e-commerce SAFETY Guide

PayPal® ebay™

The e-Commerce Safety Guide

About the Author

Robert Chesnut is one of the world's most respected authorities on Internet fraud and high-tech crimes.

As Vice President of Trust and Safety for eBay and with strategic responsibility for all protection programs for PayPal, Rob created and leads eBay's Rules, Trust and Safety Department, which is responsible for the formation and coordination of eBay's trust and safety strategy worldwide.

Chesnut has been a member of eBay's legal team since 1999, coordinating the company's relationship with state and federal law enforcement agencies and devising policies to inform eBay users of laws that ban or regulate the sale of certain merchandise and services. He also works with law enforcement to investigate allegations relating to eBay and PayPal users who may be engaged in fraud or the sale of stolen property.

Prior to joining eBay, Chesnut worked as a federal prosecutor with the United States Attorney's Office for the Eastern District of Virginia for 11 years. He served as the chief of that office's major crimes unit for five years and handled several noteworthy espionage cases. He is a graduate of the University of Virginia and Harvard Law School.

Why Shop Online?

Few developments have altered America's lifestyle more quickly and more completely than the Internet. Online access has enabled people from all walks of life to bring entire libraries, entertainment venues, post offices and financial centers to a workplace, to a desktop or to a shirt pocket. The Internet's largest and most meaningful impact may very well be on the way consumers shop for everything from gifts, gadgets and groceries to clothing, cars, and cruises.

The ease and selection that the Internet provides to shoppers has changed the face of retailing. More and more, consumers visit a store's Web site to make their choices before traveling to the store itself; and in a rapidly swelling tide, many shoppers are bypassing the store altogether and ordering online directly from the Web sites of their favorite brands and outlets. Companies like Sephora, Sears and Crate & Barrel have increased the range and quantity of products available at their online stores and are sending online coupons and sale announcements via e-mail directly to their customers.

Because online stores are open 24 hours a day, seven days a week, and their inventories are often more complete than those of their brick-and-mortar counterparts, the Internet makes it easy for shoppers to compare products within or between stores, to read product reviews from other customers, to access vendor return policies and to find warranty information.

A recent study of the marketplace by Nielsen//Net Ratings found more than 200 million Americans (or 75%) are using the Internet. Those who shopped online in 2003 spent $17.2 billion online in just the fourth quarter alone. Research firms anticipate that, in 2004, the number of online shoppers will increase by 14 percent, representing 30 percent of the U.S. population. In four more years, half the country's population will be purchasing online.

Research firms anticipate that, in 2004, the number of online shoppers will increase by 14 percent, representing 30 percent of the U.S. population.

Americans' Concerns About Safe Shopping

Increasingly, American consumers are expecting merchants – from major department stores to individuals who sell handcrafted jewelry to electronics and cars – to make their products easily available on the Web. They're also expecting these online retailers to make payments a simple and secure process. While consumers have confidence in online stores, recent research suggests their confidence levels in the security of the actual purchases from these stores, especially from lesser-known or unknown sellers, lag behind their desire to engage in shopping over the Internet.

An April 2004 survey by AC Nielsen found that news stories about identity theft and fraud have confused many consumers about how to shop safely online. The survey revealed the top security concerns of American online shoppers, which are:

- Not receiving the items purchased, or receiving items that are substantially different from their descriptions on the Web site
- E-mail addresses sold to third parties
- Fears about personal or financial information being stolen
- E-mail scams known as "phishing" or "spoofing" that result in messages being sent to consumers from disreputable sources that are disguised as messages from trusted retailers or financial institutions.

In fact, online transactions can be as secure, if not more secure than payments made by mail or in a store; and fraud can be avoided if consumers understand a few simple steps they should take when they enter the online marketplace.

Avoiding Fraud: Shopping Safely Online

Online fraud can take many forms from non-delivery of goods to non-return of damaged goods. In many cases, online fraud can be deterred by following a few simple practices.

Just as consumers should take obvious measures to protect themselves in brick-and-mortar stores – not leaving a purse in an unguarded shopping cart, protecting their PIN (personal identification number) at checkout, not carrying large amounts of cash in their wallets – online shoppers should consider sensible precautions, as well.

