<<NetAction>>

Introduction

If you like adventure and intrigue, this is a great time to be online. Electronic shopping is making our lives more convenient and our buying more cost-effective—when it works.

Electronic commerce, or e-commerce, is a term that describes the online commercial transactions that people, organizations, and businesses engage in with each other. On the customer level, e-commerce refers to the sale of goods or services arranged and carried out online, through "virtual storefronts on the web" as well as via chat rooms, USENET and newsgroups, bulletin boards, and email. This includes buying items such as books, software, and toys from web-based stores using a (secure) web server, buying airline tickets from someone in a chat room, or researching a product in appropriate newsgroups.

This guide will help you become educated about the online shopping experience. Here are several examples of various resources and activities.

Shopping Online

Shopping online has elements similar to traditional shopping, with added conveniences such as price and availability comparisons, 24-hour access to stores, and more. Shopping online also has disadvantages: you can't feel the fabrics, or smell the northern woods before your vacation. As a time- and money-saving tool, it can be very useful.

If you're thinking of buying something over the Internet, you might start with larger, reputable retailers with which you have already done business in your neighborhood or through their mail-order catalogs. They are likely to have relatively intuitive online catalogs with search features, secure online ordering, and dependable delivery and return/refund policies. Many of the smaller retailers will have these features too, but their reputations and histories may be harder to determine.

Comparison Shopping

Want to know how one company's price compares to another's? Many sites feature this information. (See the Researching Products and Vendors section for more on this.)

Travel Services

Finding a travel bargain online can be a great way to start planning that long-needed vacation. Increasingly, airlines and hotels are making last-minute bargain fares available online through special e-mailing lists, and on airline and related web sites. With quicker and more thorough information available, individuals can conveniently search and compare flights and other travel arrangements to their hearts' content. Beware, however, of travel scams—one of the fastest growing forms of fraud on the Net today. (See the Protection from Fraud section for more on this.)

Banking and Online Trading

Because the Internet and related technologies offer customers lower cost and faster access to financial markets, e-commerce is changing the way our markets work. Banks are one example; many now offer online banking, allowing account holders to transfer funds between accounts, pay bills, and more.

If the stock market is your passion, stocks, bonds, and mutual funds can be purchased, sold, or traded through various online trading firms. Online brokerage accounts currently represent some 25 percent of all retail stock trades. Remember that the same laws and rules of return that apply to traditional trading also apply to trading online.

> SITES TO SEE:
>
> SEC Chairman Levitt Cautions Online Investors
> `http://www.techlawjournal.com/seclaw/19990128.htm`
> and Levitt's statement: with cautions on trading volatility, execution delays, and other concerns:
> `http://www.techlawjournal.com/seclaw/19990127.htm`

Auctions

Auction and bidding sites are increasingly popular forms of e-commerce. These sites carry collectibles and retail products sold by individuals, as well as manufacturers' overstocked and clearance merchandise. Many auction sites require registration or membership. Many also have buying safeguards to help you confirm that the item you're bidding on is really what you want. Auction sites can become dangerously addictive for some people. Because auctions are not regulated, be sure to review the cautions in our Protection from Fraud section.

Online Charitable Giving

A variety of web sites are available to make charitable giving easy and convenient. Online environments are set up as donation clearinghouses, charity-supporting online shopping malls, and more. These companies help support the work of your favorite charities and non-profit organizations. Be sure to keep records for tax purposes.

SITES TO SEE:

FTC's Operation "False Alarm" (about online charitable giving)
`http://www.ftc.gov/bcp/conline/edcams/badge/index.html`

NetAction Notes 51 (also see Notes 53, & 54)
`http://www.netaction.org/notes/notes51.html`
`http://www.netaction.org/notes/`

Gift Certificates and Coupons

Many online merchants encourage you to shop or dine with them by offering electronic coupons which can be printed from your home computer and used like the coupons you find in your Sunday newspaper—to save money on a vast array of local goods and services. Shoppers should be aware that visiting these web sites and downloading their coupons also helps marketers learn more about buyers' interests and purchasing patterns.

Many large department stores also have online versions of their gift registries. Receiving gift certificates can make your online shopping experience convenient, since someone else has already paid for what you purchase.

Spam

As Internet use has skyrocketed, so have complaints about unsolicited commercial email, also called "junk email" or "spam." Most Internet Service Providers publish Acceptable Use Policies (AUP), which prohibit sending spam. Nevertheless, the promise of a quick buck is a powerful motivator. (See the Marketing and Protection from Fraud sections for more on this.)

Researching Products and Vendors

Few shopping experiences are complete without a little research. When you're looking to buy something new, you may ask friends what they know about a product that interests you, or you may look for product reviews. Different kinds of information might be helpful in your decision making.

At times, the Internet makes such research easy. There are search tools, independent reviews and product recommendations, comparison shopping sites, public-reputation references, and other resources available to buyers. Types of research can include product feature comparisons on the items and models, different manufacturers, warranties, and prices.

Here are some tips to help you get started on researching products and services. Bookmark those sites you find the most helpful.

Check Manufacturers' Sites

Some manufacturers have gotten wise to customer needs and interests. Their web sites offer general sales information as well as detailed specifics about each of their products. Some offer comparison guides for similar goods, while others offer detailed reports with illustrations or schematics. In addition, manufacturers' sites often offer FAQs (Frequently Asked Questions), along with the company's warranty and return policies. Some even offer online discussion areas, and referrals to vendors carrying their goods and services.

Check Out the Used-Equipment Market

Used-equipment sites like used-goods dealers, auctions, online chats and discussions, and alternative support sites can reveal how well something was built and how long it lasts. Do you see a lot of these goods for sale cheap—as if people are getting rid of a product—or do people seem to be looking for them? Are the products in need of repair—or all as good as new?

