RANDOM
COMMUNICATIONS WITH A PURPOSE
THOUGHTS

William Blinn
COMMUNICATIONS
179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

January 2005

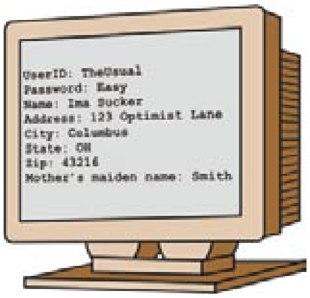
It's 2005. Do you know where your identity is?

Unless you have an e-mail account based in another solar system, you probably receive several "phishing" messages every week. Maybe you receive several per day. Or several per hour. The messages claim to be from a bank (maybe even your bank) or from Ebay or PayPal (even if you've never dealt with either) and they warn you about identify theft. To make sure your account is safe, they want you to visit a website to confirm your information. If you follow the link, they ask for everything they need to steal your identity.

But that's not the only way to get access to your money. Consider this account from the executive vice president of Strike Force Technologies, George Waller: "You receive a message that is a phishing spam, but doesn't really look like one. You own a dog and you subscribe to several Web-based newsletters that deal with dogs. The message invites you to visit a website about dogs and to register for a newsletter. New registrants, the message notes, will receive some free kibbles for their dog." The hook has just been set.

So you visit the site and look around. You see a lot of good editorial information (stolen from other websites, but you don't know that.)

Then you fill out the registration form. It wants the usual information – your name and address (to send the free kibbles for your dog). Because you're signing up for a newsletter, it also wants you to create a user ID and a password. You fill in the same user ID and password that you use for everything.



```
UserID: TheUsual
Password: Easy
Name: Ima Sucker
Address: 123 Optimist Lane
City: Columbus
State: OH
Zip: 43216
Mother's maiden name: Smith
```

Kiss your money goodbye

Of course, you'll never receive the kibbles, but you'll still receive a surprise. What you've just handed the owner of the site is your name and address, a user ID and password (far too many people have one user ID and one password that they use for everything), and a couple of other security questions that are the same kinds of questions other secure sites use to confirm your identity.

The operator of the website knows that you probably use a bank in the town where you live (you've told him where that is) so a quick trip to the websites of all the banks that do business in your town, armed with the user ID and password you obligingly provided, allows the crook to remove money from your account.

This is not a desirable outcome.

What's the next threat?

Waller says that, as bad as phishing is and as insidious as is the fake dog site just described is, something far worse will become prevalent in 2005: Keystroke loggers.

A keystroke logger is a small piece of software that someone tricks you into installing on your computer. It watches everything you type and, every few thousand characters, it sends a small text file to the person who sent you the logger. If you have a firewall and if that firewall watches outbound connections and if you pay attention to warnings from the firewall, you might catch the logger before it sends anything.

But given the fact that already there are hundreds of thousands – if not millions – of computers that have been compromised with malware that has turned them into "zombies" for the people who send spam and phishing messages, it seems naive to expect most users to notice an attack of this sort.

Keystroke loggers aren't the products of futuristic imaginations, either. They exist today. Hardware keystroke loggers have been around for years, but those require access to the computer. Software loggers also exist, and have for several years. Visiting a bad website with a browser that can run ActiveX applications and an operating system that doesn't have up-to-date security patches is all that's necessary to get one installed on your computer.

The real problem is people. Crooks can count on people to create passwords that can easily be guessed or that can be cracked by the most rudimentary dictionary attack. But they don't need to do any guessing or set up any password cracking applications if they can use social engineering to convince someone to hand over user IDs and passwords.

The solution omits human shortcomings

One of the largest problems involving user IDs and passwords is that they are sent and received "in band". In other words, when you visit your bank's website, the bank asks for a user ID. You provide that. Then it asks for a password. You provide that. Even if the connection is secure and encrypted, a keystroke logger running on your computer will see both the user ID and the password.

Random Thoughts (ISSN 1543-1525 [print] – ISSN 1543-1533 [electronic]) is a publication for clients and friends of
William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085.

But what if you went to your bank's website, identified yourself, and they provided confirmation via a phone call – "out of band" where a keystroke logger can't eavesdrop. That's what Strike Force Technologies is working on.

