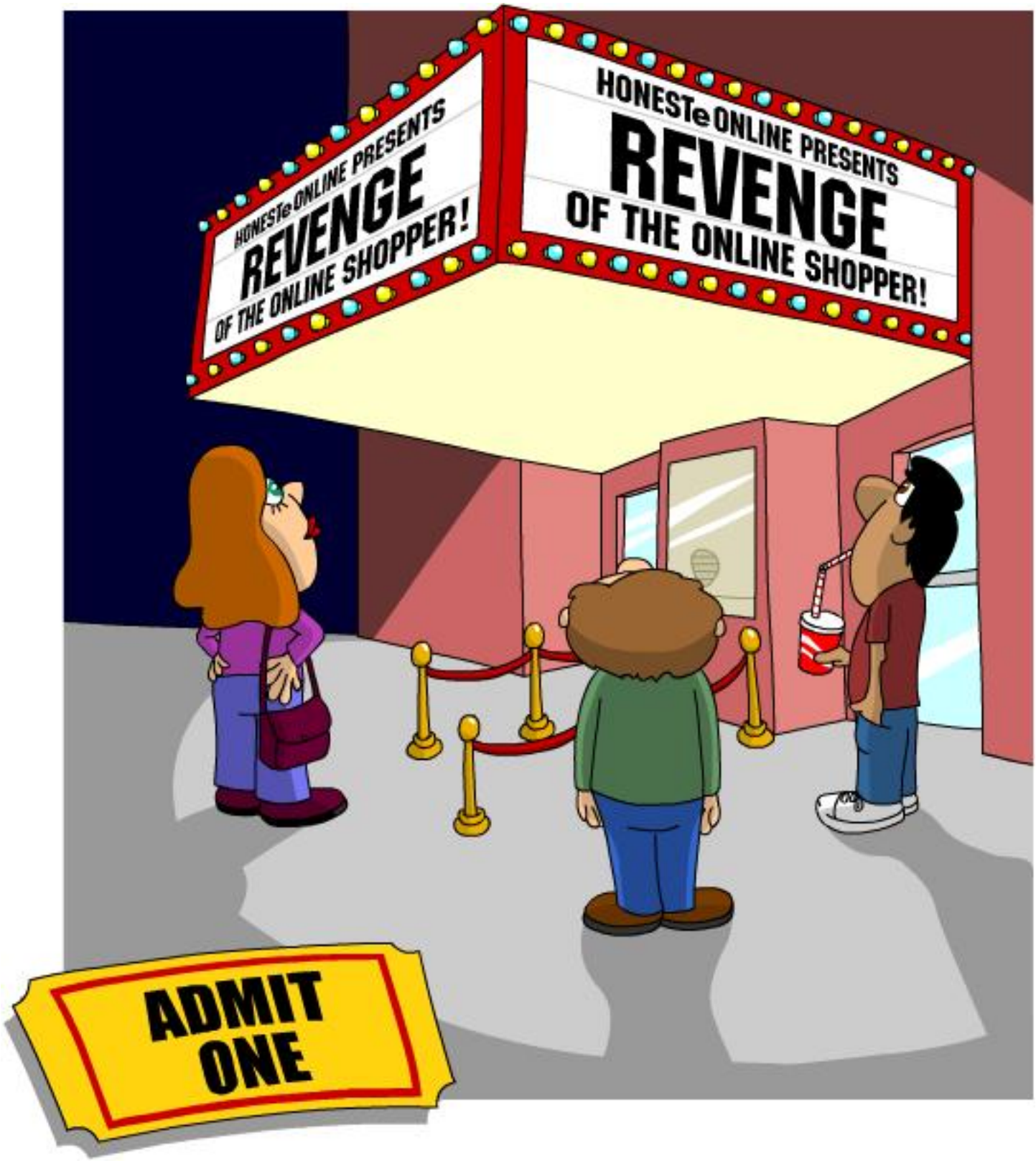

Here's your ticket to
Safe, Smart, Secure,
Online Shopping...

YOU… A Victim Of Online Fraud?

Fraud Fact: Internet Scam Artists LOVE "doing business" with trusting, naïve consumers. They absolutely HATE safe, smart, secure shoppers.

Which One Are You?

Find out by reading the world-famous, **"Revenge of the Online Shopper"** eBook. Someone who cares about you put this into your hands.

Here's What You Can Do:

1. Take 5 minutes to get "eSafe, eSmart and eSecure." Read "Revenge of the Online Shopper" right now and never fall victim to online fraud again.
2. Pass on "Revenge" to your family and loved ones with the email subject line: "Revenge of the Online Shopper."
3. Enjoy the fact that you've taken part in helping others you care about get safe, smart and secure when shopping online. And SMILE, you just contributed to smacking another Internet Fraudster over the head with a frying pan!

