IT@Diocesan House #7

INTERESTING WEBSITES:
This week we highlight some interesting reference sites. The first is for anything, and boy do I mean anything, on the web. Most of you know of it, but for those that don't, Wikipedia is an awesome online free encyclopedia policed by everyone. Some stuff needs to be researched further, but it is a good start for general info about nearly any topic and it links to related information quite nicely.

The second is a site devoted to computer technology definitions called Webopedia. So the next time you don't know what the geek speak means, check out Webopedia!

IT IN the NEWS:
From CNN.com:
Inventor: Camera phone evolution has only just begun
The chilling sounds of gunfire on the Virginia Tech campus; the hateful taunts from Saddam Hussein's execution; the racist tirade of comedian Michael Richards.
FULL STORY

Study: 25 countries block Web sites
At least 25 countries around the world block Web sites for political, social or other reasons as governments seek to assert authority over a network meant to be borderless, according to a study out Friday.
FULL STORY

Backlash against RFID is growing
Civil rights and privacy rights groups have opposed radio frequency identification, or RFID, for years. But now, researchers in the field and some lawmakers are beginning to voice concerns about the security of the technology.
FULL STORY

MySpace will turn over names of sex offenders
MySpace.com will provide a number of state attorneys general with data on registered sex offenders who use the popular social networking Web site, the company said Monday.
FULL STORY

Citywide Wi-Fi struggles to reach users
Adam DuVander likes to surf the Internet from his laptop wherever he happens to be -- at home, a coffee shop or a neighborhood park. He has been able to do so in recent years thanks to wireless hotspots set up by networking activists in Portland, Oregon.
FULL STORY

Beware of cellphone snoops

The nightmare begins early in the morning with an innocuous-looking e-mail on your mobile phone instructing you to check a specific Web site for information about repairing your credit score.
FULL STORY

Exclusive: Facebook's new face
Facebook may turn out to be a lot more important than any of us thought. It has just launched a major change in its strategy that will transform its role in the Internet ecosystem and could create a raft of new opportunities for companies of all sizes.
FULL STORY

Internet moms: Getting the best of both worlds
Jenni Hunt is an attractive, talented and ambitious professional from Portland, Oregon. She runs her own Internet business, selling on online auction site eBay and advising others how to navigate the site to gain maximum profits.
FULL STORY

From the Christian Science Monitor:
Parents turn to kids for tech support
Children are helping Mom and Dad complete online purchases and other Internet tasks, potentially altering family dynamics. By Marilyn Gardner
http://www.csmonitor.com/2007/0524/p17s02-lifp.html?s=hns

Video games, gas prices cut traffic to US parks
The number of visitors to nature-oriented national parks has been on the decline. By Ben Arnoldy and Brad Knickerbocker
http://www.csmonitor.com/2007/0525/p01s03-ussc.html?s=hns

From Christian Computing:
The Best Free Utilities and Applications
Inside the Box - Donald Stratton

Using Bible Software Effectively
WordSEARCH Word - Bob Dasal

Blog Sites and More
Scott Howard's Hotpics - Scott Howard

Whats Different About Business Continuity
Nick at Church - Nick Nicholaou

From Maclife.com:
Web Exclusive: Get More Out of iGoogle
Google does a great job bringing Web 2.0 to the world. Here are some tips to make the most of iGoogle, your personal Google homepage.

11 Foolproof Ways to Make Your Mac Secure
Don't dismiss security as something only Windows drones have to worry about - that attitude is dangerous. To safeguard both your data and your Mac, check out this common-sense guide.

News Roundup: New MacBook Pros, iMacs Coming; So Long, Freehand; Prepaid iPhones Rumored; and More
June is shaping up to be a big month for Apple, what with the iPhone's release and possible MacBooks Pros and iMacs on the runway. Plus, more iPhone news, buh-bye Freehand, the iGasm under fire, and more.

News Roundup: Apple to Dump the 17-Inch iMac, Advice on When to Buy a Mac, and More
Snap up a 17-inch iMac while you still can - word is that they're gone in June. Get some advice on the right time to buy a new Mac notebook. And even though it's a slow Apple-news day, the world keeps turning.

News Roundup: Windows-to-Mac Converter for Word, Amazon's DRM-Free Music, and More
Microsoft releases a beta version of a Windows-to-Mac Word-file converter, Amazon is set to offer DRM-free music, more iPhone and MacBook news surfaces, and a whole lot more.

