

This Free E-Book is brought to you by Natural-Aging.com.

**[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!**

How to Protect Your Online Store from the Internet Burglars, Part 4 (final)

By Lynne Schlumpf

How to Protect Your Online Store from the Internet Burglars, Part 4 (final) by Lynne

Schlumpf

Thanks for joining me for Part 4 and the final part of this article about how to protect your online store from Internet thieves. Now, I'll tell you some true stories about how we put these methods into practice to save ourselves thousands of dollars, and we got a good laugh to boot!

How to Protect Your Online Store from the Internet Burglars, Part 4
Copyright 2000 Route 66 Cyber Café, Inc.
by Lynne Schlumpf

Here are a couple of true stories for you:

1. A man in England ordered \$27,000 worth of the latest AMD K7 CPUs and motherboards. He gave his REAL address, his real phone number on the order. Boy, was he surprised to get a phone call from the United States asking him to verify the order. He sounded really scared and mumbled something about someone playing a trick on him, that no- he did not order any computer stuff on the Internet. Duh! American Express and the Justice Department got to know that boy really well!
2. Someone in Thailand ordered about \$3,000 worth of computer parts. The ship to address was his home in Thailand, and the bill to was some poor guy in New Hampshire. After calling Mastercard services, we were able to identify the card as stolen. The guy in New Hampshire was not aware that his credit card number had been "lifted". Mastercard promptly cancelled the card.

We emailed the guy in Thailand and told him the credit card number he was using was on the "list" of stolen card numbers. He promptly sent an email back (from his free email service there) and cussed us out in his native language, saying: "What's wrong with a guy ordering something as a present?" Our response: "Ordering something as a present for yourself, with some guy's credit card number in New Hampshire?" Another Duh!

Here are some resources that will help:
(if the card number provided is International, you will be referred by these numbers:)

Visa and Mastercard Services: 800-347-5004
Discover Card Services: 800-347-2683
American Express: 800-528-2121

The US Justice Department would appreciate your reporting what you know about stolen credit card numbers to them:
Their new website called Cybercrime was created to address the growing incidents of crime on the Internet.
Visit them here:
<http://www.cybercrime.gov/>

Internet Fraud Complaint Center

<https://www.ifccfbi.gov/>

This site is brought to you by the FBI, principal investigative arm of the U.S. Department of Justice, and the National White Collar Crime Center. The Complaint Center's mission is to serve as government headquarters for combatting and reporting all types of Internet fraud. Consumers can easily and securely submit complaints. It works like tech support -- you get a ticket number, and then your complaint is referred to the appropriate regulatory, investigative, or enforcement agency. The IFCC and associated agencies will collect, manage, analyze, and disseminate data, warnings, news, and statistics in order to educate the public and catch the perpetrators.

You can also read about how to better promote your website here:
<http://www.r66cci.com/Promoting.htm>

We have some e-commerce read-me's also:
<http://virtualis.com/vr/l Schlump/ecommerce.html>

You can also read an article about Computer Crime here:

<http://www.usatoday.com/life/cyber ech/cth589.htm>

SOME NOTES ABOUT SECURITY ON YOUR SYSTEM:

Here are some other useful utilities to help your business succeed:

Black Ice by Network Ice. This great utility protects your computer while you are online. If you are connected with cable modem, (and even by modem) it is especially crucial that you protect your system against some of the following types of attacks:

TCP port probes

FTP port probes

Trojan horse port probes

Orifice port probes

Subseven port probes

What are these? Many hackers set their computers to constantly scan

thousands of computers on the Internet and automatically look for systems that do not have protection on their different ports. These are areas of vulnerability that can leave your system open to viruses, Trojan horses, worms, and all types of illegal activity.

Black Ice tells you who has been scanning your system by IP address and even by host name in many cases.

It protects all ports, as long as you set the level of protection to Paranoid.

You can find a lite version of this software at their website. We highly recommend that you consider purchase of the full version. It allows you to log for proof if you need it, and it allows you to block certain IP addresses. In the blocked addresses section, you can set it to Autoblock any illegal activity IP addresses.

You would be amazed how many times a day your system is scanned by hackers to see if they can find a vulnerability there.

This was the best investment our company ever made, after switching to cable modem!

<http://www.networkice.com>

One other very useful utility if you use Microsoft Outlook is called ScanMail. It scans your mailbox for any attached viruses on any email you receive.