Comparison Shopping

One way to compare prices is to visit several retailers. Another is to visit one of the price-comparison sites such as those listed below.

You might also include a visit to discounters, and be sure to watch for sales, coupons, rebates, and special deals like inclusion of shipping costs. It also might be helpful to have a back-up option in case the specific model you want is out of date or no longer available.

Many sites such as bizrate.com, gomez.com, and consumersunion.org offer product reviews, comparisons, and evaluations. Some sites require membership or payment. New comparison sites are frequently appearing on the web—beware: the newer sites may offer fair and unbiased opinions, or they may offer reviews from a few disgruntled employees or others with a biased interest.

SITES TO SEE:

`http://www.consumersunion.org/`
& related `http://www.consumerreports.org/`

`http://www.bizrate.com/`

`http://www.gomez.com/`

`http://www.mysimon.com/`

`http://home1.bestedeal.com/cgi-bin/index.cgi`

`http://www.shoppingspot.com/`

Dynamic Pricing

Many retailers are working with or testing systems that charge different prices for the same goods under different circumstances. Prices are based on what the retailer thinks you're willing to pay, which in turn is based on where you live, whether you're a return customer, what site "referred" you (what site you were visiting immediately before), or other profiled information. Dynamic pricing also allows a vendor to change prices rapidly in response to changing market conditions by raising the price of a popular toy the moment demand starts to overtake its supply, for example. Or, if the vendor wishes to encourage visits to a local store, he or she might lower prices of goods to customers who live or work nearby. (See "Digital Profiling" in the Privacy and Security section for more on this.)

Find Out What Others Are Saying

Reputation is just as important online as in the bricks-and-mortar world of traditional shopping. When people have something to say, they say it—good or bad. These ad hoc reviews can be very revealing! Several sites, sometimes called "reputation managers," exist to provide such independent reviews and opinions. The auction site eBay, for example, allows buyers and sellers to comment and rate each other publicly, making it easier to spot the bad guys.

SITES TO SEE:

http://www.webwatchdog.com/

http://www.epinions.com/

Additional resources might include sites that your friends have recommended or that you have researched thoroughly. Remember also to check online auctions, classifieds, third-party distributors, advertisers, and commerce-oriented search engines.

Check for Compliance with Industry Certification Programs

The White House, for example, has expressed concern that citizens have no way of telling whether an online pharmacy is a legitimate operation. To be safe, make online prescription purchases from sites certified by the National Association of Boards of Pharmacy. This organization developed the Verified Internet Pharmacy Practice Sites (VIPPS) program in response to public concern about the safety of online pharmacy practices. Wise shoppers will also look for reputable brands and make purchases from web sites that provide contact information, including phone numbers and street addresses. The Food and Drug Administration (FDA) also offers useful advice to help people evaluate pharmacy sites.

SITES TO SEE:

FDA Consumer report: Buying Drugs Online: It's Convenient and Private, but Beware of 'Rogue Sites'
http://www.fda.gov/fdac/features/2000/100_online.html

The Devil Is in the Details

Before confirming your purchase, be sure to look for any extra charges including shipping and handling, rush charges, taxes, leasing arrangements, duty on imports, transaction fees for overseas buyer/sellers, return arrangement, and more.

Ask About Customer Support

Before you make an online purchase, learn everything you can about the merchant's customer support policies. Repeat business depends on customer satisfaction, so reputable online merchants will want to include information about warranties, repairs, returns, and service provisions. If you can't find this information, you may be better off buying from another online merchant. Here's a basic checklist of questions to ask before completing an online transaction.

- Does the merchant provide complete contact information, including a phone number and an email address as well as the street address where the business is located?
- Does the merchant respond promptly to telephone and email inquiries?
- Is there a warranty on the item you want to purchase? If so, for how long? Is the warranty provided by the manufacturer or the vendor?
- In the event the item needs to be repaired, will you have to ship it to the manufacturer, or is there an authorized service center nearby? Does the warranty cover the cost of parts needed for repairs, or just the labor? Do you need to request pre-authorization before you return an item or send it back for repair?
- What is the merchant's return policy? If you return an item, will you be entitled to a full refund, or will you be given credit on another purchase? Is there a deadline for returning an item you decide you don't want? Is there a restocking fee?
- What is the merchant's customer service reputation? Check for reviews.

Paying Online

You've put your selections into the shopping cart, and you're ready to check out. The next thing you'll need to do is provide a way to pay for your goods. There are many ways to do this, as explained below.

- using a credit card—on a secure server
- using an electronic wallet
- putting your payment into an escrow account
- calling a customer service number with your order and credit card
- paying by check, money order, or COD for an off-line order

There are a few special considerations to keep in mind:

- If a problem occurs and you paid by cash, check, or money order, you will have little leverage in resolving your problem. **Never** send cash through the mail.
- If you are contemplating the sale or barter of items, don't forget that you are responsible for complying with all applicable laws and regulations, including taxes.
- International transactions raise special concerns about payment, including cost and method of currency conversion, duty charges, and assumption of shipping and other expenses.

Be sure to check the Privacy and Security section for instructions on how to confirm your use of a secure server before you make an online credit card payment.

Privacy statements should also be checked! Review the site's privacy statement to see whether its database of credit information is encrypted (scrambled) and stored securely; and if access to those files is limited to necessary merchant personnel, how long the data are stored; or alternatively, if credit information could be purged after processing.

