long postpone of merchandise and administrations because of either terrible climate or atmosphere condition or system jam. Furthermore, the way to deliver items could be troublesome here based on our awful street system. Illustration Suleja to Bida.

Lack of personal association: While the principles and regulations of every e-business are laid out for you to peruse, there is a lot read and it might be befuddling with regards to the legalities. With vast or critical requests, there is nobody you can converse with face to face when you have inquiries and concerns.

Privacy and security: Encryption is the procedure of securing your information or data or set of guidelines from an un-approved workforce. Before making instant exchanges on the web, be certain to check the site certificate of security. So that your data wound is stolen online for simple and advantageous shopping.

Quality: The toughness or convey ability of any item is extremely vital in the e-business security framework in Nigeria. A shopper cannot touch items until they are conveyed to the entryway



Purpose of E-Commerce and Security Issues

The purposes E-commerce security framework in Nigeria are:-

1. Study the overview of E-trade security.
2. Proper understanding of the advantages of internet shopping.
3. Proper understanding of the purpose behind security in e-business.
4. Illustrate the different security issues in e-business.
5. Understanding the protected internet shopping rule.

Security Issues of E-Commerce

E-business security is the best possible guiding of Ebusiness resources from an unapproved access use change or obliteration. And, the security danger of business is unapproved access, burglary, and extortion. And, the security highlight of e-commerce is a hypothesis, honesty, encryption, disavowal, accessibility more so; there are some security devices of the E-commerce security framework in Nigeria. Which are:

1. firewalls-programming and physical component
2. Open key infrastructure
3. Encryption programming
4. Advanced endorsement and so forth

Relationship between E-Commerce and E-Business

The subset of e-business is e-commerce which describes the purchasing and selling of items and services and data or making an exchange through personal computer systems, including the web. The main distinction between them is that e-commerce analyzes the interaction among organizations and customers or constituents. On alternate hands-business also incorporates an organization's interior operation in other words these two can be utilized compatible. The terms e-commerce and e-business were regularly alluding to as conversely. The offering of this formal definition denoted the transitioning of the web's selection. more so, the innovation goes past e-commerce which includes different functionalities. For example, e-market, e-franchising-mailing, and some more. E-business idea is based on the above notice viewpoint and the degree digitalization of item, process and the conveyance operators, the business can be poor or incomplete e-business/e-trade. In conventional trade, all measurements are physical while all measurements are computerized while all measurements are digital in pure business/e-commerce.

Buyer behavior to E-Commerce in Nigeria



Numerous individuals in Nigeria are unwilling to exchange e-trade in Nigeria. Inspired by a paranoid fear of web extortion. Nigeria today is not that protected for the web market because there are not trustworthy concerning a client to put their well-deserved fund on a business that is not reliable. There should be legitimate and security infrastructure to be arranged by the government for the purchaser to effectively take part in trade and for the uneducated, they never have faith in trade or e-business. Furthermore, due to day-by-day stories and situations we see on web extortion this could prompt numerous debilitation on purchaser state of mind to e-trade in our dear nation Nigeria.

Entrepreneur behavior to Ecommerce in Nigeria

Numerous business merchant specialists in Nigeria cannot go to web business now because there is not sufficient incentive, formal knowledge on the capability of this lucrative business. Numerous people think that it's costly to keep an internet presence on the web. The readiness of the organization to move far from the conventional method for transacting business and created techniques and important to e-business selection.

E-Commerce Delivery Infrastructure in Nigeria.

Foundation conveyance framework in Nigeria is exceptionally poor numerous houses up till now are not number. No good road connectivity to encourage the simple development of products and services. The postal framework is minimum and secure. Effective e-commerce usage in Nigeria will require a basic redesigning of the conveyance framework in Nigeria. The part of e-business that has stretched out in Nigeria, for the most part, is e-managing an account service (EBanking Service). Internet managing an account framework has gotten to be normal for Nigeria clients as they are given in adaptability in administration their record in any benches of their bank's framework.

Parties Involved in E-Commerce

There are no less than two noteworthy gatherings included in e-commerce exchanges. They are the client and the dealer. While the ones are the backer, acquirer, and the exchanging or clearinghouse. In this task, the hobby is on both the client (person who is occupied with purchasing products) and the vendor (firm or somebody who is keen on offering a few pieces of merchandise).

