



Don't get robbed on the Internet

Roboform may be the best Robocop for protecting your information – and your clients' – online



Mortimer

BY MICHAEL MORTIMER

Let's talk about Internet security and preventing you from becoming the next victim/statistic of identity theft, fraud or "robbery."

First, I have a few questions for you:

- When parking your car in a bank parking lot, do you park in the darkest corner of the lot, the section with burned-out security lights?
- Do you leave merchandise-filled shopping bags sitting in plain view on the back seat?
- When walking to the bank's ATM, do you leave your car keys in the ignition and doors unlocked?
- When you get money from the ATM, do you put the bills into a shirt breast pocket with the upper half of the bills flapping in the wind?

If you could scream into my ear, I know your answer to all those questions would be, "What kind of lame questions are those, Mortimer? Do you think I am an idiot?"

Fair enough. I doubt there is anyone so stupid or careless that his or her answer would be "Yes" to any of the above questions.

So, if you are so cautious when driving to your bank to get cash from the ATM, why are you not equally careful when transacting business on the Net? Why don't you use similar precautions when you create passwords and user names necessary to log-on to secure sites for banking, shopping or litigating cases?

Are you using a government grade encrypted password manager on your computers? If not, then you are a careless, incompetent attorney. And it's only luck that you have not had your bank account wiped out, litigation files compromised or that you have not been sued for malpractice.

The purpose of this article is to provide you the ultimate solution to protecting yourself against online hackers, crackers, crooks, criminals and thieves. The program I am recommending in this article will also



protect you against office snoops, litigation spies, suspicious significant others and Homeland Security. (OK, not really on the last. Besides, if you are an attorney and have government agents trying to access your computers, you are in the sewers of Paris, and I can't help you there.)

The program I recommend is Roboform, which is principally a password manager. But, Roboform is much more than simply a program that helps you deal with passwords.

My usual full disclosure: I have been using Roboform since the days it was freeware, which is about six years. Roboform has not provided me anything free to review or to evaluate their program. I have always paid for Roboform licenses from the days when they offered "pro versions" that cost money. Roboform does not even know I am writing this article.



Problems and threats

The Problem: If you have spent any time on the Net, say more than a few months, you have had to enter passwords and user names in order to log-on to the multitude of sites that require such entries to log on. Nowadays people log on to Web sites to:

- **Check e-mail** (in conjunction with Outlook, for example, or strictly online use);
- **Pay bills** (utilities, cable TV, Internet);
- **Shop** (eBay, Amazon, online retailers, specialty items);
- **Conduct financial transactions** (stocks, banking, credit card payments);
- **Socialize** (tweet on Twitter, poke on Facebook, or date on eHarmony);
- **Read** (the news on NY Times, online magazines);
- **Legal research** (Westlaw, Lexis, Findlaw, Fed and State Court Portals);
- **Browse and daydream** (travel sites, destination Web sites: such as Weed, California);
- **Clubbing** (Joining forums or groups on subjects, hobbies or issues that interest you);
- **Litigate** (access court Web sites, download rules, check window hours); and
- **Litigate in federal court** (Pacer and ECF).

Today, just about all of our daily activity involves the Internet. The problem is that to engage in Web activity nowadays, you need to input a user name and password to gain access. Remembering unique passwords and user names for hundreds of Web sites is impossible (unless you are some kind of super memory freak; if you are, move on, this article is not for you.)

Simply put, if you conduct most or all of your business on the Net, eventually the number of passwords and user names you need to remember will overwhelm you (unless you have a program like Roboform.)

Sidenote: How much log-in information might you have to remember? Well, since I first started using Roboform up until today, I have 534 unique and separate Web site log-in entries. I also have

272 "Safenotes," another feature Roboform provides (more on that below.)

I know that some of you work around this problem by using variations of three or four user names and passwords, making it easy to remember the log-in information for each site. However, that's no solution. You are not outsmarting the crooks by slightly varying three passwords and user names. With this lame workaround, it is only a matter of time before a crook cracks your log-in information. After that, the crook will have access to every Web site you use, including bank and credit card sites.