1. **Learn as much as possible about the product and seller:** Shoppers will feel more secure and confident if they are familiar with the merchants from whom they're buying. The Internet offers the platform for retailers to provide information about their companies and histories while the buyers are empowered to do their research about the products and companies. Shoppers might also learn about a retailer from its reputation, from previous purchases, from referrals through friends or from reviews and comments by other shoppers found online.
2. **Understand the retailers' refund policies:** Look for and ask about what the refund policies are. Questions to ask include: the required timeframe a buyer must contact the retailers and return the items, if a full refund will be offered or a merchandise credit, and if an item that has been opened can be returned. For retailers without refund policies, consumers can use buyer protection programs from either the site or through the payment method. This ensures that if there is a problem with a transaction, the payment will be covered or refunded as a result of the protection guarantee.
3. **Choose a secure password to protect account information:** Many people use passwords for online stores that could be guessed, like their birthday, Social Security Number or a family member's name. Instead, a password should contain a combination of upper and lower case letters and numbers and symbols that no one else will know.

Just as consumers should take obvious measures to protect themselves in actual stores, online shoppers can consider sensible precautions, as well.

4. **Use a secure checkout and payment process:** Many Web sites use a technology called Secure Sockets Layer (SSL) to encrypt the personal and financial information sent over the Internet. To know if the retailer is offering a safe checkout process, look for the logos from companies like VeriSign or TrustE logo. A browser will also display the icon of a locked padlock at the bottom of the screen to indicate encryption.

   When it comes to choosing which method to use when paying online, consumers should take precautions when entering credit card or checking account information at each online retailer they visit. By entering this on several different merchant Web sites, the likelihood of this information being compromised increases. A safe and easy-to-use payment service allows shoppers to enter account information only once at a highly secure and reputable site that protects this financial information from merchants and other intruders. Future purchases should be made from that one account to avoid the need to enter credit card information separately into the Web sites of individual retailers.

5. **If an offer sounds highly suspicious or too good to be true, it probably is:** As with any purchase, shoppers should read the fine print (or, in some instances, click the links describing the purchase agreement). While Internet shops frequently offer lower prices than brick-and-mortar stores, shoppers should be wary of unreasonably low bargain prices or unusually attractive promises.

What To Do If Fraud Has Occurred

First and foremost a buyer should contact the retailer from which the product was purchased. If agreement can't be reached, the consumer should contact either the payment method or service used to dispute charges and finally contact a law enforcement official to report the incident.

Deterring Identity Theft

Identity theft is a crime that affects consumers at home, at work, in the shopping mall or online. The Federal Trade Commission (FTC) defines identity theft as the stealing of personal information to illegally obtain credit or medical care or to hide from the law.

In just the past five years, according to the FTC, an estimated 27.3 million Americans have become its victims. In 2002 alone, the identities of 10 million U.S. residents were stolen, with $5 billion in losses to the victims, and nearly ten times that amount, $47 million, lost by businesses. A study by research firm Gartner reported that 7 million U.S. adults, or 3.4 percent of U.S. consumers, were victims of identity theft during the 12 months ending in May 2003.*

Contrary to popular belief, identity theft is not simply an Internet problem. Research shows that a large amount of identity theft actually occurs in the offline world when a thief obtains an individual's personal financial information through the mail or their discarded trash.

"Identity theft is not necessarily a high-tech crime," says Avivah Litan, vice president of research for Gartner. "It can just as easily damage the credit reputations of low-tech adults who don't spend any time on the Internet."**

Analysis of identity theft cases indicates that this crime could be reduced substantially by shopping and paying bills online instead of paying through the mail. Javelin Strategy and Research, a research firm covering the payments industry, conducted a thorough examination of identity crimes and found that consumers, billers and financial institutions could reduce their risk by 10.4 percent when they move their at-risk activities to the Internet.

By shopping and paying bills online, consumers are more apt to review their account information and the accuracy of each of the transactions they make. Online bill payment also reduces the risk of a paper trail from receiving paper statements or sending paper checks. Automatic payroll, Social Security and other recurring deposits can also benefit consumers by avoiding the risk of having checks stolen from mailboxes.

Javelin projects that if all Americans tomorrow began using the electronic banking and bill payment services now available on the Internet, the amount of identity fraud prevented during the next year would total $2.37 billion. Another $2.5 billion would be saved over the same period because consumers can more rapidly detect fraudulent use of their bank and credit card accounts when they monitor them regularly online.

