

USER AWARENESS NEWS

WHEN PASSWORDS ARE NOT ENOUGH

INSIDE THIS ISSUE:

Excel Tips	2
Risky Wireless	2
Trash & Recycle Bins	2
Music Downloads	3
Effective People	3
Cartoon	4
Pharming	4


Security Experts have long argued that username/password combinations are not secure enough for web applications — with good reason. Every public web site on the Internet gets hammered daily with hundreds or thousands of attempted logins. Even our own web sites have hundreds of login attempts thrown at them daily. I know this, because I get daily alerts that show this activity.

In the realm of access control, username/password logons are considered “*something you know*”. That is, the user just needs to know the username/logon for the authentication to complete. This is different from “*something you are*” — biometrics is an example of this, or “*something you have*”, for example a smartID card.

To provide better security, we can combine these “*some things*” to create multi-factor authentication.

For example, I recently viewed a webcast that combined a username/password with a phone call to provide two-factor authentication (something you know and something you have). After providing login information, the web site automatically calls your phone number, from which you must press “#” to be authenticated. If someone else tried to log in with your username/password, they would be unsuccessful, since they do not have your phone.

Expect to see multi-factor authentication become more common as businesses realize the limitations of simple username/password access control.



Two-Factor Made Easy

Introducing PhoneFactor™ — a phone-based two-factor system that eliminates the need for expensive tokens and other devices. Users instantly receive a call when logging in and press # to authenticate. It works with any phone.

[How it works](#)

Mahalo means “Thank You”

My Hawaiian colleagues at SANS sign every email with either *mahalo* or *aloha*.

Aloha and Mahalo are two of the most important words in the Hawaiian language.

Aloha can mean “hello”, “goodbye”, or “I love you”.

Mahalo means “Thank you”.

WILL MAHALO REPLACE GOOGLE?

My studies at Albright College include tons of technical research assignments. While Google is great for quick answers to specific computer errors, it is woefully inadequate for in-depth research. In several cases, the topic to be researched cannot be found, except for Wikipedia definitions, which do not go far enough for the assignments. This is where Mahalo comes into play.

Where Google does an excellent job of finding specific problems and Wikipedia does a great job of getting quick definitions, Mahalo groups information by topic. Mahalo will show the ‘top 7’ links, as well as all news, background information, blogs, and discussions related to the topic.

How is Mahalo different from Google? Google uses computer algorithms to determine top

spots. It is completely automated. This can be good for specific search information, but may not work as well when looking for in-depth whitepapers and other research material.

Mahalo is built by people, not algorithms. It is like Wikipedia in this respect, but is not open to the general public for editing. Since there is a human element, not all topics can be found on Mahalo. A search of ‘quad core CPU’ turns up the message “*we haven’t written a page yet for this*”. I’m given the option to request it. I’m also given a tab to all other search engines with the results of this search. Pretty cool and definitely a tool worth tracking! But I don’t see it replacing Google.

SEPARATE OUT MONTH & YEAR IN EXCEL

There are times when it's really handy to separate out the month & year from a date. For example, you want to total by month or perform conditional calculations by month. Whatever the reason, Excel makes it easy to separate out the month and year from a date on your spreadsheet. Let's suppose you have a date in cell A2. To put the month and year in column B, simply enter the following formula into B:

```
=MONTH(A2) & YEAR(A2)
```

The result will be only the month and year,

for example '32008'. Now, you can perform a conditional calculation, such as adding to a monthly total if the month/year is equal to the next row:
=IF(\$B3=\$B2,\$D2+\$C3,\$C3)

Let's say this is entered into D3. This says if the month/year in B3 matches the value in B2, then add D2 & C3, otherwise just put the value of C3 in D3. Sounds complicated, but just try it and you'll see how easily it works.

Just Wing It

People often spend too much time up front trying to solve problems they don't even have yet.

Don't.

Don't sweat stuff until you actually must.

— excerpt from "Getting Real" (The smarter, faster, easier way to build a successful web application)
by 37signals.com

Thanks to Tom O'Neill for the tip on this entertaining eBook!

RISKY WIRELESS BEHAVIOR

In a study by Cisco, workers were surveyed to determine the type of risky behavior they were willing to perform on their computers. One of the questions was on risky wireless behavior. Ten percent surveyed said that they have used a neighbor's Internet connection when working remotely. Most stated they did so because "they were in a bind" and that their neighbor didn't know about it.

