



Practicing Safe E-Commerce

By Pam Baker
E-Commerce Times
02/23/08 1:30 AM PT

<http://www.ecommercetimes.com/story/61755.html?welcome=1210695634>

If you're headed to a brick-and-mortar store or a restaurant, don't leave a receipt on the table, and be sure to check your credit card bill to make sure the staff didn't heist your credit card number. Those are common-sense behaviors for real-world commerce, but similar security measures are in order when shopping online.

Despite the overwhelming success of e-commerce, there are still consumers out there too terrified to click their cart through a virtual checkout.

Are they just a silly-nilly group, nutty as a bunch of conspiracy theorists? Or are the rest of us just too naive to get it?

Neither, it turns out.


"There are as many ways to hack the physical store -- probably even more -- as there are to hack an online store," Marc Aniballi, Board Advisor at Filemobile.com, told the E-Commerce Times. "Life is risky -- get over it. But protect your interests and limit your impacts."

Defining the Risk in Brick

There are those that swear that shopping online is safe, and those that promise you're only safe inside brick-and-mortar stores founded solidly on terra firma. As usual, the truth, is a bit smudgier than that clearly drawn line.

"If you are shopping or even passing through certain areas in southern California, it is definitely a possibility that you will be shot or robbed. You may get robbed online but not shot. So the answer depends on where you are as to which is safest," Michael Gardner, life coach at The Experience Training, told the E-Commerce Times.

Those who deal in the world of gray where safety is not a black-and-white issue say hackers can sometimes make their way through actual walls as easily as firewalls.

"In reality, it might actually be more risky to pay by credit card at your local mall than online. Many brick-and-mortar retailers are simply not well protected against today's hackers," Tom Bowers, senior security evangelist at Kaspersky Lab, told the E-Commerce Times. "Identity thieves can squat outside of physical stores and steal personal credit card data off of unencrypted wireless  transactions, and the infamous TJX breach largely involved information stolen from brick-and-mortar Marshalls stores in Miami."

The Risk Between

In the end, it may not matter whether you shopped online or off. The middle guy might be the biggest threat.

"The worst problem for consumers may be externally stored repositories of their personal information. This information still belongs to you but is out of your hands to review or protect," warned Bowers.

Basically, whether you're shopping safely at all depends on one thing: "You have to trust that the companies involved will take reasonable actions to protect your information," said Bowers.

Wrong Size, Right Color

Although there certainly are risks associated with buying online -- or anywhere, for that matter -- the fear may not be as real or as large as has been reported.

"In most of the consumer research done by NearbyNow, we have found that consumers say 'security concerns' for not buying online, but the real reason is they don't trust that they will get a fully functional product on time," NearbyNow CEO Scott Dunlap told the E-Commerce Times.

Even that problem, though, isn't so clear-cut.

"Buying the wrong product is only a consideration where actually eyeballing it is an issue," Patrick Allen, a government manager in Oregon, told the E-Commerce Times. "If I'm buying a book, there's no safety difference between Powell's online and its brick-and-mortar store."

A Lock on Online

If you're headed to a brick-and-mortar store or a restaurant, drive safely, lock your doors, and don't dawdle in the parking lot. Don't leave a receipt on the table, and be sure to check your credit card bill to make sure the staff didn't heist your credit card number.

Those are common-sense behaviors for real-world commerce, but similar security measures are in order when shopping online.

"Credit cards have similar risks in both situations. You are trusting the store clerk much like trusting a Web site SSL (secure sockets layer) certificate. Neither assures you that the person or system is trustworthy, only who they represent -- and they really don't even do that well," Doug Salah told the E-Commerce Times. Salah is an information system security architect for a technology-based products and services company serving the rail and transit industry.

"Once the process button is selected or your card is swiped, you have very little assurance that the information is secure or even going where you think it may be," he added. "The Internet 🌐 site has better availability to bad guys, but the store clerk, their support guys, and a slew of other people have access to the local system and could be capable of stealing your information."

At least reputable online stores have tightened security quite a bit in recent years.

"With actively enforced PCI (payment card industry) data security standards, shopping online has become even safer in many respects," Chuck Mooney III, director of strategic business development at First American Payment Systems, a Texas-based credit card processor, told the E-Commerce Times.

Online Crime Stoppers

Even so, consumers need to protect themselves and not rely too heavily on store Web site protection. What, exactly, can one do to protect oneself?

"Be wary of sites that ask for too much information. Do you really need a Social Security Number to buy a diamond ring? If it doesn't make sense, don't enter it," advised Dunlap.

"The most nervous consumers read everything -- including the fine print -- to make sure their data will not be shared with third parties in any way. If it might, they will call or fax in the order instead," he added.

Then there are the usual precautions:

- Never use the Internet via an unsecured wireless connection.
- Password-protect your wireless access at home.
- Use an up-to-date antivirus product and install Internet browser security patches to keep out data-stealing Trojans and spyware.

- When entering sensitive data, make sure you're on a Web site that's been secured by the retailer. Look for icons noting that the retailer has taken steps to ensure a safe connection for transmitting information or logos, such as that of the Better Business Bureau.

For those who want to go even further to protect their information while shopping online, there are a few extra steps to take.

"Cautious consumers can invest in products in the identity protection market, with vendors such as [LoudSiren](#) and [LifeLock](#) allowing consumers to add layered identity security for a monthly fee," said Bowers. "Consumers can also use a more roundabout way of paying by going through payment systems such as PayPal to avoid typing in credit information directly on the retail Web site."

Now, if you can just remember to shred those credit card bills when they come in the mail -- maybe, just maybe, your shopping experience will be risk-free. **ECT**