*Underreporting of Identity Theft Rewards the Thieves, Avivah Litan, Gartner, July 7, 2003.

**Millions Victimized in 2002 as Identity Theft Keeps Growing, Don Spatz, Reading Eagle, February 1, 2004.

How Personal Information is Found

A person's name and Social Security number is all it takes for identity theft to occur.

That information allows a scammer to access existing bank and credit card accounts and can enable him to open new credit accounts that will be charged to the victim. Consider the following simple ways personal information can be lifted:

- Trash that contains discarded mail or paperwork with account information
- A wallet that contains Social Security information
- Mail that contains account numbers
- A forged Postal Service change-of-address form to divert someone's mail to another location
- Obtaining a person's credit report by posing as a landlord
- Through e-mail or a Web site, pretending to be a legitimate company or agency with which people do business
- Stealing business records by finding information at a person's place of work or removing files from an office
- By anyone who handles credit cards outside of the presence of the card holders, for example at hotel or restaurant
- Robbing from a friend, neighbor or family member, where access to the few pieces of paper required to steal an identity may be comparatively simple

ID thieves often develop creative ways to draw unsuspecting victims into providing the information they need to steal their identities. Seemingly innocuous incidents may be staged simply to gain access to personal financial information. Some people have been targeted by signing up for a raffle or by completing a survey at a mall, where they are asked to provide their Social Security numbers or other information the thief can use.

Identity theft perpetrators steal an average of $2,100 from each existing account they access, often needing only a credit card number. But they take an average $10,200 from each new account they open with the stolen information.

How Consumers Should Use Their Social Security Numbers

The Social Security number is perhaps the most common identifier for record keeping in America. Since Social Security numbers are the primary way that many financial institutions and other organizations verify identities, people should make exceptional efforts to guard their number and use them properly. Situations where someone will be required by law to reveal a Social Security number are actually very limited. For example:

- It is required when starting a new job, because employers must confirm the Social Security number for reporting earnings
- It is necessary when applying for a loan or opening a bank account, because the Social Security number must be entered into the financial or lending institution's accounting system

Misusing a person's Social Security number is a violation of Federal law that can lead to fines and/or imprisonment. This threat often is not enough to deter an identity theft criminal, however, so people should keep their Social Security number safe and use it carefully.

More information on the proper use of Social Security numbers is available at the Social Security Administration's Web site, www.ssa.gov.

Case File #1

Stolen credit card purchases ring up to $3,500

Roz Cohen – a New Jersey-based freelance writer – considers herself to be a savvy Internet user and knowledgeable about privacy rules. She never gives out personal information over the phone and even once refused to give out her Social Security number to a doctor, finally allowing its use when the insurance company wouldn't pay her bill.

She had no idea there was a problem until a retailer called asking if she had purchased a pair of expensive boots she had never heard of. The company called indicating it had "red flagged" the order as suspicious based on the shipping information. Her credit card information had been stolen.

Upon further investigation, Cohen found the criminal had quickly racked up $3,500 in credit card charges on her account. It took her more than a year to straighten out her credit information, but today, Cohen still has no idea how her credit card account number was stolen.

Cohen was also a victim of fraudsters on eBay, where she is an avid seller. Unbeknownst to her, someone had taken over her screen name on the site and begun selling items under her ID. The unknown person changed her password in an effort to use Cohen's good feedback rating to commit fraud.

"Not only was it disconcerting due to the inconvenience but it was a true violation of my privacy," she said. "I was scared and felt violated and angry. Someone got something of mine and I had no idea."

As eBay monitors activity on the site for suspicious activity, customer service had already identified the fraudulent activity Cohen's account before she realized the problem. When she contacted eBay, Cohen was told her account had been "red flagged" due to unusual activity and the issue was resolved in only a few days.

Preventing Identity Theft

Combining common-sense with the resources available through the Internet and other electronic systems can lower the occurrence of identity theft.

Consumers should review their credit card and bank statements regularly to look for fraudulent charges or withdrawals. Many times people don't know they've been victimized until months after the stolen information is first used.

