

# THE RHODENIZER REPORT

MAY 2007

www.rhodenizer.com

## INSIDE THIS ISSUE:

**PHISHING SCAMS ON THE RISE** 1

**WHAT EXACTLY IS PHISHING?** 1

**THE BUSINESS OF IDENTITY THEFT** 2

**MY IDENTITY THEFT EXPERIENCE** 2

**8 WAYS TO BE SMART AND STAY SAFE** 3

**HOW TO ENCRYPT FILES ON A USB FLASH DRIVE** 4

**ABOUT RHODENIZER IT** 4

## PHISHING SCAMS ON THE RISE

The Anti-Phishing Working Group reports that phishing hit an all-time high in July 2006 with 14,191 counterfeit sites reported.

While this scam has been around for years, many people still fall for it. The amount of money these criminals withdraw from their victim's bank accounts is staggering. What started out as a pastime of certain hacker groups has now become a billion dollar international underground industry.

"Phishing Kits" are even available for sale on the Internet that give buyers everything they need to setup and deploy their very own "money making" phishing sites. These packages include software, logos, canned

scripts, and even tips on how not to get caught.

The goal is not only to empty their victim's bank account, but to also gather information so that their victim's identity can be used to open new accounts, take out loans, even file for bankruptcy protection in the victim's name so they don't lose the property they've stolen.

Recently, one case in California involved a victim being arrested multiple times for crimes he didn't commit. A con artist had been committing thefts posing as the victim—complete with fake ID and other documents supporting his "identity". The police followed leads each time that pointed back to the victim and arrested him instead.



Phishing is only one method of stealing personal information. Other tactics used include stealing from mailboxes and trash cans in order to gather information needed to build a complete profile of the "target". The victim's identity can then be sold on the black market to others with their own scams.

## THE TAKE-AWAY POINTS:

- Phishing scams are just one means of identity theft.
- Identity theft is now a far reaching billion dollar international industry.
- There are ways you can be smart and minimize your risks.

## WHAT EXACTLY IS PHISHING?

Phishing is the popular name given to email scams targeting your personal information.

They come in the form of emails from your bank or some other financial institution instructing you to "verify your account " or to "re-enter your account information so your account will not

be closed". The message is usually worded in a way that gives you a compelling reason to click on the link provided.

The webpage you are then led to looks exactly like the real thing. Unless you know what to look for, it can be difficult to tell that these sites are forgeries

built to trick you into providing your account number, username, and password.

Once you've entered the information, it is added to a database and sold in a kind of underground "farmers market" where identities are bought and sold to other criminals.

## THE BUSINESS OF IDENTITY THEFT

According to the latest Internet security threat report from Symantec Corp., the going rate for the keys to assuming someone else's identity can be had for between \$14 and \$18 per victim on underground cyber crime forums. Deals found will typically include Social Security numbers, bank accounts with passwords, as well as date of birth and mother's maiden name.

In the latter half of last year, Symantec engineers monitored more than 330 servers used on the Internet as bazaars for stolen information and observed nearly 5,000 credit cards being traded and sold on the black market. Over 50% of those servers were located here in the U.S.

Alfred Huger, vice president of Symantec Security Response, said the bad guys are increasingly packaging

stolen data about consumers to add value to the data.

"They are data warehousing this stuff and will steal data from multiple sites to package it at fairly standard black market rates" Huger said.

"Three years ago, this kind of commerce would have been exceptional: If your data was stolen there was maybe a chance it would be sold on underground networks. Now it's pretty much a certainty."



## MY IDENTITY THEFT EXPERIENCE

I'm a professional when it comes to information security so you can imagine how shocked I was to learn that I had become a victim of identity theft ... through no fault of my own.

Several years ago, checks I didn't request were mailed to me by my bank. At that time, I lived in an apartment complex where the mailboxes were just inside the main

entrance. One night, the main cover was pried open and mail belonging to over 50 residents was stolen. I didn't notice anything missing but two weeks later I opened my bank statement to find my account overdrawn and all my savings gone.

That was the rude awakening that led to my passion for becoming an expert on identity theft. After speaking with

the U.S. postal inspector, local police, and my bank officials, I learned a great deal about how these criminals operate and how difficult it is to prosecute them. Fortunately, the offender in my case was caught and the bank restored my account. While I endured some hardships in the aftermath, the real victims were the merchants who accepted those stolen checks. - C. R.

"...you can imagine how shocked I was to learn that I had become a victim of identity theft... through no fault of my own."

## QUICK TIP FOR SAFE CHECK WRITING

One scam that has been around for a long time, but is now greatly improved upon due to modern technology, is "check washing".

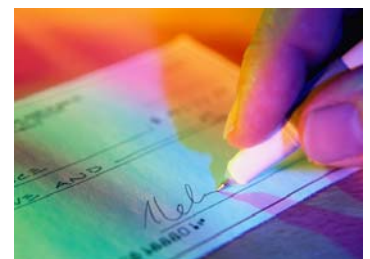
A stolen hand written check is chemically "washed", except for the signature, so all the ink disappears. The criminals can then write out the washed check to whomever

they wish. The amount they choose is cleverly arrived at by calling the bank to verify funds in the account several times. With each call they give a larger amount until the recording tells them there are insufficient funds to cover it.

They then write the check for a little less than that amount to be sure it clears.

**Here's the tip:** Pilot now makes a "gel ink" roller ball pen that they claim is waterproof, fade-proof and smear-proof. These "check safe" pens can be purchased at any office supply store now for less than \$4.00 a set.

Use these for writing checks and signing important documents from now on.