SITES TO SEE:

Federal Trade Commission's Guide to Online Payments
`http://www.ftc.gov/bcp/conline/pubs/online/payments.htm`
and their related Shop Safely Online
`http://www.ftc.gov/bcp/conline/pubs/online/cybrsmrt.htm`

Using Your Credit Card Online

Many people consider online transactions to be safer than transactions in the physical world of traditional shopping. Payment by credit card offers cardholders the most liability protection of any of the methods of payment for online purchases. Under the Fair Credit Billing Act, customers are liable for only the first $50 of reported fraudulent credit card transactions. In addition, some cards provide additional warranty or "purchase protection" plans on purchases made with that card.

In the case of credit or debit card orders, find out if your purchase will initiate a recurring charge with the merchant. For example, if you order a subscription online, will they automatically recharge your card at renewal, or will they contact you first? If it is to be an approved recurring charge, make certain to take note of the cancellation policy.

Pre-Paid Internet Shopping Cards

Major credit card companies are introducing a variety of disposable credit cards that can be used on the Internet. American Express, for example, has teamed up with 7-11 to sell you a card with values in increments of $25, up to $1000. This is a nice extension of the anonymity of cash, but is only usable at

stores that accept American Express cards. MBNA, a major credit card issuing company, offers its customers an alternative that requires them to use MBNA's website to generate a one-time use credit card number. Ask your bank or card issuer if they have something that might work for you.

Using Debit Cards Instead of Credit Cards

Your financial liability may be a problem when using a debit card for purchases, so make sure you understand your issuing bank's policy on debit cards—the limit of your liability and the process in case of dispute—before using them for online transactions. Since your payment is automatically debited from your account, you must seek other recourse in case of a dispute with your vendor. (See the Privacy and Security section for more on this.)

Electronic Wallets

Electronic wallets are another way to pay for goods and services online. A wallet service typically keeps your billing and shipping address(es) and credit card number(s) on file—in an encrypted form. Vendors who support the different kinds of wallets use special server technology that can read your credit card information when you're ready to buy.

SITES TO SEE:

`http://wallet.yahoo.com/` (an example)

Escrow Accounts

Both buying and selling on the Internet involve transactions with people you don't know. Escrow accounts can be a safe and convenient way to buy from such people. Typically, the buyer deposits a payment with an escrow service. The seller ships the goods, and when the buyer accepts them, the escrow service releases the buyer's funds to the seller. Otherwise, the goods are returned to the seller and the payment is refunded to the buyer.

SITES TO SEE:

`http://www.paypal.com/`

`http://www.rocketcash.com/`

Online Billing, Bill-Paying Services, and Account Managers

Do you dread the postal delivery of bills from utility companies, phone and cable companies, credit cards, and more? Perhaps you'd appreciate the convenience of having all your bills online, in one place, where you can review, manage, and pay your accounts from one service. You can commonly find this service through your bank or from select commercial Internet service companies. Other services, such as frequent flyer mileage accounts, can also be managed through an online service.

Be aware that your online payment may not go directly into your provider's account. Many companies don't yet participate in electronic funds transfer, so your bill-paying service may need to write a check for you and mail it. If

something happens to the check that they wrote on your behalf, you're responsible.

Online Purchases with Off-Line Payment Methods

Two common options exist for making purchases online but paying off line:

- Gather information online, then place your order by phone. This method is as safe as other mail or phone order services.
- Send your order on paper with a check or money order by regular mail, or using UPS, FedEx, or another ground or air shipper for insured safety.

The Privacy and Security section has more information on why this might be important.

Return or Exchange of Gifts

When purchasing a gift for someone, ask questions in advance. Who gets credit for returned merchandise, the purchaser or the recipient? Who is charged for the return shipping? Does the vendor site have a policy on this, and is there any way around it?

Shipping and Delivery

This is an often-overlooked area with special considerations. In general, look for the vendor's delivery options, restrictions, and policies. Read the fine print to find out if there are taxes, additional handling, or other fees; if the return policies include who pays for return shipment should that become necessary; whether delivery is available to your personal mailbox or rural address; and the expected delivery time frame. Check to see if this site lists any legal or commercial restrictions on purchase, transport, or delivery of your order, and what recourse you have in the case of unfulfilled or incorrect orders. In case your shipment is delayed, do business with merchants who don't charge your credit card until the item is actually shipped. Many of these considerations are especially complicated when you order internationally.

Take special care to consider the following:

- **Big-Ticket Items** (Automobiles, Major Appliances, Jewelry and Artwork)
  Check on shipping or delivery insurance, service warranties, installation and delivery schedules, the impact of online purchase on your homeowner's insurance, special return policies, taxes.
- **Electronics**
  Check warranties, return and refund policies, customer support options.
- **Clothes**
  Check size, color, and fabric options as closely as possible to reduce returns.
- **Food and Other Perishables**
  Confirm delivery times, avoid purchasing highly perishable items.

- **Contractors and Other Services**
  Confirm service delivery options, cancellation and refund procedures, possible arbitration options.
- **Postage**
  Check the refund policy for misprinted or unusable postage.

Keep a record of your transactions, including the date, the name of the person you spoke with, and a confirmation number, as well as the estimated date of delivery.

The Law is On Your Side

Mail order and telemarketing laws also apply to online merchants. The Mail or Telephone Order Merchandise Rule, which is enforced by the Federal Trade Commission (FTC), applies to all orders placed by phone, fax, or over the Internet. Under these rules, it's assumed that the item will be shipped within 30 days unless the merchant states otherwise. If the item you ordered can't be shipped by the promised date (or within 30 days), the merchant must notify you of the delay, provide a revised shipment date, and explain your right to cancel the order and obtain a prompt refund. You should be aware that merchants also have the right to cancel orders that can't be filled on time. If the merchant cancels your order, you are entitled to a prompt refund.