Department of Treasury's Electronic Fund Transfer Act – also known as RegE – protects consumers from unauthorized transactions. If a victim reports a problem involving an electronic funds transfer within two days of discovering its occurrence, they are liable only for the first $50 of the transfer. Otherwise, they are liable for up to $500 if they report the problem within 60 days of discovering the occurrence of fraud.

To help prevent identity fraud before it occurs, consumers should follow these recommended practices:

- Do not carry Social Security cards in a wallet or purse, but instead locked in a safe location until the rare times when the owner will need access to it
- Carry only those credit cards and checkbooks (and associated account numbers) that are needed on a regular basis
- Never carry PINs or passwords in a wallet along with the cards they activate
- Read and understand their credit reports
- Close accounts that they are not using or that they don't need
- Remove and photocopy all the contents of their wallets and keep the copies locked in a secure place
- Sign a new or renewed credit cards immediately
- Avoid printing driver's license numbers on personal checks

To help prevent identity fraud before it occurs, consumers should follow these recommended practices.

Individuals can take other precautions as well that, in large part, will deter identity theft. They should:

- Refuse to give personal financial information to solicitors who phone
- Instead of throwing out such potentially sensitive information as unneeded tax records, old checks and statements, obtain a shredder and destroy these documents
- Gather mail every day and never leave it in the mailbox overnight
- Check telephone statements for calls not made
- Never reply to e-mails that ask for personal information
- Don't download e-mail attachments that are sent from someone you do not know
- Order a credit report every year and review it to ensure it is accurate
- Switch to electronic statements and checks for banking and credit card accounts. These can be viewed anytime of day or night to monitor against fraudulent use and eliminate paper statements that contain account numbers.

What Consumers Should Do When They Become Identity Theft Victims

Restoring a person's accounts and credit reports once he or she becomes a victim of identity theft can be an extremely frustrating and time-consuming process. The non-profit Identity Theft Resource Center estimates that the average victim spends 600 hours over several months to a year resolving the issues that derive identity theft.

An identity theft victim should contact a number of organizations that have an impact on credit ratings and security, including creditors and lien holders. The Federal Trade Commission offers an Affidavit of Identity Theft that can be notarized and then sent to creditors and agencies.

Early contact should be made with the three major credit reporting bureaus:

Equifax
www.equifax.com
Report fraud:
1-800-525-6285
Order a credit report:
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
www.experian.com
Report fraud:
1-888-397-3742
Order a credit report:
1-888-397-3742
P.O. Box 1017
Allen, TX 75013-0949

TransUnion
www.tuc.com
Report fraud:
1-800-680-7289
Order a credit report:
1-800-916-8800
Fraud Victim
Assistance Department
P.O. Box 6790
Fullerton, CA 92834

If fraudulent charges are discovered, the victim should call their local Consumer Credit Counseling Service at 800-388-2227 (or locate a regional bureau at www.nfcc.org) for assistance in clearing false claims from his or her credit report.

In cases where bank accounts have been opened fraudulently in a person's name, that individual should call a check guarantee company like Telecheck, at 800-366-2425 or online at www.telecheck.com. These companies can flag the file so that the counterfeit checks will be refused.

- Telecheck, at 800-366-2425
- International Check Services, at 800-526-5380

These companies can flag the file so that the counterfeit checks will be refused.

Targets of identity theft should keep detailed logs of all correspondence relating to attempts to report and correct the fraudulent activity. They should track the money they spent in the process including postage; phone calls; and fees from notary publics, accountants and attorneys. Keeping track of these expenses helps if the case is ever prosecuted and a victim is seeking restitution or to assist in closing fraudulent accounts opened.

Where identity theft involves the mail, victims should contact the U.S. Postal Service to report a mail fraud claim at www.usps.com. Other agencies that should be notified are:

- The Department of Motor Vehicles (varies by state)
- The Social Security Administration: www.ssa.gov
- The FBI: www.fbi.gov
- The Federal Trade Commission: www.ftc.gov

Case Study #2

Timely warning allows potential victim to escape phish hook

Working from home for a major food distributor, Lisa Cook wakes up each day and immediately checks both her work and personal e-mail. In January 2004, Cook woke up to find a message in her personal e-mail box, seemingly from PayPal. The e-mail asked her to follow a link to update her account information threatening her recent transactions would not go through unless she updated immediately. Having recently bought some items off of eBay, she quickly clicked on the link and updated her account information on a site she believed to be PayPal.