## 8 WAYS TO BE SMART AND STAY SAFE

### #1 - Do not give information in response to an email.

Legitimate companies just don't operate this way. Also, emails are easily spoofed (faked). If in doubt, type the website address into your browser and login on your own. DO NOT click on any links within the email. Or, just call your bank using the number you already have.

### #2 - Get the NetCraft toolbar.

It's a free download from <http://toolbar.netcraft.com> that puts an additional toolbar in your web browser. It's completely safe and helps verify that the website you are on is actually the website it appears to be. It also gives you useful information about the site such as the name of the web hosting company and its country of origin.

### #3 - Use the wrong password.

If you're in doubt as to whether or not a website is authentic, here is a way to test it. Enter the WRONG password when you log in. If the site is legitimate, it will compare the password they have on file with the one you typed and return an error message telling you to try again. Now that you know the site is real, you can proceed with the true password.

If, however, it accepts the wrong password and admits you to another screen, you'll know that the site is fake... and so is the password you just gave them.

### #4 - Shred your papers.

Many cases of identity theft begin with what "dumpster divers" find going through your trash. All junk mail, credit card offers, anything with your personal information on it should go through a shredder before it goes into the trash. You can pick these up at any office supply store for less than \$100.

### #5 - Secure your computer.

AntiVirus and antispyware is not enough. Unless you have some technical knowledge of your Windows-based PC, you should have it checked out and "locked down" by an experienced IT professional. Why? Because the Microsoft Windows operating systems are configured by default to make file sharing easier. In most cases, this also makes it easier to penetrate and exploit. Before you trust your confidential data to a new PC, ask your IT service provider to disable any services running in the background that you don't need. If he doesn't understand... it's time to call someone else.

### #6 - Check your credit card statements thoroughly.

Sometimes criminals will try making a small charge to a stolen credit card account as a test to see if the info they have is good before they sell it on the black market. Check your statement carefully each month and promptly report transactions you do not recognize, no matter how small.

### #7 - Have more than one email address.

Don't use one email address for everything. Use one for business, another for friends, and another for things you sign up for online (so you can change it later when the SPAM builds up). This way, you can get clues about the identity of a sender by which email address they used to contact you. Most ISP's allow you several email addresses with your account. You can also sign up for free email accounts with Google and Hotmail.

### #8 - Check Your Credit Report Every 6 Months.

Georgia Law provides for two free credit reports each year. Check yours closely for any mailing address or open account that you do not recognize as yours. You can sign up for your free report at [www.annualcreditreport.com](http://www.annualcreditreport.com).



**“Don't use just one email address for everything. Use one for business, another for friends, and another for things you sign up for online...”**

**Be Cybersavvy,  
think before  
you click.**

**STAYSAFEONLINE.org**  
Make it a habit

## HOW TO ENCRYPT FILES ON A USB FLASH DRIVE

So, you're backing up all your files to a handy USB flash drive that's small enough to fit into your pocket. Good for you! Now, what happens when you lose it?

Unless that data is encrypted in some way, you could be in for some deep trouble if it falls into the wrong hands.

There is a way to password protect all those files. And, like many of the solutions I tell you about, the best part is it's FREE.

Some USB flash drives now come with built-in fingerprint

security scanners. (shown at right is the Kanguru Bio Drive). But, if you don't have one of those yet, you can still secure the one you have with TrueCrypt software from [www.truecrypt.org](http://www.truecrypt.org).

TrueCrypt is a free open-source tool that creates an encrypted volume on your USB drive to safeguard your files. Files in the encrypted volume cannot be accessed without entering the correct password.

The steps required to download, install, and set it

up can all be found on [www.windowsitpro.com](http://www.windowsitpro.com). Just go to the website and enter the InstantDoc ID number 95235.

Once your USB drive has been reformatted and configured with TrueCrypt. You have the peace of mind knowing that your confidential data is not only backed up, but it's also safe from unauthorized access. All it costs is a little of your time.

Now, all you have to worry about is remembering where you left it.



## ABOUT RHODENIZER IT

Rhodenizer IT is a different kind of IT service provider for the Metro Atlanta area.

We sell no hardware or software. We have no quotas or retail markups. We provide IT consulting services that include finding the best deals on what you need and passing the savings along to you.

We also provide complete service for business computers and networks, but our

mission is not just about fixing computers. It's about solving your IT problems in a way that's guaranteed to save you time and money.

We also help create strategic IT plans for small businesses that set achievable goals for reducing costs and increasing worker productivity.

An organized and efficient IT operation will save your business time and money in the

long run. Let us show you how at no cost to you!

Just call for your **free initial consultation with no obligation**. Tell us about your IT problems and concerns. Then, let us recommend a solution. It costs you nothing to find out if we can help you.

Feel free to call or email with any questions you may have. All inquiries are responded to promptly and courteously.

**Rhodenizer IT**  
Information Technology Services

**RHODENIZER IT, INC.**  
P. O. Box 768122  
Roswell, Georgia 30076

Email: [info@rhodenizer.com](mailto:info@rhodenizer.com)  
Phone: 404-202-8657

[www.rhodenizer.com](http://www.rhodenizer.com)

The Rhodenizer Report is published and distributed by Rhodenizer IT, Inc. © Copyright 2007. All Rights Reserved.

DISCLAIMER: The information, opinions, and recommendations expressed within are for general knowledge and are not intended to be a substitute for personal consultation. Furthermore, some information may be based upon other information provided by third parties. Unless specifically stated, no form of independent verification is undertaken. The author is not responsible for any errors, omissions, or inaccuracies. This information is provided free of charge and is without warranty, neither explicit nor implied. The reader assumes all risk when performing any computer modifications without the supervision of a qualified professional.