Marketing

Promotional versus Informational Content

It is increasingly difficult to distinguish between advertising and content in online media, as the lines between them blur. Not only are advertisements appearing in web banners, but they are attached to information "tickers," built into games, and written into "news" items. Targeted delivery of combined content and advertising tends to obscure any distinction between them. It takes a conscious effort to recognize the characteristics of advertisements in these unusual placements. Occasionally it is difficult to realize that entire corporate sites may be advertisements.

Visitor Information Gathering

In order to better market to a consumer's tastes and interests, online businesses frequently use "cookies," a little bit of text placed on your computer by the web sites you visit. (To learn more about cookies, see the Privacy and Security section.) Cookies help businesses identify you as a registered customer; track your purchases, movements, and actions; and develop an understanding of your interests. This information helps them tailor advertising more effectively on web sites and via email. Remember, too, that online registrations and applications—as well as special offers such as banner ads, coupons, special promotions, contests, sweepstakes, give-aways, discounts, and rebates—enable businesses to collect more personal information about you.

Express Your Preferences

Some people enjoy receiving targeted product information, but others would rather not receive it. To some extent, you can control the amount of marketing information that is targeted or directed to you. For example, you may wish to encourage targeted marketing if you'd like to receive particular news, updates, and discounts. Alternatively, you may wish to decrease your exposure, for more privacy or freedom from unwanted advertising.

Except for spam, you can take control of what is marketed to you online.

If you *like* to get direct marketing information:

- Set the preferences in your web browser to **enable** cookies, javascript, and java.
- When you visit sites that interest you, register yourself by signing guest books and completing questionnaires, surveys, and applications.
- If you spot a banner ad that interests you, click on the ad.
- Take advantage of personalized (My) sites by customizing and using them.
- When you see offers for personalized newsletters, searches, and other application tools, sign up to have them emailed to you.
- Watch for free offers, contests, coupons, rebates and other special deals, and register with the sites that offer them.
- If you receive an unsolicited commercial email, answer it if the sender is offering something that interests you.

If you *don't like* to get direct marketing information:

- Set the preferences in your web browser to **disable** cookies, javascript, and java. Note that some shopping cart and other features may become disabled. (If you don't like this, send feedback to the site's webmaster.)
- Never sign guest books or fill out surveys, questionnaires, or applications, even when you visit sites that interest you.
- Don't click on banner ads, even if you spot one that interests you.
- Don't customize any of the personalized (My) sites.
- Don't subscribe to newsletters or ask for personalized searches.
- Ignore free offers, contents, coupons, rebates and other special deals, and never register with the sites that offer them.
- Ignore all unsolicited commercial email; just delete it rather than asking to be taken off the list.

- Be proactive about fighting spammers—bring their abuse to the attention of your ISP; and if you know how, to the host of relayed domains being used by the spammer, and the domain hosting the spammer.
- Let your legislators and representatives know how you feel.

Opt-In versus Opt-Out Approaches

Find yourself getting junk mail you didn't request? You're in a database that's being shared among marketing departments or companies. If you could remove yourself, you would be opting out, or choosing the option to be removed from that database. When you call a company for a catalog, you are opting in, or joining its list. As we know from our practical daily lives, we do not have the option to choose removal from most marketing lists these days. Once you're in, you're everywhere.

Congress is currently considering legislation that would allow individuals to opt in or opt out of various databases. You should write to your congressperson voicing your opinion on your choice of practices.

SITES TO SEE:

Tech Law Journal's Summary of Anti-Spam Legislation
`http://www.techlawjournal.com/cong106/spam/Default.htm`

Branding

Many online products and companies are those you already know from catalogs or your neighborhood. A brand name often comes with a dependability and reputation you know about.

Be aware that brands you are familiar with may be linked to unrelated sites and services of separate businesses, with different histories, policies, and practices. Each linked site should be researched separately. Remember that the linked company's site is not covered by your vendor's policies.

Spam

Unsolicited commercial email (UCE), also called "junk email" or "spam," continues to plague us like a bad cold. In general, people do not want their e-mailbox clogged with ads promoting pornography, unwanted products or services, or come-ons for the latest get-rich-quick scheme. Many people abandon the use of their online accounts when junk email gets to be more onerous than the account is beneficial.

Spam is such a hot-button topic among Internet users that anti-spam legislation has been passed by Congress and continues to be a topic of debate among lawmakers. Most Internet Service Providers (ISPs) publish Acceptable Use Policies (AUP) which prohibit sending spam. Account holders agree to these conditions when they sign up for an account; violations can result in having their accounts closed and possibly being assessed fines. Still, it's a prevalent practice. (For more on this topic, be sure to check out the Protection from Internet Fraud section.)

Be aware that most spam senders do not care if you are interested in their email or not. It's free to them. Most will not remove you from their lists, and in fact will use your request to confirm that your email address is working, which makes their database more valuable for resale to other spammers. Some spammers use a reference to a Murkowski Bill making their activities legal—there's no such law, and their activities are not legal.

SITES TO SEE:

JunkBusters
http://www.junkbusters.com/

Sample Acceptable Use Policy
http://www.earthlink.net/about/policies/aupolicy.html

Marketing to Children

There are growing numbers of children online. According to a recent report, some 16 million young people under age 18 are online, and over 6 million of these are children aged 12 and under.

Children, like adults, are online visiting stores—as well as using email, game software, chat systems, and message boards. But, unlike adults, children often don't know how to recognize unsafe situations or invalid claims. Children are surprisingly susceptible to things that blink or are animated, look like games, can be personalized, or "do something" or even simply say "click here." Some unscrupulous Internet companies exploit children's trusting nature by enticing them to share private information. Children need help with their privacy and security online. If parents decide to allow their children to use the Internet to buy online, they should make sure their children understand how to use and make purchases safely and responsibly.