Remember: Safe, Smart, Secure online shoppers rarely fall victim to fraud. Knowledge is power.

Quick Introduction:

The Internet is a *unique* and *exciting* place to shop. It's filled with fabulous products and services. And what could be better than shopping from the comfort of your own home in your pajamas?

However, DANGER lurks. Thousands of unscrupulous people are after your personal and financial information every time you place an order.

Worry no more! My name is Jimmy Sweeney, president and founder of HONESTe Online Revealed for the first time in one free eBook, the best little-known secret solutions to keep you super-safe, smart and secure when shopping online.

Get Ready To Enjoy The "Wild,Wild,Web" With A New Level Of Confidence.

Thanks to consumers like you, "Revenge of the Online Shopper" is making its way around the globe. Let's clean up the Internet using the power of consumer education. Take a moment to send a copy to everyone you know. They will thank you for it.

How To Make Safe Online Payments Every Time!

Here's a secret you can bank on. Most financial institutions offer FREE checking and FREE online services. Why? Because online banking costs them less money. Generally, there's no minimum balance required and if there is, it's very low.

Three Steps For Super-Safe Online Shopping…

1. **Set up your primary checking account so you can access it online.** I've been doing this for years, and find it very convenient. As a side note: You can also use the "bill pay" feature to pay most of your bills online. Bills will come to you electronically, cutting your paper bills to a minimum. Never again deal with stamps or envelopes. Most important, you can safely transfer funds online from one account to another in a matter of seconds.

2. Next, ask your bank for a secondary FREE checking account.
Then, get a FREE debit card to go with this secondary account.
Use this one debit card for ALL of your online purchases.

Key Secret...

3. **Transfer just enough money** from your primary checking account into your secondary 'online' account to cover any Internet purchases. Remember, you only keep a small amount of money in this account or enough for the online purchase you are about to make. This means you can safely use the debit card to shop online, and never worry that someone will use the card to run up huge bills. They can't. There's no money to spend! One word of caution: Tell your bank to NEVER authorize over limit charges on this account. They may think they're doing you a favor with this service. Then they do you another favor, and charge you an over limit fee for the "privilege."

OR, Pay For Online Purchases With A FREE PayPal® Account…

PayPal has been around for years, and provides a simple, superb, and secure payment method. Most eBay sellers prefer PayPal payments, as do many online merchants. In fact, eBay was so impressed with the company, they ended up buying PayPal!

Set up a PayPal account FREE of charge, and earn interest on your balance.

If you buy or sell on eBay, PayPal is the way to go. Virtually all online merchants accept PayPal payments these days. Hook your PayPal account to your special 'online' checking account AND the debit card (usually MasterCard or Visa). Then use the PayPal account for your purchases. PayPal is a banking institution, operating with the same safeguards and regulations as your local 'brick and mortar' bank.

I highly recommend using PayPal for your online purchases when this option is available. Plus, if you feel you've been ripped off, you can report this to PayPal and have a much better chance of being reimbursed. You can also dispute a bad charge with your bank too, thus, making it almost impossible to get ripped off for any amount of money when shopping online!

If you sit quiet and close your eyes for a moment, you can almost see the online thief's face turning bright red with anger!

PRIVATE: Do Not Enter!

Passwords And Online Privacy: ALWAYS create a completely different username and password for each account--particularly financial ones. And don't forget to change your passwords on a regular basis!

Two smart choices to protect all of your online login information.

1. **Do-It-Yourself Solution.**
2. **Software Solution.**

Do-It-Yourself Solution:

Keep Fido, Your Mom, And Webster Out Of It!

Do not use your pet's name, anyone's birthday, or any word commonly found in the dictionary. These are easy to guess for someone with a little information about you.

Keep 'em Guessing!

A safer choice is something totally random, like "R9g25_bcX4k" or a password phrase consisting of the first letter of a sentence you will easily remember. For example, "IneccbdoF" comes from "I never eat chocolate cake before dinner on Friday." With a little thought, you can come up with a reasonably secure password you won't easily forget.

A truly secure password contains UPPER and lower case letters, numbers, spaces, and other symbols.

You might even think it looks like the cartoon version of swearing!

If you have as hard a time remembering all these usernames and passwords as I do, there's a neat software solution I detail below. For you "do-it-yourselfers" just make sure to write down all your login information and keep it in a safe place. Most important, be sure to remember where that safe place is!

The following are usually NOT safe places to store your passwords:

1. Inside your computer carry bag.
2. On your hard drive itself.
3. In your wallet or purse.
4. Under a magnet on the refrigerator door...

You get the idea.

.Zip It Up!

Keep your login and password information as individual text files in one folder and update them as necessary. For more security, store them in an encrypted .zip file. If you do this, remember the master password, or you'll never get them back!