From Macworld.com:
iPhone wins FCC approval, on track for June
Read the story

Paul McCartney's complete catalog coming to iTunes
Read the story

From PCWorld.com:
Chinese Hackers Grow in Number, Skills
China's hacking scene appears poised for growth, as Internet users rise along with interest in hacking.
http://www.pcworld.com/article/131992-1/article.html?tk=nl_dnxnws

Report: More Governments Filter Online Content
As more people use the Internet to inform themselves, more governments around the world want to filter what they read.
http://www.pcworld.com/article/131994-1/article.html?tk=nl_dnxnws

FCC Approves iPhone
The Federal Communications Commission approved Apple Inc.'s iPhone, clearing the way for the combined phone and music player to hit the shelves.
http://www.pcworld.com/article/131988-1/article.html?tk=nl_dnxnws

Apple Planning Thinner, Lighter Laptops
A new Apple patent posits portables that will be thinner and tougher than any

seen so far.
http://www.pcworld.com/article/132000-1/article.html?tk=nl_dnxnws

Windows Update for IE7 Doesn't Work for Some PCs
After installing this month's six-bug patch, some users aren't able to use the IE7 browser, Microsoft said.
http://www.pcworld.com/article/131973-1/article.html?tk=nl_dnxnws

15 Tech Myths: Busted and Confirmed
We examine common tech beliefs and do some digging to find out what's true--and what's trumped up.
Read the story

Vista Security Woes
Though Windows Vista may be safer than XP, Microsoft's far-from-impregnable new operating system is already proving to be vulnerable.
Read the story

Attention Shoppers: Check Stand 4 Now Open to ID Theft
Using your debit or credit card to pay for goods could be expensive if a scammer is bugging your store's keypad.
Read the story

How to Set Up a Wi-Fi Network
A Wi-Fi network is a great way to network your home PCs, stream media files, or share a Net connection. We'll show you how.
Read the article

Tips & Tweaks: Get Smart About Downloads
Tips and tools for downloading software; help staying awake during teleconferences.
Read the article

Linux Users Say 'Sue Me First, Microsoft'
Some users of Linux and other open-source software are inviting Microsoft to sue them.
http://www.pcworld.com/article/132108-1/article.html?tk=nl_dnxnws

Profit-Driven Viver Trojan Hits Smart Phones
New Trojan horse variants steal money from smart phone users by sending text messages to premium-rate numbers.
http://www.pcworld.com/article/132125-1/article.html?tk=nl_dnxnws

Office 2007 Left Unprotected in Update Snafu
Accordint to Microsoft, Office 2007 users running Windows Vista may not have

received a patch for "important" Excel and Office 2007 holes.
http://www.pcworld.com/article/132081-1/article.html?tk=nl_dnxnws

Spyware Bill Passes House
The U.S. House of Representatives passed an antispyware bill Tuesday on a voice vote.
http://www.pcworld.com/article/132143-1/article.html?tk=nl_dnxnws

Florida Bans Touch-Screen Voting Machines
Bill requires Florida precincts to replace Direct Recording Electronic machines with optical scan systems.
http://www.pcworld.com/article/132138-1/article.html?tk=nl_dnxnws

Wal-Mart Will Sell Dell PCs
Dell moves beyond direct sales to market two models of desktops through Wal-Mart in June.
http://www.pcworld.com/article/132221-1/article.html?tk=nl_dnxnws

Wi-Fi Poaching Draws Fine
A Michigan man was fined for using a local cafe's Wi-Fi connection from his parked car.
http://www.pcworld.com/article/132218-1/article.html?tk=nl_dnxnws

School-Porn Case Raises Computer, Spyware Questions
K-12 IT administrators search for better ways to protect school PCs as they wait for the June 6 sentencing of substitute teacher Julie Amero.
http://www.pcworld.com/article/132169-1/article.html?tk=nl_dnxnws

New Antiphishing, Antispam Specifications Unveiled
DomainKeys Identified Mail, a proposed standard for e-mail authentication, would help fight spam and phishing attacks.
http://www.pcworld.com/article/132203-1/article.html?tk=nl_dnxnws

From ITBusiness Edge:
Microsoft Incorrectly Uses Report Backing Patent Claims, Says Author :: out-law.com

Open Source Community Unafraid of Microsoft :: iTWire

Analyzing the Open Source Patent Claims of Microsoft :: Seattle Post-Intelligencer