She next checked her work e-mail and saw a message from her company warning employees of spoof e-mails from phishers. Cook immediately called PayPal customer service and told them what had just happened to her. In less than five seconds, the customer service representative confirmed that Cook had been a victim of phishers. PayPal's customer service immediately changed her password and recommended some additional steps she should take for protecting herself, the first being to call her credit card company. Lisa Cook had caught on to the fraud and stopped it from causing any potential danger to her accounts in only one hour.

Phishing and Spoofing

Some thieves on the Internet simply go fishing, or "phishing" or "spoofing," as the practice has come to be known. The "ph" is a common substitute for the letter "f" among Internet hackers, and phishing is an attempt by scammers to troll the sea of online consumers in hopes of netting unsuspecting victims.

Identity thieves send massive numbers of e-mails to Internet users that ask them to update the account information for their banks, credit cards or online payment service or popular shopping sites. The e-mail may assert that the recipient's account information has expired, been compromised or lost and that the account holder needs to immediately resend it to the company.

Sometimes this fraudulent e-mail appears to have been sent from the domain of a legitimate bank, insurance agency, retailer or credit card company. In fact, the fraudster's identity has been hidden behind these credible sources, in a practice called "spoofing," which goes hand in hand with phishing. In recent months, scam artists have used spoofing or phishing for customers of such organizations as Citibank, Best Buy, EarthLink, eBay, PayPal and even the Federal Deposit Insurance Corporation.

Such phishing expeditions often include e-mails with official-looking links to a Web page. Other times, e-mails ask the recipient to download and submit an electronic form. While these links and forms may appear to be directed to a legitimate business site, they actually take personal information to a site created by the phishing thief.

These messages, forms and Web pages all have only one purpose: to persuade the recipient to divulge personal authentication data, such as account user names and passwords, credit card numbers and Social Security numbers. These e-mails look "official" and, as a result, as many as five percent of recipients respond to them, becoming victims of financial loss, identity theft and other crimes.

The U.S.-based Anti-Phishing Working Group estimates that, in just a two-week period in December 2003, more than 90 phishing attacks hurled more than 60 million fraudulent e-mail messages into the Internet sea; and five percent of the recipients, or 3 million people, took the bait. No one knows how many of these scams have been perpetrated on consumers, nor the total cost; but industry experts believe hundreds of millions of people have been targeted. The con artist makes a killing if even a small fraction of the recipients respond.

Identifying Fraudulent E-mails

It is incredibly difficult to detect fraudulent emails – as spoofers have become increasingly sophisticated in their attacks. There are certain characteristics Internet users should look for, though, that are common to many spoof e-mails:

- **Personal information requests:** An indicator of spoof e-mail is a request for the recipient to enter such sensitive personal information as a user ID, password or bank account number by clicking on a link or completing an e-mail form.
- **Sender's address:** E-mail recipients should not rely on the sender's e-mail address to validate the true origin of the e-mail. While it may look legitimate, the "From" field be altered easily.
- **Greeting:** Many spoof e-mails begin with a general greeting like, "Welcome User," rather than being directed to a specific person.
- **Threats to accounts:** Some spoof e-mails declare that the recipient's account is in jeopardy and that authenticating information is required to keep the account from being closed, suspended or restricted.
- **Lost information:** Consumers should be wary of claims that a company is updating its files or accounts. Companies like PayPal, eBay and other organizations with an established Internet presence and strong security measures are not likely to lose account information.
- **Links:** Links that look like they connect to a particular site may have been forged. Always open up a new browser window and manually type in the Web site address.

It is incredibly difficult to detect fraudulent e-mails – there are certain characteristics Internet users should look for, though, that are common to many spoof e-mails.