In this way, two separate arrangements of surveys were managed over these elements.

The firm (Merchant): The entirety of 100 polls were regulated haphazardly among the real firm inside of Lagos city (the business operational hub of Nigeria). The firm cut over petroleum, aeronautics, fund, combinations, IT, and private firm. The firm inside of a specific part was arbitrarily chosen yet with reasonable scope and representation. 99 of the surveys were returned which speaks to 99% of the aggregate number directed.

The Individual (Customer): The aggregate of 500 surveys were controlled and 390 of them were returned, which speaks to 78% of the aggregate. Critical inquiries, for example, Internet access, accessibility of installment cards, level of web trade support, and likely difficulties were postured to them. This gathering is contained arbitrarily chosen people who are transcendently regular workers low maintenance postgraduate understudies of an establishment, and somewhere in the range of a couple of individuals from the overall population.



The AMO/MOA Model

Accessible exploration has distinguished three central points that affect message elaboration and message evoked thinking as inspiration, open door, and capacity (MOA) that direct or serve as predecessors to data preparing by people.

Ramaswani et al., (1998) introduced the same model as the AMO model. That is, a determinant for web determining to obtain qualities the clients' capacity to buy on the web, their inspiration to do that, in addition, the accessible open doors for Internet access. In this manner, the gathered information was dissected taking into account inspiration, capacity, and opportunity (AMO) structure, and unmistakable measurements utilizing the SPSS bundle.

E-Commerce Models

Making an e-commerce arrangement predominantly includes building and sending an e-business site. The firsts Depending on the gatherings included in the exchange, venture in the improvement of an e-business site is to recognize the e-commerce model. e-commerce can be characterized into four models. These are:

1. Business – to – Business model
2. Business – to – Consumer model
3. Buyer – to-Consumer model
4. Buyer – to – Business model

Business-to-Business (B2B) Model: This is otherwise known as a business - to- plan of action which includes electronic exchanges for requesting acquiring, and other authoritative undertakings between houses. It incorporates exchanging goods, for example, producing, business memberships, expert administrations, and wholesale dealings.

The Merits Of Business To Business Model Are:

- a. Business to business productively keeps up the supply's development chain, assembling and obtaining procedures.
- b. Business to business improves fast conveyance of the right items and services. Business to a plan of action is anticipated to end up the greatest quality division of the business inside of a couple of years which is said to be the speediest developing segment of e-commerce.

Business-to-Consumer (B2C) Model: This is the second model of e-commerce which is otherwise known as the Business to purchaser model which includes exchanges between business organizations and customers. The Business to shopper demonstrates likewise incorporates wellbeing data, administrations internet saving money, travel administrations. Consider a theoretical case in which an exchange is directed between a business association and a buyer.

Buyer-to-Business (C2B) Model: This is the last and final e-commerce model which is sometimes called the customer-to-business (C2B) model that includes an exchange between a shopper and a business association. Also, purchaser to business (C2B) is like the Business to shopper (B2C) model, on the other hand, the distinction is that for this situation the customer is the dealer and the business association is the purchaser.



Various Models in the E-Governance Scenario:

Government-to-Government (G2G) model: This is the first e-governance demonstration that includes exchanges between two governments. For the sample, if the Nigerian government needs to buy oil from the American government, the exchange included is ordered in the administration to government (G2G) model. +

Government-to-Consumer (G2C) model: In government to consumer (G2C) model, the legislature executes with an individual purchaser in other to achieve a particular errand. Case, an administration can uphold laws relating to duty installments on individual customers over the Internet by utilizing the legislature to buyer (G2C) model.

Purchaser to-Government (C2G) model: This is the third model of e-governance, and it can sometimes be called customer to government (C2G) model which is an individual buyer cooperates with the legislature. For example, a customer can pay his pay assessment or house charge on the internet. The exchanges included for this situation are shopper to government (C2G) exchanges. Government-to-Business (G2B) model: This is the second to the last and final model of the e-governance model which includes exchanges between a legislature and business associations. example, the administrative arrangements in other to assemble a flyover. For this, the administration demands tenders from different contractual workers. Government can do this over the Internet by utilizing the administration to business (G2B) model.