Why is this a risk? For several reasons. First, if you attach to your neighbor's network and it becomes compromised with malware, it can easily spread to your home network and possibly through remote access into your network at work. If other people attach to your wireless router, they can monitor your network traffic. Everything that is sent unen-

rypted can be viewed quite easily with free tools.

The risk is greater for people who use the older 802.11b wireless routers, which have poor encryption options. Tools like wep-crack will break 802.11b (WEP) encryption in a few seconds. What can you do?

First, upgrade your router to a newer version that supports WPA2, which offers better encryption (for example: Linksys WRT54G). These routers enable you to set encryption on for all network traffic. Then set filtering to limit the PCs allowed to access your router. Newer routers come with security software to help you set up secure wireless networks. Monitor activity to make sure your home network stays secure.

TRASH BINS & RECYCLE BINS

Computers provide a couple of temporary storage objects for user convenience. These objects aren't meant for permanent storage. In fact, on some systems these temporary locations are cleared every time the user logs off. Let's look at two examples of temporary storage.

The first example is the trash bin/folder in your email application. This folder should only be used to store actual trash — emails that you want to throw away. You can configure your trash folder to empty each time you close the email application and this is an excellent way to save space.

—> Never store legitimate email in the trash as a method for temporarily saving information! Believe it or not, I've known users to do this.

The next example is your computer's recycle bin. This is also meant for files you no longer need — it should never be used to store anything you may need later. Again, I've seen users do this, only to wonder where their files ended up later.

If your helpdesk has regular PC maintenance scheduling, sign up for it. Otherwise, try to schedule your own maintenance quarterly. Part of this maintenance work should include *emptying* the recycle bin and *deleting* old email from the trash folder. Obviously, if you are using these objects improperly, you may end up losing information. Please think of these temporary storage locations as real trashcans that will be emptied regularly.

COPYRIGHT INFRINGEMENT ON MP3S

In October 2007, a single mother from Minnesota was fined \$222,000 for downloading 24 songs and sharing them online using a peer-to-peer network. If she had been prosecuted to the fullest extent of the law, she would have faced \$3,600,000 in fines and 240 years in jail...for 24 songs!

Copyright infringement is a topic that has come up in my home many times over the past year. My 15-year old daughter watches videos on YouTube that con-

tain bits of movies put to popular music. She wants to try making her own video. Is this copyright infringement? Clearly, it is. Why is the web full of kids creating these types of videos? Because the laws haven't caught up with the technology. It's all a bit fuzzy.

If you steal a CD, you are breaking the law, no question. But what if you borrow your friend's CD and burn one song to your MP3 player — is this a crime? Technically it is, but what

are the damages? The cost of a CD, the cost of a song, the cost per use? As it stands now, the copyright law is brutal when applied to individual song downloads, but many kids (and adults) don't think they are breaking the law when they share music or movies with each other.

If you like to be safe rather than sorry, buy your music online, subscribe to a monthly download service, and avoid making copies for friends. No song is worth 10 years in jail!

Why so much information about security?

You may have noticed that this newsletter always contains a few information security topics. I include them because it's what I know. I'm an instructor with the SANS Institute (www.sans.org). My responsibilities in this role ensure that I keep up-to-date with the latest cyber security trends and I like to share this information with others. The Internet is like the wild, wild west. There are few laws and lots of dangers. I would love to see it become self-managed through informed use, rather than regulated to death by politicians. The more people know, the better off we are. Sharing this knowledge is part of my personal mission!