Keep your login and password folder on a removable USB flash drive. These are small, convenient little gadgets that plug into the USB port on your computer. They're also quite handy for a quick, convenient backup of most any documents you have on your drive that you'd rather not be toting around with you on your laptop.

My Favorite Software Solution

I discovered this a couple years ago. If you'd like to say goodbye to all your username and password storage problems forever, say hello to RoboForm. I love this tool. If you feel like you're losing your mind trying to manage all the login information to your various online accounts, try this. It's my personal favorite. With one click of the mouse you can create secure passwords and save all your logins. Roboform automatically encrypts this sensitive information on your computer. When you need to access an account the names are listed in alphabetical order for easy access. One click logs you into any account of your choice. Too many features to describe here but I'm a big fan and avid user. Millions of people have downloaded RoboForm worldwide. They have a free trial version but I bought the paid Pro Version because it's inexpensive. The woman who recommended Roboform to me could literally not stop talking about it. Neither can I. But I'll stop now.

How To Avoid Identity Theft From This Day Forward…

Hey, No Fishing! (Phishing)

You know the twisted game 'they' play. You receive an email directing you to visit a familiar website where you're asked to update your personal information. The website asks you to verify passwords, credit card numbers, social security number, or even your bank account number. You recognize the business name (Citibank®, PayPal, etc.) as one you do business with or have in the past.

Take Me WHERE?

You click on the convenient "take me there" link and then provide all the information requested. Unfortunately, you find out later the website is a fake. It was created for one purpose only--to steal your personal information.

If this has happened to you, you have been caught at the old Internet 'phishing' hole!

Bait And Switch

Phishing (pronounced "fishing") is defined as the act of sending an email to a recipient falsely claiming to have an established, legitimate business. The intent of the *phisher* is to scam the recipient into surrendering his or her private information, and ultimately his or her identity.

At first glance, the email 'bait' you receive may appear to be from a legitimate company. The "From" field of the email may have the .com address of the company mentioned in the email. The clickable link even appears to take you to the company's website, when in fact, it's a fake website built to replicate the legitimate site-complete with a recognizable logo or graphic. Criminals make a profession of this. Keep clear of them.

'Phishing' Without A License

A 'phisherman' will do everything possible to make his email look like the real deal. A great way to check the legitimacy of the link is to point at it with your mouse. Then, look at the bottom left hand screen of your computer. The actual website address to which you are being directed will show up for you to view. It is a very quick and easy way to spot these scams. This is not 100% foolproof! A truly clever 'pfisherman' will use attractive bait. Don't bite!

More Than A Click Away

NEVER, EVER, click the links within the text of an email, and always delete the email immediately. Once you have deleted the email, empty the trash box in your email accounts. If you are truly concerned that you are missing an important notice regarding one of your accounts, then manually type the full URL address of the website into your browser and login to your account if you have one. Now you can find out if you've really missed something important or have just avoided a "phisherman" trying to reel you in!

Spies Beware!

Spyware, Adware And Viruses: Have you heard of the terms *spyware* and *adware*? Well, they are not only an ever-increasing nuisance for computer users everywhere, but also a booming industry. According to Webroot Software, Inc., the distribution of online advertisements through spyware and adware has become a MULTI-BILLION DOLLAR business.

You might be asking:

"Why do I feel as if somebody's watching me?"

Probably because somebody *is*! According to the National Cyber Security Alliance, spyware infects more than 90% of all PCs today. These nasty programs are designed to silently bypass firewalls and anti-virus software without the user's knowledge.

Once embedded in a computer, it can wreak havoc on the system's performance while gathering your personal information. Fortunately, unlike viruses and worms, spyware programs do not usually self-replicate.

Where Do They Come From?

Like viruses, spyware and adware can find their way to your computer from email attachments, software downloads, especially freeware and shareware.

What Can Spyware Programs Do?

Some of their deeds are simply annoying for the user; others can become downright aggressive.

Spyware and Adware can:

- Monitor your keystrokes for reporting purposes.
- Scan files located on your hard drive.
- Snoop through applications on your desktop.
- Install other spyware programs onto your computer.

- Read your cookies.
- Steal credit card numbers, passwords, and other personal information.
- Mutate into a second generation of spyware thus making it more difficult to eradicate.
- Cause your computer to run slower.
- Deliver annoying pop-up advertisements.
- Add advertising links to web pages for which the real author does not get paid.
- Provide the user with no uninstall option and places itself in unexpected or hidden places within your computer making it difficult to remove.

YUCK! How Can I Prevent Or Combat Spyware And Viruses?

Let's keep this section simple and powerful for you: You must invest in a reliable commercial anti-spyware and virus program. There are several currently on the market.

