

SHEERAN I.T. NEWS

INSIDE THIS ISSUE:

Excel Tip	2
New Sheeran Systems	2
Data Theft	2
Web Proxies & You	3
Highly Effective Employees	3
Pharming Cartoon	4
Pharming—Part 2	4

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

—Colin Powell: 65th U.S. Secretary of State

MEET DOLORES!

Dolores Strouss started work with us in November 2006. She came after we had set up the original direct-to-consumer (DTC) system and helped us finish up the first season. Since then, she has continued to work on the DTC system and has also helped Clint with TOPS changes.

Dolores graduated from Goldey Beacom College with a BS degree in Information Systems. Here are a few things we've learned about Dolores over the past 18 months:

- She has one daughter who is a dancer and will be graduating from high school this year.
- She worked on a Habitat for Humanity house in 2003.
- She has been involved in many committees with her Homeowner's Association in the past.
- She loves to ski!
- Her vacation this year will be a trip to Italy!

- She has been programming for 13 years.
 - She likes to garden.
 - Dolores recently started indoor rock climbing and is working towards climbing the rocks in the picture below!
 - She helps out at Cornerstone Church in Glasgow.
- We appreciate Dolores' quick smile and easy-going nature!



WHEN PASSWORDS ARE NOT ENOUGH

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 access to be given. 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 "*somethings*" to create multi-factor authentication.

I recently viewed a webcast that combined a username/password (something you know) with a phone call (something you have) to provide two-factor authentication. 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.

PREVENT EXCEL FROM TURNING FRACTIONS INTO DATES

One of the things I dislike about Microsoft products is their insistence that they know what I'm trying to do, which often results in overriding my commands. One annoying example of this can be found in Excel. When you type a fraction of 1/3, Excel converts it to Mar-03.

How do you make Excel stop? You must format the column to tell Excel you are working with fractions (do this before you enter any values).

Here are the steps:

- Right-click to select the column that will contact the fractional data.
- Select 'Format', 'Cells'
- In the number tab, under 'category', select 'fraction'.
- Under type, select the number of digits you want, then click OK.

Details at:

<http://blogs.techrepublic.com.com/msoffice/?p=424&tag=nl.e056>

NEW SYSTEMS

This past quarter we've added/started a few new systems for employee use.

IDEAS in Bugzilla

Not really a new system, but a new feature of Bugzilla, the new IDEAS product is available for you to submit your ideas about anything! This is based on the system used at Armstrong World Industries to collect and implement employees ideas. At Armstrong, it works by matching each new idea to a 'corporate sponsor', who helps get the idea implemented. I know our employees have many good ideas and I'd love to see some of them come through the system. To submit an idea, simply go into Bugzilla,

click "NEW", click "IDEAS", click on the appropriate "component" and enter a summary and description. That's it! See Lori for help.

Quoting/Job Ticket/Job Cost

We are working on a new quote and job ticket system that will be connected to the existing job cost system. Our goal is to integrate all of these functions to reduce duplication of effort and minimize errors. The result will be a fully integrated system that will help streamline the processes from sales, through production, all the way to billing. More details will follow.

"You become what you think about."

—Earl Nightingale
Author, *The Strangest Secret, Lead the Field*

DATA THEFT—THE NUMBERS ARE STAGGERING

Since January 2005, the Privacy Rights Clearinghouse (PRC) has reported more than 220 million exposed personal records. The rate of exposure is growing faster each month. Each exposed case represents the potential for serious misuse. Identity theft is an expensive problem that can take years to resolve an individual case.

The potential for damage from data privacy breaches and the resulting risk of identity theft is only one of the reasons we take security very seriously. Intellectual property disclosure, trade secret theft — even competitive intelligence — are other risks that can cause damage to the company and its employees.

How can you help? There are several things you can do to keep personal information safe:

- Encrypt consumer data before sending to clients in excel or other file formats.
- If the client is unable to handle encryption, password-protect the file prior to sending.
- Make sure the web sites you visit are encrypted before entering personal information. Look for 'https' in the URL.
- Consider the classification of reports, policies, procedures, and documentation before sharing with clients and vendors. If the information is confidential, a Non-Disclosure Agreement may be required.
- Don't send documents to your home computer.

WEB PROXIES AND YOU

Every time you enter a web page to visit, our proxy server is working for you. It handles the web request on your behalf. If the web page is static (has not changed), the proxy doesn't bother to retrieve it, but just displays a cached version. The result is that you get to view the web page very quickly.