SITES TO SEE:

http://www.ftc.gov/os/1998/9809/priva998.htm

Children's Online Privacy Protection Act of 1998 (COPPA)

A recent law, the Children's Online Privacy Protection Act of 1998 (COPPA), went into effect on April 21, 2000. This law requires certain commercial web sites to post a privacy policy, obtain verifiable parental consent for a child's information to be submitted online, and offer options regarding disclosure of that information to third parties. The act allows civil penalties for violations.

SITES TO SEE:

http://www.ftc.gov/bcp/profiling/index.htm

In planning this law, Congress established in October 1998 the Child Online Protection Act (COPA) Commission "to study methods to help reduce access by minors to certain sexually explicit material, defined in the statute as harmful to minors." The Commission recently issued a report that recommends steps to assist in empowering and educating the public, in law

enforcement, and in industry self-regulation. Under public education, their recommendations include a campaign to promote public awareness of technologies and methods available to protect children online, and promotion of Acceptable Use policies. "Consumer Empowerment" efforts include allocating resources for independent evaluation of child-protection technologies; improvement of industry mechanisms; a private-sector conversation "on the development of next-generation systems for labeling, rating, and identifying content reflecting the convergence of old and new media;" and our government's encouragement of the use of these technologies.

SITES TO SEE:

`http://www.copacommission.org/report/`

`http://www.peacefire.com/`

While NetAction agrees in principle with the Commission's findings, we encourage a more hands-on approach, as described below.

What Parents Can Do

Supervise your children's use of your credit card, and/or fund a pre-paid account for their use. Guide them through a basic budget so they know where their online finances stand.

Teach children to think carefully about what they read online so they can:

- recognize and understand the difference between information and product ads
- decide for themselves if information is truthful and comes from a reliable source
- understand that web sites they visit for entertainment may in fact be advertisements

Teach children to recognize when they are being asked for personal information and to refuse requests for personal information unless they first obtain your permission. You should also discuss with your child the implications of supplying false information.

Make it a rule that your children get permission from you before registering on a site, signing up for a contest, asking for a pen pal, responding to a poll, survey, questionnaire, or application, signing a guest book, or giving out any personal information.

Explain to your children why they should never divulge personal information publicly in chat rooms or message boards, or privately in email, without first asking for your permission.

Investigate the "parental control" features on private membership sites so you know what content they exclude. Filters differ widely in their identification of harmful material. Their priorities affect their ability to

discriminate, for example, between pornography and legitimate medical reference materials.

If you are considering using any parental control tools, do your own research and only use those tools that are suited to your needs. These include:

- browsers or membership sites oriented toward childeren
- software intended to be used for filtering, censoring, or blocking access to particular web content or ads
- Internet Service Providers that offer filtering services, or censoring or blocking software
- rating systems
- software that lets you track or monitor the sites your children visit

Talk to your children about what they may see on the web, whether or not they are using filtering or other parental control programs. Make sure your children know that you have concerns about some of what they might see online. Explain that many web tools do not block alcohol and tobacco sites and advertisements.

Privacy and Security

How and Why to Protect Your Privacy

Your privacy is valuable and should be guarded! If it is treated carelessly, you could find that unauthorized charges have been made to your credit card, or that your credit has been damaged, or even that your credit profile and financial reputation have been hijacked by another.

Less seriously, you could even find yourself swamped with unsolicited email, an increased amount of junk postal mail, or more telemarketing calls. The benefits of being online far outweigh the risks, but being aware of the risks and knowing about available resources and support is important.

Make sure you know whom you are giving private information to, why they need it, who will have access to it, how it is protected, and what it may be used for. Also find out how you can correct any errors, or remove yourself from a company's database. If you're ordering a gift for a friend, will the recipient mind the disclosure of his or her personal information?

Be especially cautious when asked to provide Personally Identifiable Information (PII), such as:

- Social Security number
- place of birth
- mother's maiden name
- driver's license number
- bank account information

- credit card number (if it is not necessary for the transaction)

Remember that any page collecting Personally Identifiable Information (PII) should be linked to a privacy policy. Check it out!

SITES TO SEE:

Electronic Privacy Information Center
http://www.epic.org/
and their online report:
http://www.epic.org/reports/surfer-beware3.html

Privacy Rights Clearinghouse
http://www.privacyrights.org/

Profiling and the Digital You

Profiling, also called "creating a digital profile" or a digital persona, is the practice of compiling information about your habits, preferences, and interests—gathered primarily by tracking your movements online. While your movements and interests at one site may not be significant, the combination of your total movements, interests, and purchases across the Internet paint a more complete (if, at times, false) picture. Using the resulting consumer profiles, advertisers create targeted advertising for any web site you visit. Some consumers enjoy this personalized experience; others consider it an invasion of their privacy.

Some sites work in covert partnership to convey visitor information to each other. Data can then be compiled about you in many ways and places.

If you are concerned about your privacy, you might find it helpful to research some of your interests anonymously, using one of several anonymizing web services as a proxy for your surfing.

SITES TO SEE:

http://www.ftc.gov/bcp/profiling/index.htm

http://www.anonymizer.com/

http://www.epubliceye.com/

Another option is to use a “disposable” email address. A good “disposable” email address is separate from a personal or work email address and prevents strangers from easily gaining information about the sender merely by looking at the address. The email address jsmith@netaction.org would not make a good “disposable” address because strangers can easily decipher that the address belongs to someone at NetAction whose last name is “Smith.” But an address like howdy@yahoo.com doesn’t reveal anything about the sender.