Business-to-Government (B2G) model: This is the last and final e-government model which includes business houses executed with the legislature over the Internet. Illustration, like an individual shopper, business houses can likewise pay their assessments on the Internet.

Effort Of Nigeria Government over Ecommerce

1. **Lawmakers' Effort:** The government had initiated various administrative measures to purify the account segment of the economy, for example, the Independent Corrupt Practices Commission (ICPC) Act of 1999; the Money Laundering Act of 1995.
2. **IT Policy:** The Nigeria National IT approach is in charge of the considerable advancements in the division. The vision is to make Nigeria an IT-competent nation in Africa and a key player in the data society.
3. **CURRENT ICT PROJECT:**
 - A. The Mobile Internet Units (MIUs): These incorporate transports furnished with ICT offices, for example, PCs, fringe gadgets, and VSATs which are utilized to convey ICT instruction to country zones.
 - B. The Win Project: This undertaking is labeled "Wire Nigeria". It was planned to give an ICT framework to every one of the alcoves and corners of the nation.
 - C. The E-Government Project: This is a piece of the common administration changes which was intended to make the Nigerian common administration proactive and react forcefully to the general's needs populace.

Analysis of Result

Capacity is alluding to the abilities or capability is the comprehension of an idea. That is, amplifying individual aptitudes and capability in deciphering the idea. By and large, the absence of capacity forecasts absence of information to make online buy or absence of access to the medium. In this way, the capacity examination depended on the accompanying variables: web vicinity, Internet access, accessibility of



installment cards, and support in the online buyer. The outcomes are introduced in the table underneath.

E-Commerce Ability Analysis Table

Legend for Chart:

A - S/N

B - FEATURES

C - Individuals Yes

D - Individuals No

E - Organizations Yes

F - Organizations No

A	B	C	D	E	F
1	Web Presence	148 (47%)	196 (50.3%)	88 (88%)	11 (11%)
2	Internet Access	283 (72.6%)	100 (25.3%)	97 (97%)	2 (2%)
3	Payment Cards Accessibility	141 (36.2%)	241 (61.8%)		
4	Participation in online buy	82 (21%)	296 (75.9%)		

(**) (**) (**) Much of the installment exercises are restricted to installments for utilities/administrations with ATM cards and charge cards utilized as a part of markets and filling stations and not for buys on the web.

Digital E-Commerce Cycle

Security is very important in online shopping sites. Nowadays, a huge amount is being purchased on the internet, because it's easier and more convenient. Almost anything can be bought such as music, toys clothing, cars, food, and even porn. Even though some of these purchases are illegal we will be focusing on all the items you can buy legally on the internet. Some of the popular websites are eBay, iTunes, Amazon, HMV, Mercantila, dell, Best Buy, and much more.