THREE HABITS OF THE HIGHLY EFFECTIVE EMPLOYEE

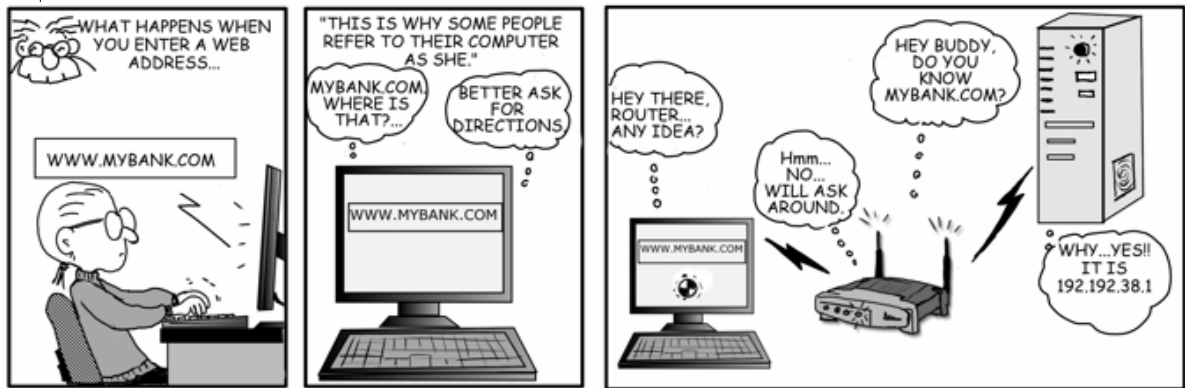
TechRepublic recently had a post that extolled the virtues of the highly effective employee. Here is *TechRepublic's* opinion of the most important qualities for employees to succeed in the workplace. I'd add that these qualities can be beneficial to succeed in *any* area of life.

- Flexibility: Everybody knows of someone who, every time he is told about a new goal or task, wastes time grumbling about how it won't work. If you've ever read the book "*Who Moved My Cheese?*", you understand the natural aversion to change held by many people. However, if you take the time to set new goals, work toward new objectives, and learn from failures, you realize how rewarding flexibility can be. Don't be the mouse who dies waiting for the cheese to return. Be flexible. Move with the changes, not against them.
- Self-motivation: The self-motivated employee does not wait for the boss to tell him which new projects to take on when the workload slows down. You'll never hear the self-motivated say "That's not my job". Self-motivation is recognizing when something has to be done and then doing it. This is quite different from talking about what has to be done and

NOT doing it, and the very-similar *trying* to do something, but never getting to completion. At SANS, we refer to this last example as projects that "die on the vine". As Master Yoda says "*Do or do not, there is no try*". My karate instructor uses this quote by Yoda so often that I now cringe inwardly whenever I hear someone say "I'll try" in response to a request.

- Initiative: This is one of my personal favorites. Nothing excites me so much as an employee who comes to me with a solution to a problem, without being asked. Synonyms of "initiative" are inventiveness, resourcefulness, and ingenuity. A workplace that fosters initiative can be a wonderful place to work, since employees are free to think 'outside the box'. This is the Value-Add that goes beyond just doing a job.

<http://blogs.techrepublic.com.com/career/?p=277&tag=nl.e124>



Editor: Lori Homsher
 www.LoriHomsher.com
 SANS Instructor
 www.sans.org
 Email: lori@homsher.net



Reproduced with permission from www.SecurityCartoon.com

"The freedom to do your best means nothing unless you are willing to do your best."

—Colin Powell: 65th U.S. secretary of state

PHARMING

Pharming, a cousin to phishing, is a scamming practice where users end up redirected to bogus websites.

Pharming can happen by poisoning a DNS server, by compromising a router, or by changing out host files. Here is a quick description of each of these methods:

- DNS poisoning: Since DNS servers are responsible for translating host names (ebay.com) into IP addresses (66.135.205.13), if a DNS server is poisoned, its name lookup services cannot be trusted. A compromised DNS server can redirect traffic to bad web sites, often without user knowledge.
- Router compromise (see cartoon): routers often answer DNS inquiries for users. Wireless & home routers with default settings are among the most easily compromised. If the router is compromised, it may get bad DNS information and send users to the wrong site.
- Hosts file: This is one more method of redirecting a user. The host file is the old-

fashioned way of resolving host names to IP addresses. If a user's PC is infected, the malware may include a new hosts file that contains direct hostname/IP address lookups to send the user directly to pharmed web sites.

The end result is that the users get placed on a web site they *think* is trusted, but is actually bad. Normally, the bad-guy's goal is to steal identity information, access credentials, usernames and passwords.

The bad news: antivirus software and spyware removal software CANNOT protect against pharming. Web browser add-ins may help, but your best bet is knowledge, user awareness, and diligence.

For home computers, I recommend a complete security suite, such as Trend Micro Internet security. Security suites offer additional protection over plain old anti-virus by providing web filtering, fire-wall protection, intrusion detection and intrusion prevention, and wireless security.