Strike Force provides a service to commercial sites and banks. The company validates that you are who you say you are and gives you several options for out-of-band confirmations. Most people choose to use the telephone.

Here's how it works: You visit your bank's website and identify yourself in the usual way with a user ID. There is no password. But before you can proceed, the screen asks you to wait for a few seconds while your identity is validated.

A few seconds later, your phone rings and an automated system asks if you are trying to use your bank account. You press a key to confirm that you are and proceed. While this process takes slightly longer than entering a password on the website, it's much more secure.

If you don't answer the phone, the person trying to gain access to your account is stopped cold.

This is the kind of creative thinking that will be needed if we're going to beat the crooks of the world. ß

How secure is your data

I was having a chat with an acquaintance who said that she found that her "grossly overstuffed 'Sent' folder in Outlook Express apparently exploded and the entire contents are gone." She also noted that she had a vague memory that this had happened previously and that there wasn't anything she could do to restore the information.

If something like this happens to you, the solution will probably be a data recovery service and you can plan to spend $1000 or more for them to recover the data. Backup is faster and easier. It also costs a lot less.

Just copying data from one place on the hard drive to another is no good if the hard drive itself fails. Just copying data from one disk drive to another disk drive that's inside the same computer does no good if the disk controller dies and scrambles both drives or if someone steals the computer. Just doing a backup to CD, DVD, tape, or external hard drive and then storing the backup media in the same building does no good in the event of a fire.

If you don't have a *verified good* backup that's stored in another building, you do not have a backup.

Good DVD burners cost less than $200 and quality DVDs (don't use the cheap ones for anything you might someday actually need) are reasonably priced. You can obtain an external (fast) USB or FireWire hard drive for $200 to $300.

I did not use this event as an opportunity to denigrate MS Outlook or Outlook Express. I don't particularly care for those programs, but this is not a problem unique to those programs, to Microsoft software, or to any particular operating system.

At that point, another person involved in the discussion said that she'd like to establish a regular backup procedure for her home office and asked what I do.

Mine is a little more chaotic than it should be. I do a full backup once a quarter and a differential backup (changed files) on Thursdays. The rest of the week, the backup drive lives safely in a builint 15 miles away.

There a large and obvious problem here: Given this schedule, I could lose a full week's worth of work. This would make me extremely unhappy, so I do other things to reduce any possible catastrophes. Most website development files are stored on the same server as the website. The server is in Florida. Some files (time billing and the like) are backed up to a second drive inside the machine daily and I've already mentioned the shortcoming in doing that. Critical files go onto a solid-state drive that I can carry in my pocket. I've seen these in stores recently at $50, after rebate, for 1GB.

Back up what?

Having climbed up on the soap box, I found it difficult to dismount. Before I could leave, I was asked "How do you know which files to back up? I suspect there are lot of files that I really need to back up, to save my working environment, but I don't know what they are."

Both Windows and OS X scatter things where you might not expect to find them. Windows probably does more of this than the Mac OS, but some programs (Adobe in particular) install typefaces in their own program directories.

If you modify program interfaces so that they work the way you want them to, then you need the files that store that information. These can be just about anywhere, but they'll generally be inside the program's directory or in the Registry. Sometimes the names aren't at all obvious and, in the case of Macromedia products, you may find several settings files and Registry settings. In some cases, I've made interface changes, closed the application, and then searched the program directory to find files that were changed at that time. It's inexact at best and a good indication that computers are still in their infancy. This is like wanting to change the oil in your car and having to find the oil filler cap, which some auto makers place under the car, others put in the engine compartment, and some put in the trunk.

By comparison, data files are easy. Most programs will (by default) store things in MyDocuments, which will be on C, possibly under your user name. I store all data on D and have my own hierarchical system for keeping things in order (or so I like to tell people).

One backup program I'm evaluating (Dantz Retrospect) recommends against anything but a full backup every time. You won't miss anything that way, but a full backup on my home computer would take nearly 10 hours and would no longer fit on my external hard drive.

The good news is that there are several good solutions for backup. Some are expensive, but none is more expensive than losing your data. ß

on the market CORNER

by A.J. Stinnett

"You are responsible
for everything
your people do
or fail to do."