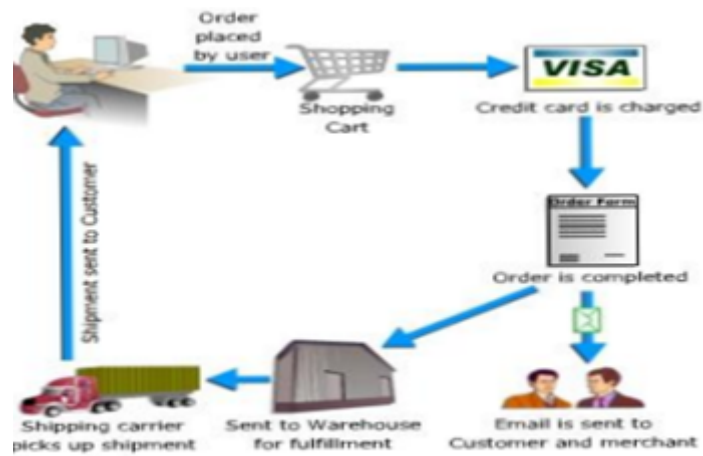


Fig1.: Digital E-commerce cycle

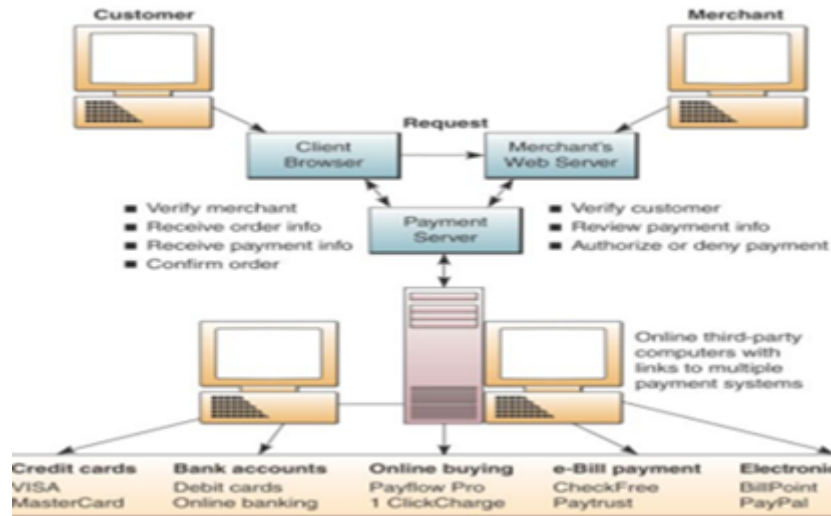


Fig2.: Digital E-commerce cycle

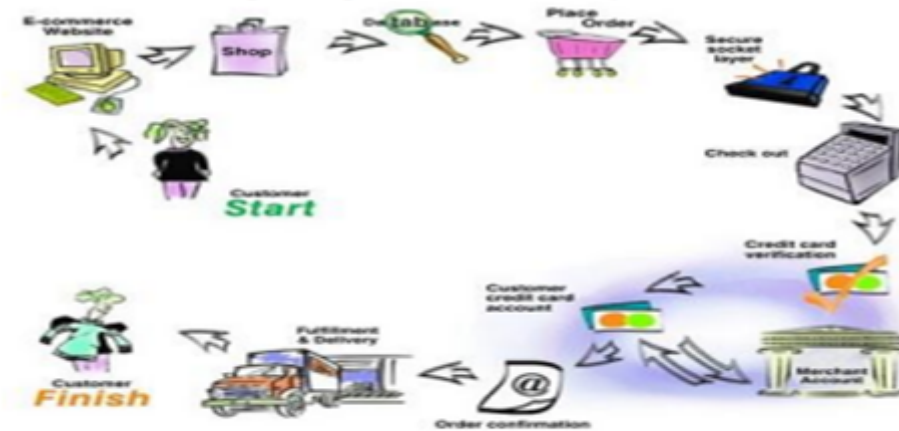


Fig.: Online Shopping - Steps to place an order





Fig. E-Commerce Security Strategy

- § Firewalls – Software and Hardware
- § Public Key infrastructure
- § Encryption software
- § Digital certificates
- § Digital Signatures
- § Biometrics – retinal scan, fingerprints, voice, etc
- § Passwords
- § Locks and bars – network operations centers

Purpose of Security

1. Data Confidentiality – is provided by encryption / decryption.
 2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
 3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
 4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
 5. Non-repudiation – not to deny a sale or purchase Implemented with digital signatures.
- Plaintext/Cleartext – message humans can read.
 - Ciphertext – unreadable to humans, uses encryption. The reverse process is called decryption.
 - A cryptographic algorithm is called a cipher. It is a mathematical function. Most attacks are focused on finding the —keyll.

Security Issues

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:



- **Authentication:** Verifies who you say you are. It enforces that you are the only one allowed to log on to your Internet banking account.
- **Authorization:** This allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- **Encryption:** Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- **Auditing:** Keeps a record of operations. Merchants use auditing to prove that you bought specific merchandise.
- **Integrity:** prevention against unauthorized data modification
- **Nonrepudiation:** prevention against any one party from reneging on an agreement after the fact
- **Availability:** prevention against data delays or removal.