You can find this great utility here:

<http://www.trendmicro.com>

If you follow these guidelines, you'll have almost zero percent loss in your online store. If you have a success story,

we'd like to hear about it. You'll receive a free case of delicious Penguin Caffeinated Mints if we choose your testimonial to feature.

Lynne Schlumpf is the CEO of Route 66 Cyber Cafe, Inc., <http://www.r66cci.com>, a Web hosting and design company specializing in promoting websites for new owners, building affordable e-commerce sites, and providing reliable web hosting solutions as an affiliate of Virtualis Incorporated.

How to Protect Your Online Store from the Internet Burglars, Part 2

By Lynne Schlumpf

How to Protect Your Online Store from the Internet Burglars, Part 2 by Lynne Schlumpf

Thanks for joining me for Part 2 of this important article about how to save your store from online thieves.

Here's a scenario that will help you identify who is savvy to credit card fraud and who is not.

Let's say that John Smith runs an Internet store that sells books. His store is called Leaflets for Life. Customers order, then he ships the product a few days later.

We have another Internet store owner named Joe Black. He runs a computer parts store called Laptops 4 U.

The owner of Laptops 4 U is aware that his merchandise is THE HOTTEST ITEM to

steal on the Internet. (besides credit card numbers, of course)

John Smith puts his feet, turns on the satellite TV, and lets the Internet run his business silently.

John Smith gets a sale on his online store. The order is for 300 books.

John loves the way the Internet allows his business to pretty much operate on autopilot.

He knows that the 3rd party vendor he uses to take all his credit card sales took care

of it, so all he has to do is print an invoice and pack it up. Off he goes with the

merchandise to the post office, marveling at his first sale from his store.

Joe Black gets a sale on his online store. The order is for a \$3,500.00 laptop.

He does not use a 3rd party vendor for his credit card processing. He just has a store that uses Secure Socket Layer, then it emails him with a link that he clicks on to take him to his orders. Joe Black's process takes a lot more administrative work, but he feels in control of his business. He really wants to be aware of what goes on every minute. Joe, or whoever prints out the orders from the store, takes a long, leisurely look at this order. He knows what he is looking for. He gives the order to a

orders clerk.

The orders clerk picks up the phone, dials the number on the order.

"Mr. Jones, hi, my name is Angela. I work here in the customer service department, and we are verifying your order from our online store. To protect your security could you tell us if you ordered items from our online store today, and if you did, could you please

provide us with some verification of your order. We WANT TO PROTECT YOU.

Could you

please give us the 800 number on the back of your credit card and your bank's name?"

Customer: "Uh, who are you trying to call? This is the roller skating rink in Topeka, Kansas."

Angela thinks that perhaps the person who ordered just mistyped the phone number.

She gets out her list of merchant phone numbers and calls up Mastercard.

"Hello, My name is Angela, and my company is Laptops 4 U. We are a merchant on the Internet,

and we need to somehow verify that a card number used on our online store was not stolen."

Mastercard happily gives her address of the cardholder and other information that tells

Angela that her company could have lost a laptop and possibly their merchant account when

the credit number does not go through the system.

.....the transaction stops RIGHT THERE. Go no further.

(this is not a totally untrue story...happened to us in a similar situation)

John Smith gets the statement from his Merchant Account provider about a month later.

He has sold about 1,000 books this month. His books are a real hot item!

Two days later, John Smith gets another letter from his merchant provider.

John's merchant provider, like many, automatically deposits or deducts credit card transactions from his checking account. After John got the first statement, he gave most of the profits to his wife so that she could go down to the A&P superstore and buy some food. She also decides they need a new living room couch. The money's spent. The 300 books that someone ordered, well – they were ordered on a stolen credit card number. Did John or his automated online store merchant know this? How could they? The owner of the credit card did not know their number and expiration date had been lifted from a

store somewhere on the Net. John is out 300 books and \$4,485.00 in revenue. He also receives a threatening notice that if this happens again, he'll lose his merchant account.

Did you notice anything strange about the merchant account provider taking the money away from John? Mastercard did not eat any of the loss, and neither did John's merchant account provider..notice that? The merchant eats ALL OF IT. John is now in debt to the merchant account provider, and some nimrod is off selling his books in some far away corner of the Internet.

Lynne Schlumpf is the CEO of Route 66 Cyber Cafe, Inc.,<http://www.r66cci.com>, a Web hosting and design companyspecializing in promoting websites for new owners, buildingaffordable e-commerce sites, and providing reliable web hostingsolutions as an affiliate of Virtualis Incorporated.



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!