Good places to obtain “disposable” email addresses are web sites that offer free webmail, such as Yahoo or Hotmail. A list of free email services is at:

http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Communications_and_Networking/Internet_and_World_Wide_Web/Email_Providers/Free-Email/.

Cookies

Cookies, the little bits of text placed on your computer by web sites you visit, help the vendor identify you, including when your last visit was, which pages you visited, and references to past or potential purchases, among many other things. A cookie can stay on your computer for minutes or for years.

Cookies are also placed on your computer by advertising companies as a part of their banner ads. Whenever you click on such an ad, a little bit of data about you gets added to their "digital profile" of who you are and what you're interested in. The Marketing section has more on this.

In your browser's preference settings, you can choose to turn cookies off or receive an alert each time a site wants to set a cookie on your computer. If you turn cookies off, some sites (shopping carts or other features) may be disabled or less functional. However, not all shopping technologies are dependent on cookies, and not all sites tell you if cookies are required. You should feel free to explore your options to find a level of functionality and comfort that suits you.

Low- and no-cost programs are available to edit your cookies file. You may wish to get rid of those cookies from one-time visits or from specific sites or advertisers.

Keeping Track of Your Accounts and Transactions

Remembering all of your data interactions—account identification, password, and other registration details—can be a challenge. In this time of major corporate mergers and acquisitions, the company that collects your data may, along the way, be operating under different policies. Even without changes in administration, information-use policies may be changed, even retroactively, so it is advisable to keep track of your vendor's evolving behavior. Check your accounts and site policies occasionally, and exercise your option to correct information or opt out of your vendor's database.

How to Protect Your Privacy

There are many practical and common sense things you can do to help guard your privacy if you are concerned.

- Is your credit card numbers in a file cabinet near your computer—where family members or business colleagues can get access? You might be surprised at how resourceful people can be.
- Is your password on a piece of paper stuck to your computer? Don't share your accounts and passwords. Use different passwords for each service, and change them regularly. Choose a strong password (one that has upper-

and lower-case letters and numbers or characters, and is not easy to guess), and then protect it.

- Afer you make a purchase online, do you leave your computer so your kids can use it? Your passwords are stored in your browser's cache for as long as that browser remains active. Quit your browser before you leave.
- Tempted to make a purchase from a computer at the library, a convention show floor, an Internet café, or another public terminal location? If you must use one of these for your access, think about using an off-line payment method.
- Did you remember to erase your financial information from your discarded computer? Reformat discarded hard drives to make sure sensitive or confidential information isn't compromised.

Seals, Privacy Programs, and Other "Guardians"

You may see privacy seals on some web sites. These seals are part of voluntarily programs used to validate a vendor's web site's policies and practices. These seals are intended to help ensure "consumer confidence." However, buyers are not always well protected by such policies due to a vendor's changing behavior or patterns. (Amazon.com is one example. They originally posted a privacy policy referring to their intent to keep customer information private. More recently, Amazon informed its customers that the policy had changed and they were no longer assuring customers that their information would remain private.)

These voluntary seal programs vary widely in their use and effectiveness. Some programs are new, while others may sound familiar. There are no significant punishments for violators. None of these programs is legally enforceable, and not all businesses displaying these seals are valid program participants.

Here are some guidelines for reviewing privacy policies, as suggested by the Online Privacy Alliance (OPA). The privacy policy should be clearly stated, be available on the page where the information is collected, and include the company's statements regarding disclosure, choice, and data security. Look for the following details:

- description of the information collected
- identification of possible third-party distribution of information to associates, agents, or contractors
- options available regarding information collection
- description of intended use of the information
- description of data storage security
- description of data integrity and access

- company contact information, including street address, email, and phone number
- consequences of refusal to provide requested information
- options regarding how information is to be used
- options for opting out of information use unrelated to the purpose for which it was collected
- opportunity to refuse third-party use of collected information
- assurance of appropriate measures to protect reliability
- assurance that third-parties, if involved, protect data
- an opportunity for customers to review and correct inaccuracies in their information

Three of the more widely-recognized programs are briefly discussed below.

BBBOnline Privacy Seal Program and the Children's Privacy Seal Program

The Better Business Bureau offers a program and web site seal (BBBOnline) that indicates vendors have established a privacy policy to protect consumer information in a way that meets the BBB's standards. This means that "businesses must include notification to consumers of how information is collected, used, and shared; provide adequate data security; provide opt-outs for third-party information transfers; provide reasonable access to information; and use encryption for the receipt and transfer of sensitive information."

Web sites and online services displaying a BBBOnline Privacy Seal have also committed to the BBBOnline dispute resolution process, and are subject to random independent audits of their information practices. Penalties for violators are minimal.

P3P

The Platform for Privacy Preferences Project (P3P) enables privacy practices to be retrieved automatically, interpreted easily, and responded to automatically, in a standard format, as part of your interactions with a web site. The focus is to automate decision-making and transfer of basic visitor information when appropriate. This approach is not yet widely adopted and lacks enforcement mechanisms.

TRUSTe

TRUSTe is a partnership and seal program that requires a web site to have a posted policy explaining its privacy practices. That policy "will openly share, at a minimum, what personal information is being gathered; how it will be used; with whom it will be shared; who is gathering the information; what options the user has; what security procedures are in place to prevent misuse or loss and how users can correct information to control its dissemination."