Security Threats

Three types of security threats

§ denial of service,

§ unauthorized access, and

§ theft and fraud

Security (DOS): Denial of Service (DOS)

Two primary types of DOS attacks: spamming and viruses

→ Spamming

- * Sending unsolicited commercial emails to individuals
- * E-mail bombing is caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
- * Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.
- * DDOS (distributed denial of service attacks) involves hackers placing software agents onto several third-party systems and setting them off to simultaneously send requests to an intended target

→ Viruses: self-replicating computer programs designed to perform unwanted events.

→ Worms: special viruses that spread using direct Internet connections.

→ Trojan Horses: disguised as legitimate software and trick users into running the program Security (unauthorized access)

→ Illegal access to systems, applications, or data

→ Passive unauthorized access –listening to communications channel for finding secrets.

- * May use content for damaging purposes

→ Active unauthorized access –Modifying system or data



- * Message stream modification

- Changes intent of messages, e.g., to abort or delay a negotiation on a contract

- Masquerading or spoofing—sending a message that appears to be from someone else.

- * Impersonating another user at the “name” (changing the “From” field) or IP levels (changing the source and/or destination IP address of packets in the network)

- Sniffers—software that illegally accesses data traversing across the network.

- Software and operating systems' security holes Security (theft and fraud)

- Data theft already discussed under the unauthorized access section

- Fraud occurs when the stolen data is used or modified.

- Theft of software via illegal copying from the company's servers.

- Theft of hardware, specifically laptops.

Secure Online Shopping Guidelines

1. Shop at Secure Web Sites

How can you tell if a Web site is secure? Secure sites use encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your credit card number, to prevent computer hackers from obtaining it en route. The only people who can unscramble the code are those with legitimate access privileges. Here's how you can tell when you are dealing with a secure site:

- If you look at the top of your screen where the Web site address is displayed (the “address bar”), you should see HTTPS://. The “s” that is displayed after “HTTP” indicates that Web site is secure. Often, you do not see the “s” until you move to the order page on the Web site.
- Another way to determine if a Web site is secure is to look for a closed padlock displayed on the address bar of your screen. If that lock is open, you should assume it is not a secure site. Of course, transmitting your data over secure channels is of little value to you if the merchant stores the data unscrambled. You should try to find out if the merchant stores the data in encrypted form. If a hacker can intrude, it cannot obtain your credit data and other personal information. Be sure to read the merchant's privacy and security policies to learn how it safeguards your data on its computers.

2. Research the Web Site before You Order

Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start with an inexpensive order to learn if the company is trustworthy. Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line. Call the phone number and ask questions to determine if the business is legitimate. Even if you call after hours, many companies have a “live” answering service, especially if they don't want to miss orders. Ask how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.



You can also research a company through the Better Business Bureau (see listing below), or a government consumer protection agency like the district attorney's office or the Attorney General. Perhaps friends or family members who live in the city listed can verify the validity of the company. Remember, anyone can create a Web site.

3. Read the Web Site's Privacy and Security Policies

Every reputable online Web site offers information about how it processes your order. It is usually listed in the section entitled —Privacy Policy. You can find out if the merchant intends to share your information with a third party or affiliate company. Do they require these companies to refrain from marketing to their customers? If not, you can expect to receive —spam (unsolicited emails) and even mail or phone solicitations from these companies. You can also learn what type of information is gathered by the Web site, and how it is — or is not — shared with others. The online merchant's data security practices are also often explained in the Privacy Policy, or perhaps a separate Security Policy. Look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related practices, such as TRUSTe (www.truste.org), Verisign (www.verisign.com), or BBBOnline (www.bbbonline.org). However, be aware that a strong privacy policy and membership in a Web-seal program don't guarantee that the Web merchant will protect your privacy forever. Policies can change. The company can file for bankruptcy and sell its customer database. The Web merchant might be purchased by another company with a weaker privacy policy. And the company's data can be subpoenaed for law enforcement investigations or civil cases. You have little control over the use of your customer data in such matters. Given all of these uncertainties, you will want to think about the sensitivity of the data that is being compiled about you when you shop online. We cannot prescribe the best approach to take. Each consumer has a different interpretation of what is considered "sensitive."

