1-1-2007

Digital Hygiene: Internet Traps and Trails

Charles Boulet

Follow this and additional works at: http://commons.pacificu.edu/inter07

Recommended Citation

This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 7 (2007) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Digital Hygiene: Internet Traps and Trails

Posted on February 1, 2007 by Editor

By Charles Boulet

About

This article continues the discussion on self-inflicted data compromise. The discussion will focus on identifying and avoiding some common traps we fall into while using email, browsing the web, and using instant messaging. As we maneuver through and navigate through the various avenues on the Internet, we leave information trails that can compromise our data security. These traps and trails are discussed with a special emphasis on protecting children and other vulnerable things, like your money.

Tip: When you use Internet resources, you put yourself at risk, in other words you gamble. This is a bad game, you lose all the time; the question is whether you lose $40 or your life savings. It seems silly not to simply buy good network security software instead of trying to save a few dollars. It almost doesn’t even matter what you buy.

Remember: Just assume someone is trying to rob and steal everything you own. It’s best to take a defensive position. It’s easy to protect yourself if you take deliberate logical steps to do so. (See the previous article on network security software.)

It would be impossible or at least impractical to learn everything there is to know about every threat. Rather than focus on describing a series of specific threats, it’s best to be familiar with the sorts of threats that exist, then you can identify and intercept the new ones before they cause trouble.

Direct Attacks: Trojans & Robots

It is possible for hackers (individuals, companies, government) to install software on your computer to take full control of your computer. Imagine all of your screen activity, audio, drive
contents and network activity (email, instant messaging, chats, downloads) and camera available to the pirate whenever they are needed. While this is thrilling to consider, it doesn’t often happen. Regular anti-virus scans should account for and protect against most robots and Trojans.

Unless you use specialized network monitoring software (sniffers and other tools), you can never know for certain if your data is compromised.

**Tip**: Be very careful when opening attachments to emails and other files you receive. **If you don’t know the source, you probably shouldn’t open the attachment.**

**Network Sniffers**

Some hackers and phishers will monitor network traffic for opportunities to pounce. Consider the simple postcard. A postcard allows you to issue a quick note regarding some non-critical item, slap a stamp on it, then simply place it in a mailbox for delivery. It is well accepted that anyone who has direct access to the postcard can not only read the contents, but also alter the contents if they so choose. Unless you are using fairly robust encryption, ALL of your emails, instant messages, and other Internet communications (this also holds true for other wireless communications) are subject to relatively easy snooping and potential compromise. It is quite possible, for example, to send an email to a friend and have that email intercepted and replaced enroute with another email. This is somewhat more sophisticated and it is far more likely to have some simply watch your network traffic for low-hanging fruit such as account numbers, user ID’s, and passwords. Consider this possibility the next time you decide to make an online purchase from an unsecured wifi access point at a neighborhood Internet café.

**Trails**

Your instant messenger client will allow you the choice of keeping a history of your conversations. Though the storage of this data is not a terrific risk, you should at the very least be aware of what information is kept. Take for example an IM conversation with someone wherein you offer a phone number or other personal information. This information is very easy to retrieve to anyone who then has access to your computer, say, a computer technician. Check the options in your IM client to see if your conversations are being kept in history.

When ever you browse the web, there are three different logs kept on your behalf.

- **Browser History**: This is a log of the websites you have visited, listed in chronological order. If you look at your history, you will probably note a number of entries that are unfamiliar to you. This is because web ‘pages’ are often comprised of entries, or components, from a number of different sites all compiled into one document.
  
  **Tip**: Whether you use web/URL filtering software to control your children’s access to web content or not, it’s worth sneaking a peek at their histories to keep tabs on their activities. If you can’t determine the nature of a site just by reading it, try
copying/pasting the address into the browser to see where it takes you.

- **Cookies**: Cookies themselves are simply text files used by web designers to track information for you. For example, you might like a particular news site and have set it up so that it presents you with news and weather from your region. A cookie could be sent to your computer to make a list of these and other preferences so that the next time you visit that site, it knows what to show you. Another common use for cookies is to maintain ‘shopping carts’ at shopping sites, or to hold log-in information for you so that you don’t have to remember so many user ID’s and passwords. Given the nature of cookies, they can be a great source of data for marketing agents, surveillance agencies (government and otherwise), and of course hackers and phishers.

- **Temporary Internet Files**: When you visit a website, page information is transferred to your computer which then displays it. The pages you view are comprised of many different bits of text, images, sound, video and other small programs according to the needs of the authors. Your browser, with your implicit permission, stores these pieces of information so that the next time you view the page it will load even more quickly given that the information doesn’t have to be transferred, once again, to your computer.

The temporary Internet files, or the storage thereof, do not pose a threat in and of themselves. But in an effort to ward off ‘garbage snoopers’, you should ensure that your ‘temp’ files are regularly purged. Also, hackers can design pages to trick you into clicking on certain links or buttons that can cause your browser to download **malware** or **spyware**. The temp files area is where these programs land and wait until needed.

Your browser history, the cookies you collect and the temporary Internet files are all collected to assist you and enhance your online time, but these areas also represent trails that can be tempting to hackers and phishers. Any comprehensive network security software will provide tool for clearing out the three logs very simply and you should do so regularly, especially if you’ve been using the web for purchases or other business where you’ve entered personal data into forms.