Another problem is that it's difficult to come up with passwords that are unique, somewhat complicated, but still easy to remember. To deal with this problem and what you think is another crafty workaround (despite repeated warnings not to do so) people use the names of their pets, birthdates or street addresses as passwords or user names to log-on to highly confidential Web sites.

However, with Roboform, all of the above problems are solved.

The Threat:

There are many ways that you can become the next victim or statistic of Internet crime. Having watched the news or read articles, you are probably aware of how thieves on the Net ply their trade, so I won't go into detail. But some ways that criminals get your computer's log-on information include:

- **Trojan Key Loggers:** These malicious programs get installed in one way or another on your computer. Once invisibly installed, the Trojan logs all of your keystrokes and the Web sites that you have visited. The hidden program then sends the information to the criminal. It does all this without you knowing it.
- **Phishing:** This is where you open an e-mail and visit a linked Web site in the e-mail. When you go to the "phished" site (basically a phony Web site that looks legit) and enter your user name and password, the criminal gets your information and uses it to drain your bank account, for example.

- **Hacking and cracking supposed secure Web sites:** This is where the criminal cracks supposedly secure Web sites and obtains customer log-in information.
- **Coworkers and snoops:** This is simple. It is where someone you know simply logs on to your computer and accesses all of your confidential information.

The bottom line on Roboform is that the program, when used properly, adds an extremely secure layer of protection on your computers should any of the above-mentioned threats attack your computers.

For example, if someone snoops on my computers or gains unauthorized access via a virus or Trojan, the criminals or snoops absolutely will NOT find my log-on info for the 534 Web sites nor can they see or read my 272 Safe Notes. This is because Roboform protects the information with military grade encryption.

How Roboform works and protects you

I won't get into detail since the technical talk would bore you into sleep. I'll just relist the above threats and briefly tell you how Roboform addresses the problems and threats.

- **Multiple Web sites requiring log-on information:** Roboform deals with this issue by automatically storing (remembering) the log-on username and password you enter on a Web site. Basically it works like this:

After installing Roboform, the program stays "hidden." When it detects that you are on a Web site and entering log-in information, Roboform opens and asks if you want to save the log-in information and Web site log-in page it is associated with.

When you click "Yes," Roboform saves the Web site page and the log-in info needed to get into the site. From then on, you click the Roboform "logins" menu item, Roboform goes to the Web site, automatically enters your log-in information and gets you into the site.

With Roboform there is no need to remember the 534 Web sites and their unique log-in information.

Bonus Tip: Roboform also acts as a great "Favorites" or "Bookmarks" of the



Web sites most important to you and that you actually use. For me, I stopped using my Internet Explorer Favorites folder since I use Roboform to visit the sites I most often use.

Bonus Tip: You also have the option of letting Roboform generate passwords for you. This is a great way to avoid falling into the bad habit of using just a few passwords and user names for all your sites.

- **Trojan Key Loggers:** Roboform defeats key loggers because you are NOT pressing keys to enter your confidential log-in information. In other words, for a key logger, there is nothing to detect. Moreover, when Roboform enters the information it is encrypted. So there is no way for someone remotely to see what Roboform is entering.

- **Phishing:** Roboform helps you here but you must ALWAYS use Roboform to log on to Web sites. NEVER press a link provided in an e-mail, a communication that's supposedly from a company with whom you are conducting business. If a company sends you an e-mail and requests you to log on to their Web site, simply click the Roboform entry for the site and access it that way.

- **Hacking and cracking supposed secure Web sites:** The way to prevent your Web site information from being compromised is to occasionally (every six months, for example) change your log-on information. That way if a criminal gets the info from a bank's Web site, for example, the criminal will have outdated information.

Obviously, changing log on info on 534 sites is ridiculous. Who the hell has time to do that, except some paranoid freak with too much time on his hands? No problem. Roboform makes it easy to do this because you don't have to remember the changes, you let Roboform do the remembering for you. You simply go to a Web site, change the log-on information, make the changes in Roboform and the program takes care of the rest.