Personally, Here's My Weekly "Combat" Routine:

1. **I scan my computer using Norton® AntiVirus.**
2. **I scan my computer with AOL's Spyware Protection. (free popular download)**
3. **I run Spybot - Search and Destroy®. (free popular download)**
4. **I run Ad-aware®. (free popular download).**

NOTE: Make sure you're downloading the REAL versions of Spybot and Ad-aware if you choose to use these. If you're not sure ask a computer technician to help you with this.

Bottom line: There are a TON of free and paid virus and spyware software solutions for you to choose from online. I've listed what works for me. I recommend running two, three or more anti-virus and spyware protection software programs at least once a week to keep your computer as "yuck free" as possible

I still surf the web using Internet Explorer® but many people use the Mozilla Firefox® browser which is reportedly not as susceptible to viruses. However, things change quickly online and there are no absolutes.

Many people prefer to use an Apple® (Mac) computer because spyware, adware and viruses are not nearly the problem they are with regular PC's.

When All Else Fails?

Notice I said "when" and not "if"? As spyware continues to grow and wreak havoc (it covers easily more than 90% of the computers, that's you and me, 9 in 10!), the only solution is to back up your data on a regular basis, and perform a complete reinstall of the operating system! This is something any computer technician can perform for you fairly easily.

CONGRATULATIONS!
Online Thieves Don't Like YOU Anymore!

Let's wrap this up with a quick review and three hot tips:

1. Super-Safe Online Payments - At the very least, designate ONE lower limit credit card for ALL your online purchases. Using one card cuts your exposure dramatically.

Other excellent strategies to protect your wallet…

Open a free PayPal account and use PayPal whenever this option is available. Link one of your bank accounts to your PayPal account.

Open a free secondary online checking account with your bank. Get a debit card for this account (link it to PayPal as well and use PayPal whenever possible). When PayPal is not an option, simply transfer funds from your primary checking account to your secondary "online" account for only the amount needed to cover the purchase. Repeat this process anytime you need to make a purchase online. No one can run up a big bill with your debit card when there's no money to spend!

- Always dispute charges you don't recognize. Always dispute charges when a company does not comply with their stated money back guarantee. You can dispute charges with PayPal and/or your bank when necessary. Using these strategies it's nearly impossible to get ripped off shopping online. Great news for you, bad news for the e-bandits!

2. Privacy and Password Protection - Do not use the same username and passwords for all your online accounts. Use symbols, upper and lower case for the most secure passwords. Store these in a password protected zip file or use a removable USB flash drive. Or checkout the password management software program I use, RoboForm.

3. Phishing - Don't bite! There are some amazingly well-designed scams out there "phishing" for your identity and purchasing power. Never click links within emails even when they appear to be from a major bank or PayPal (a common scam) that you happen to have an account with. There is no reason to "update" your profile, credit card

information, etc., clicking a link from an email. Instead, login to your own account you know is correct and authentic if you feel the email may pertain to you. This way you can clearly find out EXACTLY what's going on.

4. Spyware, Adware and Viruses - Scan your computer at least once a week with a minimum of two well-known updated software programs. I use and recommend Norton Anti-Virus and SpyBot. But there are many great programs to help keep your computer clean.

- **SPAM** is still a real problem for many people! There are several solutions you can find online to cut down on the spam emails you receive. I use AOL for my personal email and I think they do a great job of fighting spam. They also have switched their business model to offer free email accounts so you may want to check this out because the Spyware Protection software and spam filters are all part of the free service they provide.

- **BACK IT UP!** If you value the information you store on your computer you MUST back it up at least once a week. You can use a USB flash drive, an external hard drive, a second or third computer or an online backup service but whatever you choose, back up your computer at least once a week! Hard drives don't last forever and viruses can wipe you out faster than you can scream "OH NO!" So trust me, it's only a matter of time until you'll find yourself tickled pink that you had the good sense to BACKUP your computer's data!

It's Time To Get Even!

You've just the joined the growing number of safe, smart and secure online shoppers.

It's so easy to avoid getting ripped off when you put these simple, powerful strategies to use.

Now You Can Enjoy The "Wild,Wild,Web" With Confidence.

Please remember to pass on "Revenge" to your family and loved ones with the email subject line: "Revenge of the Online Shopper." And a little note that you enjoyed reading this and thought they would too. They will thank you for it.

This Copy Of…

"Revenge Of The Online Shopper"
Compliments Of HONESTe Online Member:

R&R InfoSystems, Co.

www.jedreay.com

Ethical Business Practices

Consumers

The Best Internet
Fraud Fighter Is YOU.

Click to visit our "Be Safe.
Be Smart. Be Secure."
Consumer Resource Center.

eBusiness Owners

Increase Online Sales Up To
17.6 % Or More!

Educate and empower your visitors by
displaying the HONESTe Online
WebSeal on your website today.