

Newsletter 1 May 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 3rd party sites and is intended to provide a quick drill-down to items of interest. Dolce Vita actively solicits the input from 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 or visit us at <http://www.dvits.net>. Obviously Dolce Vita IT Solutions assumes no responsibility for the content of these 3rd-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>

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 – In April Service Pack 1 was released by Microsoft. Along with some significant security enhancements there were some expected problems with applications running on the server. It is crucial to point out that the version of SP1 released was for 2003 Server ONLY. Attempts to apply this patch to Small Business Server 2003 will cause potential severe problems (like operating system failure). SBS 2003 SP1 is expected to be released in the next 60 days. [Info on SP1 can be found here.](#)

Spyware issues and SPAM – 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](#), 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

Phishing – This term has come into use to describe Internet “fishing expeditions” for personal information. It is an issue directly connected with SPAM in that an organization will send out a SPAM message directed to an authentic e-mail address which appears to be from a valid business (i.e. Citibank, American Express, Bank of America). The e-mail looks authentic enough to be real and requests confirmation of personal information (i.e. maiden name, Social Security number, address). The concept is that if a recipient actually has an account with Bank of America and attaches to the offered update link one of two things is likely to happen. First is that spyware in the form of a keystroke logger, etc. may be surreptitiously installed. Second is that if any information is provided then identity theft is almost certain to occur. It should be noted that in individuals identity information (name, address, social security number, account numbers, etc.) can fetch up to \$300 on the open market. If only 1 in 5000 recipients responds in any form, and you can buy a SPAM distribution list of 3 million people for \$1000 the math tells us that this can become lucrative very quickly. And 1 in 5000 responses is extremely conservative.

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.

Operating system updates – Microsoft has released Windows Server Update Services (formerly called Windows Update Services or WUS...can't imagine why they would change the name). Information is available at [WSUS page on Microsoft.com](#). Based on our lab experiences, deployment of WSUS must be properly planned. We would not recommend installation in a production environment until the user has deployed at least once in a lab environment. At this time WSUS will update the current Windows operating systems (none of you are running NT, 98, or ME, right?), Office 2003, and will eventually grow to encompass SQL, Exchange and several other business-essential products.

Content Filtering – DVITS is currently in the process of testing several products from [Sophos](#)...we'll pass along what we find.

New Cyber Attack Strategies – In recent weeks, additional attack codes are being written to attack key virus scanning websites (Norton, Trend Micro, etc.) in an attempt to reduce their automated patching capabilities. Some of the minor issues we've noted in recent weeks with Trend and McAfee may actually be rooted in some of these attacks. It is essential for administrators to check that virus scanning is functioning properly. Any changes in the numbers of machines registered with the scanning system, or substantial delays in updates of damage cleanup service templates should be investigated. At least a brief daily check is warranted.