We recently added a filtering component to our web proxy. This filtering is done based on blacklists. They aren't 100% accurate, but they are free and will protect our desktop systems from many bad web sites.

While we know this may be

an inconvenience to some, we need web filtering for many reasons. Here are a few:

- Our anti-virus software does not protect your computer from a malicious web site.
- Just visiting a malicious site can compromise your computer — you don't even need to click anything to become infected.
- Botnets can be installed on your system without your knowledge. Anti-virus may not pick it up.

- Our network is protected by a firewall, but our firewall cannot evaluate the content of traffic. In other words, it cannot see if the web site content is bad.
- Web applications currently represent the largest single type of threat on the Internet.

Please let I.T. know if you have a legitimate business need to access a site that is blocked by the proxy server. We can set up exceptions. The proxy server is a safety mechanism to keep your systems safe and it does this at no cost. What a bargain!

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 category 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>

Why so much information about security?

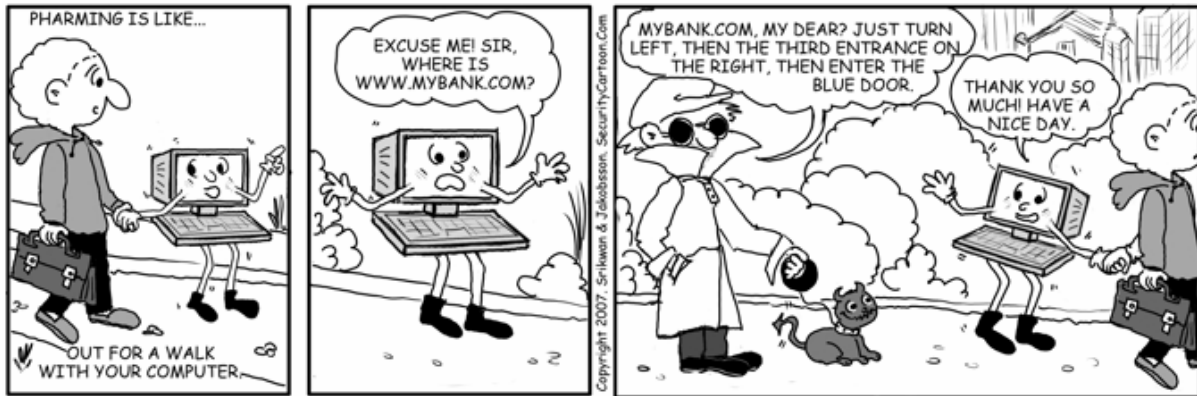
You may have noticed that this newsletter always contains a few information security topics. I include them for several reasons. First, it's what I know. I'm an instructor with the SANS Institute (www.sans.org). My responsibilities in this role ensure that I keep up-to-date with the latest cyber security 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!



Sheeran Direct Marketing
 71 Southgate Blvd
 New Castle, DE 19720
 Phone: 302.324.0200
 Fax: 302.324.0213
 www.jjsheeran.com

Editor: Lori Homsher
 Email: lhomsher@jjsheeran.com



Reproduced with permission from www.SecurityCartoon.com

PHARMING—PART 2

After two of our very own employees have experienced some form of router compromise (wireless routers, of course), I thought it might be nice to spend some time on that topic. In this issue we are talking about “drive-by-pharming”. It can happen when wireless routers are installed with no changes to the default settings. This probably describes more than half of home user wireless set-ups, so it’s a fairly large problem.

Here’s the blueprint: you buy yourself an 802.11b wireless router for cheap (only \$10 on ebay!), plug it in, configure it for your Internet connection, and you’re done. Did you change the default password? If not, you are a candidate for a drive-by-pharming attack. Using simple JavaScript attacks, settings on the router can be changed, including the DNS servers used by your home network computers. Keep in mind, it is the DNS servers that point your computers to web sites.

Pharming is a type of attack in which a user is fooled into entering sensitive data

onto a malicious web site that impersonates a legitimate site. Imagine this: you type www.mybank.com to do a little online banking. Since your router has been compromised, you are sent to a malicious site that looks just like mybank.com. You enter your login credentials, which the malicious site very nicely uses to log into the real banking site and take your money. It’s very slick. What’s an online banking customer to do?

- First, change the default password on your router.
- Make sure your bank uses a secure connection (https).
- Do not ignore certificate warning messages. These messages indicate there is a discrepancy between the certificate issued and the domain you are visiting (see sample to the left).
- Use web filtering proxies when possible (see inside story). They protect you from visiting bad web sites. Many Anti-virus suites contain good web filtering options.

