

# Ho, ho, holy cow! I've been scammed!

By Bill Brooks  
Coeur d'Alene Press

[cdapress.com /local\\_news/20171120/ho\\_ho\\_holy\\_cow\\_ive\\_been\\_scammed](http://cdapress.com/local_news/20171120/ho_ho_holy_cow_ive_been_scammed)

What does this time of year mean to you? Snow? Maybe. Colder temps? Maybe. Turkey? Of course! Gift giving? YES! Scammers and crooks? Without a doubt!

Holiday gift buying brings out these bad guys like sugar attracts ants and cockroaches. Online shopping is SO easy. You can jump on your computer, peruse thousands of products and compare consumer reviews, shipping costs and return policies. How wonderful!

The problem is you'd better be VERY careful that you're on the website you think you're on, otherwise you're likely to get scammed — BIG TIME!

One of the biggest ruses out there is to send out emails to millions that mimic well-known websites like Amazon. The email often offers fantastic deals and prices to you, "their best and most loyal customers." How about a brand name, spanking new 4K, 65-inch TV for \$999 instead of the normal price of \$1,999? That's a thousand dollars savings! In the smaller, but readable type, it warns you that "this item is being offered nationwide and there are only 200 units available."

Quick, you'd better jump on this! Whip out that plastic; enter your information (including your card number, expiration date and pin code). The website promises the TV will be delivered within three days to your address.

On the third day — no TV. You call Amazon. They search their records and can't find any such order. YOU'VE JUST BEEN SCAMMED!

The email from "Amazon" offering this unbelievable deal was not sent by the real Amazon, in fact it was sent by a website mimicking Amazon's website, right down to the smallest detail. The fact is that the website was housed in a temporary server in some country bordering Uzbekistan. By the time you figure out you've been had, the website has been shut down and your money is gone. If you used your credit card and put the charge "In Contest" you will likely get your money back. (Sorry NO TV!)

REMEMBER — Use a credit card, NOT a debit card, for all online purchases. Credit cards offer you protections that debit cards DO NOT. If you're in doubt as to what kind of card you have, look at it. Debit cards say "Debit Card" on the card.

ANOTHER HOLIDAY SCAM: You get a frantic email from your bank (but it's NOT really your bank). It warns you that the bank has detected "suspicious activity" on your card and in order to protect you and your ability to continue to use your card (especially during this busy holiday season), you need to click on the link provided and confirm your personal information, including Social Security number, credit card number, expiration date, pin number and address. Unless you take action within 8 hours, your credit card will be cancelled and it will take at least 10 business days to get you a replacement card. "If you want to confirm the validity of this warning, please call our fraud investigation division and ask for Mr. Smith." (By the way, "Mr. Smith is at a card table set up right next to the crook who sent you the bogus email.)

DON'T DO IT! It's NOT your bank!!! The telephone number is the number of the scammers. NEVER click on the link, never call the number — delete — delete — delete!

**THIEVES ARE BOLDER THAN EVER:** Here's one you'll find hard to believe. Most of the online shopping sites require the purchaser to specify the delivery address and if it doesn't match the profile of the buyer, the merchant requires additional information to safeguard the delivery of the merchandise.

Last week, a local consumer was surprised when over a \$1,000 of stereo gear arrived on her doorstep. Unfortunately, the days of the delivery services requiring a signature and proof of ID are over. (I love my FedEx and UPS delivery people. They bring me things — my wife says too many things!) The delivery truck pulls up, the hard-working driver jumps out of the truck and carefully but quickly puts the boxes on the front porch and sprints back to the truck.

The consumer who received the unexpected \$1,000 of stereo gear was shocked when she noticed HER address and a different person's name was on the boxes. The really creepy part of this scam is the thief is actually watching your house for the delivery. As soon as it's made, they run up to your door and take the merchandise and drive away.

To be successful, the thieves MUST have your home under surveillance. A security camera with a recording function on your front door is best. At least post a fake sign stating "This Area Under Video Surveillance." Vigilance is the key here. (ALSO — use a CREDIT CARD — NOT A DEBIT CARD.) Also NEVER leave your door unlocked — NEVER.

The companies "RING" and "NEST" offer some relatively inexpensive security recording cameras for your front door. (The camera system we have is so sensitive it will detect and record a mouse passing gas within 25 feet of our front door!)

**HOLIDAY GENEROSITY:** Don't ever donate money over the phone. Be VERY careful about any charities sending you requests in the mail. Check out EVERY charity at the website [www.charitynavigator.org](http://www.charitynavigator.org).

If you don't have a computer or access to one — call me — Bill Brooks at (208) 699-0506. I'll look it up for you. Thanks again to The Coeur d'Alene Press, and the staff (especially Mike Patrick the Managing Editor) for making this column possible.

It's a wonderful time of year. Let's all work together to make it a safe for all consumers, friends, family and neighbors.

**REMEMBER:** I'm in your corner. (P.S. Happy Thanksgiving to all!)

Bill Brooks is the CDA Press Consumer Guy and  
Broker and Owner of Bill Brooks Real Estate in Coeur d'Alene.  
Phone: (208) 699-0506 | Fax: (866) 362-9266 | Email: [BillBrooksRealEstate@gmail.com](mailto:BillBrooksRealEstate@gmail.com)