- **Coworkers and snoops:** You can set Roboform to time out (close) the program

from 1 minute to 360 minutes. What this means is that if you set it to close after 10 minutes, for example, and someone tries to open Roboform after it has closed, Roboform will ask for the master password in order to again access Roboform's information. No password, no access. If you work in an area where there are a lot of people milling about, setting Roboform to time out after a few minutes gives you a comfortable, secure feeling.

Bonus Tips:

- **Use Roboform to generate passwords.** This way you don't get lazy and use the same passwords (with slight variations) on every site. Don't forget, Roboform does the remembering for you so there's no need to have just a few user names and passwords.

- **Roboform comes in desktop and USB versions. Get the USB version.** It's called "Roboform2Go." This means the program will install on a thumb drive. What's good about this is that you can then use Roboform on any computer with a USB port. True confession: I carry a thumb drive on a chain around my neck. It looks like a military dog tag setup (both the thumb drive and chain.) On that 8GB drive I have my most sensitive and valuable files – Word files containing books I am writing, current cases, Breevy and Roboform.

- **Backup, backup, backup, backup.** As time goes on, Roboform will be one of your most valuable, if not the most valuable, program you have. Trust me when I say you cannot afford to lose five to ten years' accumulation of Web site log-in information. So **BACKUP ROBOFORM FILES IN MULTIPLE PLACES.** I have mine backed up in about 10 different places so that if a thumb drive or hard disk gets corrupted I have backups elsewhere.

- **Safenotes:** This is a cool feature Roboform includes with the program. It's where you can open Safenotes and enter information the same as you would in Microsoft Notepad. The difference is that you can save and backup Roboform

Safenotes and the information is encrypted to military standards. I use Safenotes to store all my banking information, tax data, software licensing information (license numbers, receipts, e-mails sent to me) and credit card info.

- **Pricing:** Roboform usually costs about \$40 by the time all things are said and done. But they have a "Discount Code" box where you can enter a promo code found on the Net. To get one, in a Google search enter the exact name that Roboform calls the discount, put the term in quotes and see what comes up on the Net. For example, enter <"discount code" Roboform> and there is usually a Web site somewhere on the Net offering discount coupons. Be mindful of coupon expiration dates.

- **Updates and upgrades:** Roboform is always coming out with program updates and upgrades. I like that. To make sure you get the latest versions, set your Roboform program to notify you of updates.

Out-of-Context Tips

Although this article is about Roboform, I have some additional security tips:

- **Social Security Number:** Don't ever enter your SSN on Web sites, even if a site requests it. Note I said "request." This is because most sites have other ways to ID you or run a credit check, so giving an SSN is typically optional.

Also, don't ever use your SSN as a password (or your driver's license). If you use your SSN as a password or user name, you are simply lame. Please close this magazine and leave.

- **Lie:** For Web site chat rooms, forums or even free mail (G-Mail) that ask for your name, DOB and address, make up that information even if the site says that the info is required. Make up a DOB, make up a name, make up an address. Why falsify? Well, I for one don't trust what a company will do with that kind of information. Let's face it. Despite a Web site's dandy privacy policy, those are a joke and most companies have a dishonest employee or two who will sell your info to the highest bidder.



JUNE 2010

• **Look for the “s” in the URL address:** On pages where you are entering confidential or sensitive information look for a small “s” in the URL or address of the page you are on. The “s” appears like this:
<<https://onestopshopping4cigarettes-booze&forgiveness.org>>

The “s” after http signifies that the page is secure and the Web site has taken

measures to make sure your inputted data is protected from snooping eyes.

Conclusion

There is a lot more to Roboform that I have not been able to discuss due to space constraints. You can visit the Roboform Web site for a more thorough read. The site is very informative and tells you

how the program works and how it addresses threats. Here is the address:
<http://www.roboform.com>

Michael Mortimer is a federal trial lawyer and author with offices in San Francisco. You can reach him at sanfrancisco@att.net.

