

Newsletter 6 June 2005

This newsletter is being sent to update our clients on technology developments...the provided items are those likely to be of interest to small and mid-sized businesses. It includes links to 3<sup>rd</sup> party sites and is intended to provide a quick drill-down to items of interest. Dolce Vita actively solicits the input of our clients as to issues which they would like to see addressed in these newsletters. This newsletter can be freely distributed to those you feel might be interested in its content. Please send suggestions to [lane.griffing@dvits.net](mailto:lane.griffing@dvits.net) or visit us at <http://www.dvits.net>. Obviously Dolce Vita IT Solutions assumes no responsibility for the content of these 3<sup>rd</sup>-party sites. To have your name removed from this mailing list, please e-mail to <mailto:lane.griffing@dvits.net?subject=Remove from Technology Newsletter>

**Dolce Vita IT Solutions is now Dolce Vita IT Solutions LLC** – On June 1, 2005 DVITS filed as an LLC in Oklahoma.

**DVITS is now a channel partner for Aladdin** – Please see <http://www.ealaddin.com>, especially the [information on eToken](#).

**Longhorn (next Windows version)** – Latest information we have indicates that the next version of Windows (currently code-named Longhorn) will be commercially released for desktops in 2006, with the server to be released in 2007. No good indications as to the hardware requirements, but its fairly safe to say that 1.5GHz+ processors and 1GB minimum physical memory would run the desktop version.

**Windows 2003 Server SP1** – Windows 2003 SP1 for Small Business Server was released in May...this is a different service pack from that released in March for Windows 2003. Issues with 2003 SP1 related to SQL installations are still being evaluated. All of our clients who use DVITS for admin will be “service packed” on 2003 by the end of June.

**Spyware issues and SPAM** – In May the level of SPAM rose to new levels, estimated at over 82% of all emails transmitted. These issues have become significant for nearly every business we talk to. Besides the obvious remedies of maintaining anti-virus which also deals with spyware, caution with browsing, and setting the browser up to prompt before installation of cookies there are other steps which can substantially help. Use content filtering (ie [WebSense](#), [Aladdin eSafe](#), etc.), plan to use multiple products (AdAware, SpyBOT, etc.), use SPAM filtering integrated with Exchange 2003, and use internal port blocking on the enterprise firewall.

Currently the use of Windows Server 2003, Exchange 2003, Windows XP Pro, and Office 2003 provide substantial protections due to their integrated security features and the simplicity of setting up suitable group policy objects (GPO) to control the network environment. However it takes some “tweaking” to maximize the effectiveness of these products. For those customers who do not use in-house e-mail, your ISP should already have SPAM controls available. Sometimes it does require a call or configuration of the e-mail account to turn these features on at the ISP.

### Critical Issues

**Legacy Systems – (From CIO Magazine)** Risk Management: Bound to Fail - Over the 2004 winter holidays, Comair's almost 20-year-old system for flight crew scheduling crashed, canceling or delaying 3,900 flights, stranding nearly 200,000 passengers, and eventually costing Comair and its parent company, Delta Air Lines, \$20 million--not to mention prompting an investigation by the U.S. Department of Transportation. Neither Comair nor Delta had taken steps to mitigate the risk the system posed, although the problem had long been identified. Legacy systems exist at the core of many businesses, and they cannot handle the velocity and volume of today's transactions. To avoid a Comair-like failure, CIOs must test these mission-critical applications

thoroughly, doing performance tests at least annually, simulating conditions that can lead to failure. They must make risk management an ongoing process.

<http://www.cio.com/go/index.html?ID=3663&PMID=15337426&s=3&f=1>

**Spyware** – Don't underestimate the damage which spyware can do to your network and the loss in productivity which it can cause. To learn more, take the following [quiz from Microsoft](#).

**Recent "Phishing News"** –

**May 13, Chicago Sun-Times** - Identity theft ring at doctors' offices. More than 100 patients who visited doctors belonging to two Chicago physicians' groups were the victims of an identity theft ring that tapped into the groups' records. <http://www.suntimes.com/output/news/cst-nws-hosp13.html>

**May 17, Finextra Research** - Nearly half of U.S. adults have been phished. Consumer studies conducted by First Data indicate that 6.8% of U.S. adults have been victimized by identity theft and 43.4% have direct personal experience of phishing fraud. The research, conducted in late 2004 by Synovate on behalf of First Data's Star Network, found that more than one-third of consumers surveyed had received a phishing e-mail, while 19% had taken a phishing phone call. On average five percent of consumers contacted fell for the scam and divulged personal details. Of those, 45% reported that the information was used to make an unauthorized transaction, open an account, or commit another type of identity theft. Nearly one-third of consumers said that the phisher had posed as a financial institution, while one in 10 reported that the phisher had impersonated a credit card company. Debra Janssen, president, First Data Debit Services, describes the survey results as worrying. "Close to five percent of phishing attempts are successful, despite significant efforts by the financial community to raise awareness and educate consumers about phishing. It's clear that more remains to be done." Research:

[http://www.star.com/pdf/IDTheft\\_Research\\_3\\_3\\_05.pdf](http://www.star.com/pdf/IDTheft_Research_3_3_05.pdf) Source:

<http://www.finextra.com/fullstory.asp?id=13681>

**June 1 - Organized Phishing Attacks and "Breeding" or cultivation for future attacks** – See E-Week article (<http://www.eweek.com/article2/0,1759,1823633,00.asp>) . This refers to the release of early versions of code which compromise workstations and server and create a new "backdoor" for future use. Some of the code used is intended to either damage or surreptitiously disable the existing virus scanning. This can be manifested by the spontaneous shutdown of the virus scanning services, or with the disabling of scanning schedules. The DVITS clients who are service-monitored have not been caused problems by these issues to date.

