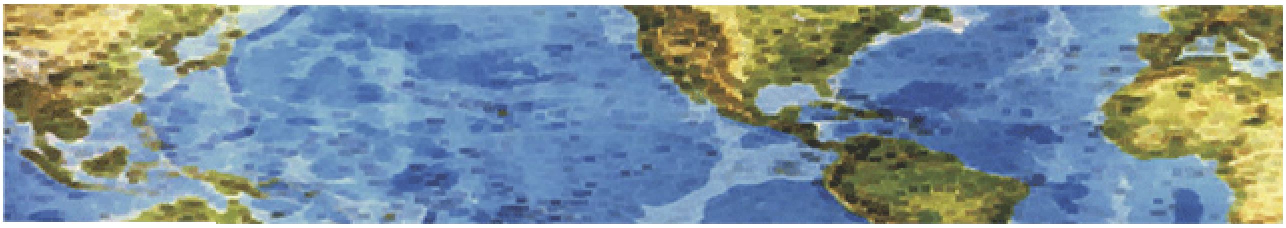
HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 February 2014 Newsletter

Scam Website Targets Army Info
Bogus Benefits Site Collects Service Member Log-Ins

The U.S. Army Criminal Investigation Command is warning service members to avoid a false benefits website that's attempting to collect account log-in information for soldiers and veterans. The website, us.militarybenifit.org, is being used to collect U.S. Army service members' Army Knowledge Online e-mail accounts and passwords, according to the Criminal Investigation Command. The real Army Knowledge Online is the main intranet portal for the military.

The bogus website makes the false claim: "The U.S. military has granted access to unclaimed and accumulated Army benefits for the under listed active duty soldiers. Benefits not claimed within the stipulated period will be available for claims after 60 months”. Service members are reminded to visit the authorized Army benefits website, myarmybenefits.us.army.mil. "Cyber-crime and Internet fraud presents unique challenges to U.S. law enforcement agencies as criminals have the ability to mask their true identities, locations and cover their tracks quickly," the Army says. "Website and accounts can easily be established and deleted in very little time, allowing scam artists to strike, and then disappear before law enforcement can respond."

This illustrates how simple and easy it is to establish a scam website and try to collect personal information. Always know where you are going by putting in the URL yourself and not clicking on an e-mail link.

http://www.govinfosecurity.com/scam-website-targets-army-info-a-6493?rf=2014-02-11-eg&utm_source=SilverpopMailing&utm_medium=email&utm_campaign=enews-gis-20140211%20%281%29&utm_content=&spMailingID=6113167&spUserID=NTQ5MzMzMDA3ODES1&spJobID=381003344&spReportId=MzgxMDAzMzQ0S0

Fake Funeral Notice

Scam artists (criminals) are forever trying to trick you into clicking on links that lead to downloading malware on your computer. This latest scam takes that to a new low. There are now bogus e-mails with the subject line “Funeral Notification”. The message appears to be from a legitimate funeral home, offers condolences, and invites you to click on a link for more information about the upcoming “celebration of your friend’s life service”. But instead of sending you to the funeral home’s website, the link sends you to a foreign domain where malware is automatically downloaded to your computer. You can always hover the cursor over an e-mail link to check on the URL it will send you to.

An Important Thing You Need to Know About “Deleted” Files

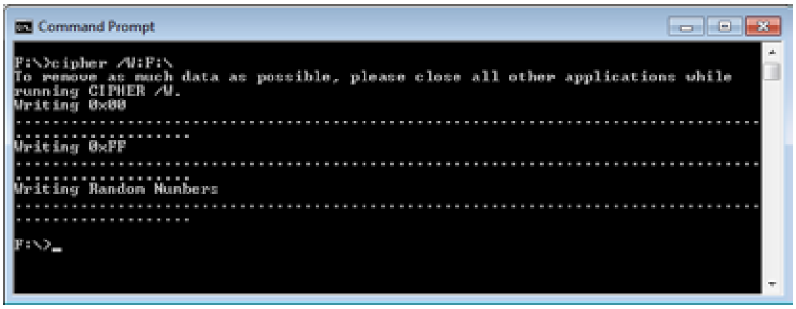
In January 2014, the Attorney General of California filed a complaint against Kaiser Foundation Health Plan, Inc. for the data breach of about 30,000 social security numbers. The SSNs were found left on an external hard drive which was then later purchased by a member of the public at a thrift store in Santa Cruz, California. You might think that Kaiser could have just deleted those files and they could have avoided this entire incident. Not really, read on.

This might come as a surprise: when you delete a file from a computer file system, it’s not really deleted in the way you would think. Rather, what your operating system (Windows, Mac, Linux, etc.) does is it “de-allocates” that file or folder so that the original space is marked as free space and available to be overwritten by new files. Until that happens, your deleted file or folder can actually be recovered by low-level disk utilities.

Of course, this is not a problem unless you intend to sell or donate or otherwise get rid of your old computer (or phone or tablet). Then you might not want anyone to be able to retrieve your files/data.

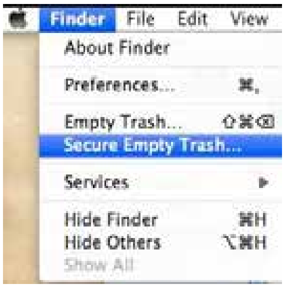
IT techies can stop reading here, but for the rest of us - just imagine your file system like a paper book. Your files and folders are the content and chapters in the book. When your computer system deletes a file or folder, all it really does is it **erases reference** to those chapters and contents from the table of contents. **It doesn’t actually erase the actual chapter**, so that content is still there. It can easily be recovered and lead to an unintended data breach. So even if Kaiser had just erased that external drive, a data breach could still have happened. They would have needed a strong method of ensuring that those files were actually deleted and can’t be recovered. Which leads to our topic.

There are several methods to better delete those pesky files. One is using applications you already have in your operating system and another is to use specialized software deletion applications. The National Institute of Standards and Technology (NIST) released a guide for Data Sanitization in September 2012 , but some of the techniques discussed might be too technical for most users. So here’s an easy way to help ensure deleted files on your computer are actually deleted. - On every copy of Windows starting with XP, there’s a utility called cipher.exe. Cipher.exe can overwrite your free space (the space containing your “deleted files”) with zeros (0s), then ones (1s) and then random data. It does this automatically for you in three passes and **helps prevent** the recovery of any deleted or “deallocated” data. You simply tell cipher.exe the drive letter with the command line: cipher /W:<directory>



```
F:\>cipher /W:F:\
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
...............................................................................
.....................
Writing 0xFF
...............................................................................
.....................
Writing Random Numbers
...............................................................................
.....................

F:\>_
```



For Mac users, it’s even easier. Under Finder, select Secure Empty Trash:

So remember, when you are about to decommission hardware, make sure to (1) delete the file contents and (2) use a free space wiping tool or a specialized one to really be sure. Some of the tools to do this are free and already on your computer, so be sure to at least use them.

http://www.goironbox.com/how-to-prevent-a-data-breach-kaiser-foundation-health-plan/