

MERCHANT PROCESSING NEWS



September 2007

What's Inside:

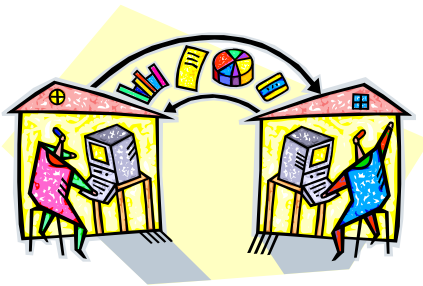
- Purpose of this newsletter
- Spam Emails
- Telemarketing Offers
- Identity Theft
- What can I do about these?

PURPOSE OF THIS NEWSLETTER

It is my desire to both educate and assist business owners on the subject of "merchant services".

Up to this point I've been sharing what I consider to be "detail" information. This month's newsletter is geared toward "business practice" concepts.

SPAM EMAILS



One of the more common (and personally irritating) challenges I experience are "spam emails". I receive a minimum of 75 to 100 spam emails on a daily basis. The subject matter covers anything from lowering my mortgage rate to get rich quick schemes; a miracle drug or pill to change a key part of my anatomy to schemes by someone in a foreign country going to make me rich. You know what I am talking about.

Recently I have begun receiving emails supposedly coming from my bank informing

me of incorrect data in my "personal information file". I'm instructed to "click here", log in and resubmit the correct information for comparison to what's on file. The *REAL* purpose, of course, is to steal my Login ID and password.

Very dangerous! My bank informed me that if there was a problem it is never handled by email.

TELEMARKETING OFFERS



Most of us are on such a fast-paced day-to-day routine in the vast world of internet information and talking heads that we tend to respond rather than think and let our guard down. Just last week I received 3 telemarketing phone calls. The first one was to update an "information database". I was leery when she told me she was calling to *verify* information about my business -- and then asked me to *clarify* the name of my business -- the information I felt she would have known already! When I asked her what she had on file -- She responded with a question. Suspicious, I told her I had a problem with my phone and requested a number so I could call her back in case we got disconnected which happened immediately -- she hung up on me!

The second phone call was an automated recording that alluded to their being my credit card issuing bank wanting to lower the rate on my credit cards. First of all, I have never known of an issuing bank offering *to lower my rate* unless I called in with a competitor's better offer or to dispute an unannounced rate increase. I pressed the appropriate button. A telemarketer responded and began the pitch. I took control and asked "which of my credit cards are you calling about?" She sounded confused when she asked what I meant. I continued that if I was going to discuss rates I needed to know which card she was referring to. Her response was "which card did you want your rate lowered on." I answered "the card I have with your bank" - - she hung up on me too!

The third phone call claimed to be able to lower my merchant account discount rate to 1.39 %. I asked her what company she represented. She replied that "her job was to schedule a "representative" to visit me at my store." I asked her if she had something in writing to fax me so I could review "this program". (In the sales game this tactic is called a "bait and switch".) The "ploy" is designed so that no one really qualifies for that rate due to a range of "excuses" such as credit rating, average ticket, monthly volume or some other reason. They just want the face to face appointment. (Ex: Today some companies will offer free equipment to get in the door - - then reveal mandatory equipment and various associated fees. . . you get the picture.) If I was a major league baseball player my batting average would be awesome as I went 3 for 3 - - she also hung up on me!

IDENTITY THEFT



Identity Theft is a very serious matter and it is extremely important that you be aware of it in both your business and personal lives. As you go through your daily routine as a consumer, examine your credit card receipt to see if your full credit card number is revealed. If so, the

business is out of compliance and can receive fines up to \$10,000.00 per occurrence reported. *AFTER* checking your own merchant account to make sure your account is in compliance, you may want to refer them to our website so they can review the new compliance mandates. Of course, you might want to sign up as an "[Affiliate](#)" first.

**For more information on Identity Theft go to <http://www.crtuneup.com/IdentityTheft.html>

HOW DO I HELP MYSELF?



Let's review and expand on the subjects of this newsletter:

Spam Emails – Most ISP's have a spam blocker and also a way to report spamming. If you receive spam "from a bank", take a moment to call that bank's customer service and see what their fraud email reporting address is and forward it to them. I have done this even though I may not have a banking relationship with that institution.

Telemarketing Offers – Take the time to remove your name from the lists that credit reporting agencies sell to vendors. Go to <http://www.crtuneup.com> and learn more.

Identity Theft – It is vital that you own a shredder so that any junk mail and / or old documentation containing business or personal information is destroyed beyond use - - don't just throw stuff in the trash.

I hear "dumpster diving" has become a new career choice for some criminals.

. . . *more to come next month.*

For more information and timely updates visit:
www.merchantprocessingnews.com