**"Spear-Phishing"** – Refers to phishing attacks which are directed to a subset of an organization. Since these attacks are directed and not mass-mailed, it is far easier for them to bypass SPAM defensive measures. An example would be a division of one company receiving a very genuine looking e-mail purporting to be from the agent which handles the company's retirement and 401K programs. Carried out over time, periodic requests to confirm or enter personal information may be successful.

Phishing is an even greater issue for those in accounting or HR who deal with an organization's banks and lenders on a daily basis. Please see additional information on phishing on the CERT website in the [2004 ECrime Watch Survey](#). Also see the US DOJ [CyberSweep website](#) which contains descriptions of several typical scams.

*If your organization is interested in additional online information or training concerning phishing or other human engineering exploits, please let us know as our contacts with the FBI and Secret Service have lots of great material available.*

**"Pharming"** Computerworld Magazine reports that "Pharming" attacks are increasing. (See article in Wired News <http://www.wired.com/news/infostructure/0,1377,66853,00.html>) -

Pharming is an exploit in which attackers modify an online site such that when a user logs in their traffic is re-directed without their knowledge to a nearly identical bogus site which proceeds to capture their valid login and password. This information is then used by the attackers to pursue other scams which obviously include identity theft.

**Recent Online Extortion Plots** - May 24, Associated Press - Web infection holds computer files hostage. Websense Inc., reported that hackers have found a way to lock up electronic documents on a target computer and then demand \$200 over the Internet to get them back. Websense uncovered the unusual extortion plot when a corporate customer they would not identify fell victim to the infection, which encrypted files that included documents, photographs and spreadsheets. A ransom note left behind included an e-mail address, and the attacker using the address later demanded \$200 for the digital keys to unlock the files. The FBI said the scheme, which appears isolated, was unlike other Internet extortion crimes. More typical extortion schemes involve perpetrators successfully footprinting and mapping a target network and installing back-doors which they can remote-control. They then contact the network owner (ie a bank, hospital, brokerage, telcom company) and threaten to bring the network down, dump customer information, etc. if the extortion demand is not met. These demands may go to \$500K+. Sometimes company management decides to quietly pay the extortionists as the costs of even a partial day of downtime may be substantially greater than the extortion demand.

**Windows Server Update Services** (formerly called Windows Update Services or WUS). Information is available at [WSUS page on Microsoft.com](#). This version has a different installation path than WUS...especially when Windows 2000 Server is used the order in which pre-requisite components are installed is critical. On Windows 2003 installations WSUS came up just fine, but we've seen several operational issues in the lower-reliability Windows 2000. DVITS has begun deployment of this technology with our clients in anticipation in summer of Office, SQL, and Exchange updates also being handled from this package. By mid-July all DVITS-administered clients will have been transitioned to WSUS.

**Multi-Factor Authentication** – We have two OKC clients and a Cincinnati client who have implemented Aladdin e-Tokens for multi-factor authentication (using smart cards) as well as for hard drive encryption. The eTokens are additionally being used with the [Web Sign-on feature \(WSO\)](#), which automatically retains logon credentials for websites and applications on the token and automatically logs in to these sites and applications. This reduces the need to have a list of logins close at hand which improves both employee productivity and security. Even if the USB token is lost or stolen, the data is not recoverable from the token. For those users who frequently use a variety of web-based applications, it is a phenomenal time-saver.

**Content Filtering** – DVITS is currently in the process of testing products from Sophos and Aladdin which deal with content filtering.

**May 17, vnunet - Lax security leaves networks wide open.** Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. Over 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus websites. Lack of awareness is key to this problem, according to the poll. Two thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training.  
Source: <http://www.vnunet.com/vnunet/news/2135301/lax-security-leaving-networks-wide>  
(DVITS notes: Be aware that having e-mail in-house with appropriate virus/malware scanning certainly helps here, but having appropriate corporate policies which are enforced as well as appropriate training is every bit as critical)

## Equipment

I'm not really into writing about hardware, but we are in the process of revamping the laptops for our consultants. One of the issues we are looking at is the use of laptops versus tablet PC's. We found an [interesting article from Microsoft](#) on the key issues to consider.

DVITS recently adopted HP IPAQ smartphones from TMobile. This device bundles a cell phone on a modified IPAQ PDA chassis and runs Windows Mobile as the operating system. Although we are only in the early stages of training, the ability to automatically move from GSM-based Internet access at about 40-56kbps to normal wireless speeds with existing WiFi infrastructure is fantastic. The ability to very quickly access our numerous Sharepoint sites, access Outlook shared e-mail and calendars, and use the Internet at normal wireless speeds adds to our responsiveness and flexibility. The ability to access GoToMyPC from a cell phone and actually work without opening a laptop is a tremendous benefit. We'll keep you updated as we pursue additional applications of Windows Mobile technology.