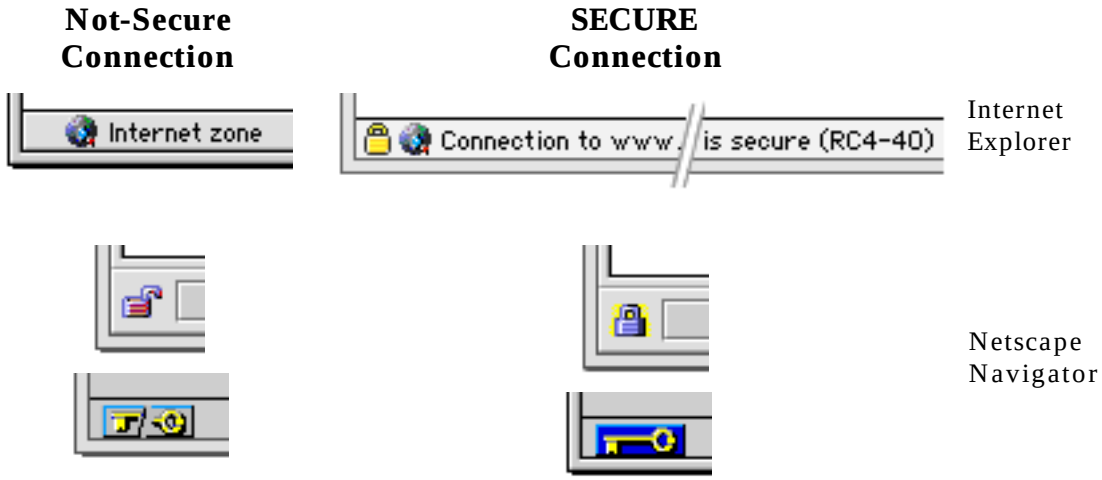
TRUSTe came out of efforts lead by the Electronic Frontier Foundation; it remains controversial. One reason: several TRUSTe members were found to violate their own privacy policies.

Finding and Using Secure Sites

Most of the information moving around the Internet is designed to be as widely read as possible. In order to protect private or sensitive information from wide dissemination, some form of encryption, or coding—like that used in a secure server—should be used.

Online ordering systems generally use a secure server, allowing your personal informaton to be encrypted as it moves across the Internet. However, the costs of setting up and maintaining a secure server are not trivial, and smaller vendors may offer other options. Some include using a third party's secure server (whose privacy policies may be different from your chosen vendor's); online ordering without the benefit of a secure server and encryption; or possibly offering an order form to be returned by fax or email. Remember that if you send credit card or personal information in a regular email message, it is not going to be secure. The level of security offered by any vendor is a matter for your consideration and trust. Don't order from any sites using methods that you don't trust. For more information on payment options, see the section on Paying Online.

Most web browsers have a little key or a lock in the lower left corner to indicate your browser's connection to a regular or secure server. See how your browser looks.



It's generally considered risky to type in any Personally Identifiable Information (PII), such as your credit card number or Social Security number, if the key or padlock is broken. If you aren't sure, call the merchant on the phone or make your purchase from another online store. Pay attention to all requests for personal information. Never share your password.

Here's a little more information about secure sites.

Secure Socket Layer

The Secure Socket Layer (SSL) creates a protected, encrypted connection between your home or work computer and your store's server. The URL (web address) of a secure site always begins with `https://` (you will need to type it in). The more common, but insecure, `http://` is assumed when you type a regular URL.

Public Key Encryption

SSL uses technology called public key encryption, one of the strongest safeguards available today. Encryption is a process by which plain text (what you type into the order form) is "scrambled" into a code that can't be read without a special key that unscrambles the code. Your vendor, if he offers a secure site for taking your orders, has this special private key.

Protecting Yourself from Internet Fraud

While the growing popularity of e-commerce has generated some brand new scams by con artists, you should also be watchful for the migration to the Internet of scams that have been around for many years. You should be alert to both the old and new varieties of fraud.

FTC's "Operation Top Ten Dot Cons"

Law enforcers from nine countries, five U.S. agencies, and 23 states are participating in a year-long effort targeting the top 10 Internet scams. These scams were culled from the FTC's database of more than 285,000 consumer complaints. The top 10 targeted scams were:

- Internet Auction Fraud
- Internet Service Provider Scams
- Internet Web Site Design/Promotions - Web Cramming
- Internet Information and Adult Services - Credit Card Cramming
- Multi-level Marketing/Pyramid Scams
- Business Opportunities and Work-At-Home Scams
- Investment Schemes and Get-Rich-Quick Scams
- Travel/Vacation Fraud
- Telephone/Pay-Per-Call Solicitation Frauds (including modem dialers and videotext)
- Health Care Frauds

Take action if one of these scams happens to you! The FTC and your ISP want to know and can help you if you are being subject to these fraudulent activities. If you find that your credit card has been involved in a scam, be sure to call and write to your credit card company right away, describing your experience.

SITES TO SEE:

http://www.ftc.gov/opa/2000/10/topten.htm

Internet Fraud Watch
http://www.fraud.org/ or call 1-800-876-7060.

Travel Scams

Although there are many wonderful travel deals available online, occasionally looking for a travel bargain online can introduce you to fraud. Travel scams are increasingly common in the form of pyramid schemes, vouchers sold through spam, online contests, and offers of frequent flier miles on auction sites. Some of the most common travel-related scams include:

- Selling a non-refundable, transferable ticket that the original buyer is unable to use. Often the high bidder sends a payment but receives nothing, or receives a useless or unschedulable travel voucher.
- Selling frequent flyer miles that are about to expire. The account award holder offers to buy a ticket to the highest bidder's destination of choice, but runs out of time.
- Offering entire travel packages sold at auction, being represented as part of a group package that was undersold.
- Selling travel vouchers as products of a pyramid scheme.
- Selling a discounted vacation package, which must be paid for by credit card, but cannot be scheduled before the voucher expires.

The best defense against fraud is knowledge and prevention. Here are some recommendations to help you identify and protect yourself against fraud.