Preventing Spoof

Individuals can take specific steps to help avoid falling prey to a spoof attack:

- Be extremely skeptical of e-mail received from someone they don't know
- Keep separate passwords for each online account so that, if one is stolen, it will not provide access to the others
- Do not click on a link embedded within any potentially suspicious e-mail. By starting a new Internet session from the beginning and typing in the link's URL into the address bar and pressing "enter" users can be sure they will be directed to a legitimate Web site.
- Call a financial institution to verify the account status before divulging information purportedly needed to keep their account out of jeopardy. Most legitimate financial companies will not send an e-mail threatening the status of an account and requiring the user to submit information immediately.
- Do not respond to any request for financial information that comes to you via e-mail
- Update anti-virus software weekly to help ward off e-mail-borne viruses that can find and transmit information from files
- Work from the most current versions of browsers and operating systems can also prevent many possible attacks
- Check online accounts regularly
- Install and run firewalls

Individuals can take specific steps to help avoid falling prey to a spoof attack.

Companies That Offer Safe Online Shopping Protections

PayPal

Many of the potential concerns that surround the safety of online shopping have been resolved by online payment services. The premier service of this type is PayPal, which has set the benchmarks for secure Internet transactions and ease of use.

When purchasing something using PayPal, users simply carry out the transaction through their PayPal accounts, rather than a credit card. PayPal then charges each purchase to the individual's credit card or checking account. Because all PayPal transactions are based on the user's e-mail address, merchants never have access to the user's account information. This method is safer, more secure and more convenient than providing financial information to multiple sites of individual sellers.

Online shoppers who pay each site directly to order products or services must submit their credit cards or bank accounts for each transaction. This crucial data is then stored by each individual retailer. With multiple merchants and servers maintaining this information, the likelihood of a breach of this information also increases significantly. PayPal allows online shoppers to set up a single account that can be used to purchase from millions of merchants around the world. Those who enroll with PayPal need only provide their account information once; and then it is stored on a secure, highly encrypted server.

PayPal supplies additional guarantees, as well, including PayPal Buyer Protection which provides coverage against fraud of up to $500 on qualified eBay transactions. When PayPal users are victims of spoof, the company offers a complete refund to qualified account holders. Its dedicated team of investigators works directly with victims of theft and law enforcement to locate and prosecute criminals, anywhere in the world. PayPal also offers fraud prevention tips and safe shopping guidelines for both buyers and sellers at its online Security Center, accessible at https://www.paypal.com/security.

PayPal makes the riskiest part of transactions safer, without compromising speed or efficiency. In addition PayPal is a foremost resource for assurance online, a safety service that makes it easier to shop with confidence and to establish mutual trust between buyer and seller. eBay's marketplace of 95 million people overwhelmingly choose PayPal as a preferred payment option.

eBay

As the world's online marketplace, eBay is especially well equipped to provide a safe, secure and trustworthy shopping environment. The eBay Security Center at www.ebay.com/securitycenter is a single source for direct information about safe shopping in the eBay marketplace.

eBay's Feedback Profile lets members of the eBay community comment on their transaction experience, so that both buyers and sellers can check an individual's history before engaging in a transaction.

Additional security comes in the form of the PayPal Buyer Protection program that provides coverage against fraud of up to $500 on qualified eBay transactions. This program protects buyers against non-delivered items as well as items that are significantly different from their descriptions. Sellers who qualify to offer PayPal Buyer Protection must have at least 50 feedback rating that is 98 percent positive. For transactions that do not qualify for PayPal Buyer Protection, eBay users are covered by its standard buyer protection feature of $200 coverage with $25 service fee.

The eBay Account Toolbar, helps combat Internet fraud as well. Designed to allow eBay users to track items on which they bid, the toolbar also helps recognize, reject and report potential spoof sites. Icons indicate if the user is on a verified eBay or PayPal site or whether the site might be fraudulent. Users can report suspicious sites by clicking the Account Guard icon on the toolbar. And, finally, eBay password protection warns users if they are entering their eBay password into an unverified site and will block it from being submitted unless the user provides confirmation to override the block.

Case Study #3

e-Commerce offers great deals, wide variety

Gregg Hensler, an independent contractor in Indiana, discovered that by using the Internet, he could find better price and selection than from local retailers.

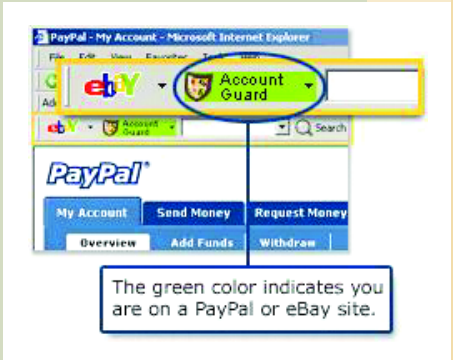
When a friend sent him to eBay in 1998, he purchased a Bobcat skid loader for his business and saved $4,000. He says he prefers the Internet and sites like eBay because it gives him more options when making large purchases.