4. Be Aware of Cookies and Behavioral Marketing

Online merchants as well as other sites watch our shopping and surfing habits by using "cookies," an online tracking system that attaches pieces of code to our Internet browsers to track which sites we visit as we search the Web. "Persistent" cookies remain stored on your computer while "session" cookies expire when you turn the browser off. Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies but the tradeoff may limit the functions you can perform online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order. Privacy advocates worry that as more and more data is compiled about us — without our knowledge or active consent — it will be combined to reveal a detailed profile, even our actual identities. This data is often collected to market goods and services to us, encouraging us to buy them. Several companies specialize in targeted online advertising called "behavioral marketing." Companies say consumers benefit by being exposed to more targeted advertising and that online merchants can make more money more efficiently by targeting the right shoppers. For example, you might buy a book on golf from Amazon, visit the Professional Golfer's Association site, purchase golf shoes at Zappos, and search online for golf courses near your home. When you do, a cookie or your computer's Internet Protocol (IP) address could be used to generate golf-related ads. When you open the USA Today site to read the morning news, you may see an ad offering you a new set of clubs at a discount. When you go back to Amazon later that day you might be offered a biography of Tiger Woods. What if your behavioral marketing profile is shared with others, without your permission? You might not care if a drug company shares your prescription drug information with a coupon service to save you money. But what if that same information were obtained by your employer, resulting in more expensive health insurance coverage?

5. What's Safest: Credit Cards, Debit Cards, Cash, or Checks?

The safest way to shop on the Internet is with a credit card. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. When it has been determined that your credit was used without authorization, you are only responsible for the first \$50 in charges. You are



rarely asked to pay this charge. For more information on credit card consumer protections, see <http://www.privacyrights.org/fs/fs32-paperplastic.htm#3> Make sure your credit card is a true credit card and not a debit card, a check card, or an ATM card. As with checks, a debit card exposes your bank account to thieves. Your checking account could be wiped out in minutes. Further, debit and ATM cards are not protected by federal law to the extent that credit cards are. The —Restore Online Shoppers' Confidence Act (P.L. 111- 345) (signed December 29, 2010) makes it illegal for a company that sells goods or services online to give a consumer's credit card number (or another financial account number) to a third-party for sales purposes. This practice is known as —data passing. The Act prohibits a third-party seller from charging a consumer for any good or service, unless the seller (1) clearly and conspicuously discloses the material offer terms and that the third-party seller is not affiliated with the initial merchant and (2) receive express consent for the charge from the consumer. The third-party seller must obtain the full financial account number directly from the consumer. The initial online seller may not transfer a consumer's financial account number to a third-party seller. The Act also regulates —negative option plans. A consumer must give express, informed consent before being charged for goods or services sold online through —negative option marketing, such as —free trials that the consumer must cancel to avoid being charged. Companies that use negative option plans must (1) clearly and conspicuously disclose the material terms of the transaction before obtaining the consumer's billing information, (2) obtain a consumer's express consent before charging the consumer, and (3) provide a simple mechanism to stop any recurring charges. Online shopping by check leaves you vulnerable to bank fraud. And sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase. Never pay for online purchases by using a money transfer service. You could be transferring cash to a fraudster. Scammers will ask consumers to send the payment using a money transfer service such as Western Union or MoneyGram because they can get your cash fast and it's difficult to trace. Legitimate sellers normally do not ask consumers to send payment that way. Money transfer services should only be used to send money to people that you know well, not to unknown sellers of merchandise online. Watch the Consumer Federation of America's video about this at <http://www.youtube.com/watch?v=R2yIW85g1So>

References

<https://www.seminarstopics.com/>

◀ Preliminary Activity for Week 5

Jump to...



Analysis, Application, and Exploration for Week 5 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 2

Network Defense and Remote Access Configuration

OJT/Practicum 2

Seminars and Tours

Participants



General

01 [Enter Module Title Here]

02 [Enter Module Title Here]


03 [Enter Module Title Here]

04 [Enter Module Title Here]


05 [Enter Module Title Here]

 Preliminary Activity for Week 5

 **Lesson Proper for Week 5**

 Analysis, Application, and Exploration for Week 5

 Generalization for Week 5

 Evaluation for Week 5

 Assignment for Week 5

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for *free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.*


PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

 Assignments

 Forums

 Quizzes

 Resources