- Deals are usually trustworthy if offered through reputable travel agents. Look at who is making the offer.
- Call the airlines to verify a claim before sending payment.
- Be wary if, while you're looking for travel offers, you see the same individual showing up with new deals.
- Understand the terms and conditions that apply to products or services being offered online, and if you don't understand, ask. Legitimate businesses will provide more information, but con artists won't.
- Don't be pressured into making a decision. High-pressure tactics are common with fraud.
- Don't judge an online business by the appearance of its web site. Online scams are increasing in part because it's so easy to set up and promote a web site.
- Remember that it's easy to disguise your identity in cyberspace. Don't assume that everyone who contacts you online is who he says he is.

Many Organizations and Laws Are On Your Side

The best defense against fraud is education. The Federal Trade Commission (FTC) recently published a report describing common scams and what law enforcement agencies are doing to combat Internet crime. The complete report is available for free on the FTC web site (see below). Copies can also be obtained by calling the FTC at 1-877-382-4357.

It's a good idea to know what sorts of problems should be reported to local law enforcement or regulatory agencies, and what sorts of problems you might be able to resolve in Small Claims Court.

The Federal Trade Commission (FTC) is empowered to investigate a company if it sees a pattern of possible violations. It's a good idea to file a complaint with the FTC if you are dissatisfied with the way an online merchant does business. The FTC's web site provides online complaint forms.

Some things about online shopping are unique to the Internet, but the rules that govern fair business practices still apply. People should promptly report any credit card abuse to the card-issuing bank in writing, by registered mail. It's also a good idea to know what sorts of problems should be reported to local law enforcement or regulatory agencies, and what sorts of problems you might be able to resolve in Small Claims Court. And if you are contemplating the sale or barter of items, don't forget that you are responsibly for complying with all applicable laws and regulations.

The following is a partial list of the rules and regulations that protect the public if the businesses are located in the United States. Buyers have more limited recourse for resolving complaints or problems with international orders.

- **The Federal Trade Commission Act** prohibits unfair or deceptive advertising in any medium.
- **The Franchise and Business Opportunity Rule** requires a detailed disclosure document prior to any commitment to purchase a franchise or business. This rule also prohibits multi-level marketing, commonly known as pyramid schemes.
- **The Truth in Lending Act** governs rules about the disclosure of finance charges.
- **The Fair Credit Billing Act** requires creditors to acknowledge billing complaints in writing and to investigate billing errors.
- **The Fair Credit Reporting Act** prohibits creditors from knowingly reporting false information to credit reporting agencies.
- **The Equal Credit Opportunity Act** governs electronic fund transfers.

SITES TO SEE:

`http://www.ftc.gov/`

The federal government's consumer protection portal
http://www.consumer.gov/Tech.htm

A comprehensive list of consumer rights enforced by federal agencies
http://www.consumer.gov/

We hope this guide has helped prepare you to be an educated online shopper. This guide is located online at: http://www.netaction.org/shoppers/

Copyright 1996-2000 by NetAction / The Tides Center. NetAction is a project of The Tides Center, a 501 (c)(3) organization. All rights reserved. This Online Buyer's Guide may be reposted or reproduced for non-commercial use provided NetAction is cited as the source.

Check It Out!

Now that you've read our Guide, are you ready to go shopping online? Here's a summary checklist of questions and circumstances to keep in mind. Answers to these questions will depend on your desires, situation, and comfort level.

Smart Online Buying Practices

- Are you familiar with this retailer?
- What do you know about the merchant's reputation and trustworthiness?
- Have you shopped with this retailer before, or received a recommendation from someone you know?
- Is the retailer in compliance with regulations enforced by your state’s consumer protection agency?
- Did you "click-through" on reputation logos, to test their authenticity?
- Did you check the privacy policy linked to any page requesting Personally Identifiable Information (PII)? Have you reviewed the site use policies, such as "Terms and Conditions" or "Terms of Use," or Rules and Regulations? (These may be hidden.)
- Is warranty and repair information posted? Have you checked for special offers, coupons, discounts, and rebates?
- Have you confirmed that there are no restrictions on sale or delivery to your location? Do you know how much it will cost for shipping and handling, taxes, rush delivery, or duties?
- How much are you able or willing to spend on a product or service? How much time do you have to research your options?
- Are you using the method of payment that is best for you? If you are using your credit card, are you doing so because it offers protection? If you are buying from an unknown merchant, are you using an escrow account to make sure you are satisfied with the product before paying? If there is no way to make a secure payment online, are you using an off-line payment method?
- Have you written down your account identification and password, then filed it in a safe place? Have you printed out records of your order, confirmation, vendor contact, return policy, and warranty?
- Have you taken precautions against fraud? Do you know where to get help and how to report fraud if it occurs?

Protecting Your Privacy

- Are you sure your password is secure on your computer?
- Have you chosen a unique password—one that has not been shared with anyone?
- Have you used separate passwords for every account, and are they filed somewhere off line?
- Did you remember to exit from your web browser after completing each transaction, to clear the password from your computer's cache?
- Does anyone else have access to your computer and online accounts?
- Is your credit card information kept in a safe place?
- Do you have a file of credit card numbers on your hard drive where others might find it?
- Are you careful not to keep your credit card bills near your computer?
- Did you confirm that the site is secure before submitting Personally Identifiable Information (PII)? (PII includes your Social Security number, place of birth, mother's maiden name, driver's license number, bank account information, or credit card number.)
- Did you look to make sure there is a symbol of a whole key or closed padlock on the page?
- Does the browser page include a statement that the page is secure?
- Does the URL start with this: "http**s**://"?
- Do you only provide PII when it is necessary for the transaction, and only provide PII that is absolutely necessary?