**Phishing**

By far the most common means of data loss is the capture of data over the Internet, and this usually means that the user gave the information away. This is classic phishing. The attacker uses false forms and emails to convince the user that they are submitting information to a trusted source.

You might, for example, get an email from what you think is your bank asking you to confirm your account number, login name and password. Of course, no reputable bank would ask you to do this, but being a trusting sort, you click on the link provided in the email and you are taken to a very slick website that could easily be mistaken for your bank’s site. In most cases, the form
you are asked to fill in is on the first page of the website, something else your bank would not do. After filling in the form and clicking on the button provided, you might be directed to a page that offers thanks for your compliance and a ‘have a nice day’ notice. You may not notice anything for days, weeks, and sometimes even months. As a general rule, the longer it takes to notice problems, the more problems you will have. This is because professional phishers, that is those connected to organized crime, will have the means to take full advantage of your identity and this takes a coordinated effort and some time — weeks to months. Compare this to than the neighborhood hacker who simply wants to use your information to buy suits, cars, stereos and Cheetos®; these things are easy to spot on your online banking statements, which you should check at least a few times weekly.

It is also possible that some individual, or organized crime cell, could set up a false front for a company, charity, or other service online where users are tricked into purchasing a product (read “providing credit card information”) or providing personal information. These situations are the hardest to protect against as the user does it to himself. Look for familiar signs and assurances on the website: Does the site use a third-party payment system and is your purchase guaranteed? How do you know? Are there references and testimonials on the site? Is the payment form secured (look for a sign in your browser like a lock icon, or ‘https’ in the address)? Look at the address of the site — it will tell you what site you’re really looking at.

There are many ways to trick you into compromising your guarded secrets. The solution is simple: Don’t give your information away unless you are completing a transaction you initiated.

**Common Sense**

As a rule, just assume that anyone who shows up on your doorstep asking you for private information is up to no good. If it is in fact your bank, your favorite bookstore or some other merchant, they will have other ways of reaching you. Unless you specifically go to your bank’s site and manage your accounts, or to a merchant site and agree to buy something, never give away personal information online.

**Tip:** I tell my children a) that on the Internet anything that comes for free comes with a big cost, b) to use **fictitious** identities when downloading useful or fun nuggets from their favorite sites, c) to **never give any personal information** unless it is supervised by someone responsible — if they can’t explain to you why they need to give personal information, they shouldn’t be allowed to do so.

Always ensure your network security software is up to date and that it covers your particular needs. Make a list of all of the ways in which you interact with the Internet — does your security software protect them all? If so, are these features turned on and properly managed?

Use common sense; it’s easy to protect yourself. There are great tools on the market today that make your life much easier and safer. Consider it insurance against great loss. If you have any
questions, try the links below.

**For More Information:**

- You can research specific threats starting at:

- For a map of current threats in North America, go to [http://www.trendmicro.com/map/](http://www.trendmicro.com/map/)

- Cross-referenced virus encyclopedia:

**Case Study:** Phishing for Chase Manhattan Account Numbers

This mail item arrived in my mailbox:

![Mail Item](image)

This looks legitimate, even the link. I particularly like this line “We recently have determined that different computers have logged onto your Chase OnlineSM account, and multiple password failures were present before the logons.” This is exactly what you might expect to hear; it’s great misdirection; while you’re busy thinking about someone trying to get into your account, you’re not able to fully attend to the possibility that there might be a thief right in front of you. You would imagine the website on the other end of that link is just as convincing.
Only, there are some problems with this email.

Your bank would not likely contact you by email regarding something so important. It is a very insecure way to communicate.

Your bank would not ask you to change your password, unless you asked them to help you to begin with.

Note also who it’s from. The alias of the address says JPMorgan Chase & Co., but the actual sender is goober2001@verizon.net. (Special thanks to Verizon for not closing this and other holes…).

Outlook has labeled this as spam. If your software labels a message this way, it’s worth considering the possibility that there is a threat or trick attached.

In Outlook, you can right-click the message and select ‘View Source’. (You can view the source code of any email.) This is what the code looks like for this message:

We will be forced to suspend your account definitively, as it may have been

Used for fraudulent purposes. We thank you for your cooperation in this manner.

**To change your Chase OnlineSM password click here:**

The blue line is the actual address you are opening. Specifically, you are opening a form on a server. The form is generated by a program called “prospect.php” and ‘change_form’ is the call that generates the form in question. Presumably, there are numerous other forms in action on this site.

The green line is an extra bonus. The code means ‘when the user places his mouse pointer over the link, don’t display the actual link in the status bar, display https://chaseonline.chase.com/colappmgr/colportal/prospect?_nfpb=true&_pageLabel=page_logonform’ instead. Again, this is great misdirection. On a legitimate site, ‘https’ indicates a secure webserver, which you would expect when dealing with your bank. The real address for the link is not secure, it’s not usually worth the trouble for hackers to provide secure data transfer between your computer and their server.

As a very simple check, you can point your mouse to the link and simply hover over it without clicking it. In many mail clients, a popup label will tell you what the actual underlying link is. In this
case, this is what appears (note that in this picture the pointer is not shown):

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3321].