"Because of the savings I've found on eBay, I've definitely been able to put more money back into my business than if I had bought the equipment new," said Hensler of his online shopping experience.

8 Reasons To Feel Safe Buying on eBay

With nearly 95 million registered users listing more than 2 million new items a day, eBay is the safest shopping marketplace on the Internet.

1. eBay's Security Center at www.ebay.com/securitycenter is a source for direct information about safety and security when using eBay.
2. eBay Feedback gives a buyer information about the seller's overall rating from previous buyers and their comments.
3. Buyers can use PayPal, the safe, secure way to pay online. Currently PayPal has 40 million member accounts worldwide, and it is available in 38 countries.
4. PayPal Buyer Protection offers up to $500 of coverage against fraud for items not received or items substantially different from their descriptions. Qualified sellers display the PayPal Buyer Protection symbol. eBay users are covered by its standard buyer protection feature of $200 coverage with $25 service fee.
5. In committing significant human, technical and financial resources to safe shopping, eBay employs hundreds of people in its Trust & Safety Department, including former federal prosecutors, and sophisticated fraud-detection systems.
6. Shoppers have access to educational resources at eBay. The eBay Learning Center at http://pages.ebay.com/education offers online tutorials on how to buy and sell safely on eBay, and eBay University at www.ebay.com/university offers classes. Additionally, many product categories have buying guides to alert visitors to special areas of consideration.
7. The Account Guard feature on the free eBay Toolbar helps protect users from spoof sites and enables visitors to report such sites.
8. eBay users can e-mail the seller before bidding or sending payment by using the "Ask the Seller a Question" link. This capability offers increased confidence for buyers who want to verify a name, city or phone number before paying.



Ways To Keep Online Accounts Safe

- Using electronic transactions in lieu of paying via mail or receiving paper statements, helps to prevent identity theft by removing private information from potential perpetrators
  - This also gives the account holder increased awareness and control of their accounts by understanding recent transactions
- Always access your account by opening a new browser and typing in the entire URL, for example: https://www.paypal.com
- If an Internet user receives a suspicious e-mail that appears to come from PayPal or eBay, the following information should never be shared:
  - First name, last name, business name
  - E-mail and password combination
  - Credit card, bank account and PIN
  - Social Security and driver's license numbers
- Send any suspicious e-mails allegedly from PayPal to spoof@paypal.com and those allegedly from eBay to spoof@eBay.com
- If eBay or PayPal require information from a user, it will send an e-mail notification requesting that the information be entered only after the user has safely logged on to the site
- Users should not download attachments, software updates or applications via an e-mail link. Neither PayPal nor eBay will ask members to download anything
- Select a unique password and change it every 30 days
- Maintain the most current versions of anti-virus software, browsers and operating systems to ward off e-mail or Web-based viruses that can find and transmit information from files

To continue to shop safely online, Internet users can benefit greatly from buying at sites that have excellent anti-fraud systems, protection programs, accessing an online payment service, keeping passwords secure and using their accounts wisely.

Conclusion

Today's online shoppers have become very smart consumers very quickly. The Internet empowers people to easily compare products, prices and delivery options which has made shopping more enjoyable, less expensive and less time consuming. Now Internet users are becoming increasingly savvy about protecting their identities and their purchases when shopping by taking advantage of sites and systems to which they can turn to online. Pursuing wise choices when corresponding and making purchases online will help ensure that consumers and their resources remain secure and that confidence in all the benefits the Internet can bring to daily living will continue to expand.

Recommended Resources:

The following are online resources recommended for information about online fraud and prevention:

Identity Theft Resource Center
San Diego, Calif.
www.idtheftcenter.org

Anti-Phishing Working Group
www.anti-phishing.org

PayPal Security Center
www.paypal.com/security

eBay Security Center
www.ebay.com/securitycenter

U.S. Postal Service
www.usps.com

Federal Trade Commission ID theft resource page
www.consumer.gov/idtheft/