Is It the End of the (Free) World as We Know It? :: CNNMoney.com

Little Fear from Open Source Community over Microsoft Royalty Threats :: CIO.com

New Bill to Attack Cybercrime :: FCW.com

Forrester: IT to Increase Security Budgets :: IT Week

From Techtarget.com:
Report: Techies anxious about lack of business skills
http://go.techtarget.com/r/1467634/5300425

Budget battle: Increasing the business value of IT
http://go.techtarget.com/r/1467635/5300425

Spyware may be a losing battle, experts say
http://go.techtarget.com/r/1474620/5300425

Next-generation spyware
http://go.techtarget.com/r/1474621/5300425

Web Filtering Stops What Firewalls and Antivirus Miss
http://go.techtarget.com/r/1476370/5300425

From Microsoft:
Office 2007 tips & tricks
Register now to view short webcasts on how to streamline your everyday tasks. Start saving time today.

If you have Windows XP, here are some tips to help keep your PC more secure. You can also download Windows Defender (automatically included with Windows Vista) for free spyware protection.

6 secrets to strong passwords
Make your PC passwords tough to crack--follow these guidelines and avoid the most common pitfalls.

Why upgrade to Internet Explorer 7?
Columnist Sandi Hardmeier explains why security and productivity features in Internet Explorer 7 make it worth the upgrade.

5 time-saving tips for Word 2003
See how Word can help you cut down on the time you spend doing repetitive tasks.

WHITE PAPERS
Demystifying wireless network access and 802.1X security
Published by: Fluke Networks
http://go.techtarget.com/r/1460954/5300425

Evolution of mobile data

Published by: Sprint
http://go.techtarget.com/r/1460955/5300425

Messaging Management for Small and Mid-sized Businesses
http://go.techtarget.com/r/1473014/5300425

SECURITY News:
From SANS:
--Estonian Websites Under Attack
(May 10 & 17, 2007)
Web sites throughout Estonia have been under attack for the past three weeks. Riots and protests broke out on April 27 when Estonia removed a Soviet war memorial statue in the capital city of Tallinn. Ethnic Russians protested the statue's removal. Russia is suspected of being behind the attacks, but no accusations have been made. The distributed denial-of-service (DDoS) attacks have hit across the board at government web sites as well as web sites of newspapers, banks and businesses. NATO has sent cyber terrorism experts to Tallinn to help the country improve its cyber defenses.
http://www.guardian.co.uk/russia/article/0,,2081438,00.html
http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
[Editor's Note (Liston): I find this incident to be troubling on many levels. While there is a great deal of disagreement on whether or not the Russian government is participating in this attack, the effectiveness of this DDoS highlights the potential for third-party agitators to potentially exacerbate an international incident. Rapid, accurate and positive attribution of this type of cyber-attack is essentially impossible, which almost invites "interested" third parties to use it as a means of stirring up trouble on an international level. (Ullrich): During the China-US standoff about the spyplane that was shot down in 2001, Chinese hacker groups defaced US websites and US hacker groups retaliated. None of these attacks amounted to more than a nuisance. It is likely that the attacks against Estonia are similarly inspired by patriotism and not necessarily government controlled. However, as the importance of cyber warfare increases, better methods are needed to determine attribution of attacks. (Honan): Arbor Networks have an interesting entry in their Security to the Core Blog outlining a summary of these attacks as seen by them, http://asert.arbonetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.
While TERENA has details on how the European CSIRT community is assisting Estonia in dealing with the attacks,
http://www.terena.org/news/fullstory.php?news_id=2103]

--Former Computer Repairman Allegedly Stole School Servers
(May 11, 2007)
A man who once worked for a contractor repairing computers at a Houston, TX school district has been accused of stealing machines from the schools. The suspect has not worked for the contractor since February 2007, but he kept his

ID badge, which allowed him access to the buildings from which the computers were stolen.
http://www.khou.com/news/local/houstonmetro/stories/khou070511_tj_computertthefts.5e2c149b.html
[Editor's Note (Kreitner): This episode illustrates one of the most frequently neglected operational security controls requiring timely human action, namely the termination of physical and electronic access to enterprise assets for departed employees, contractors, vendors, and strategic partners. (Grefer): Part on any organization's exit protocol should be to collect all physical credentials and to disable and/or revoke any logical credentials and authorizations.]

--Credit Card Fraudsters Sentenced
(May 10, 2007)
Five people convicted of what UK police called a "sophisticated" credit card fraud scheme have received jail sentences of as long as five-and-a-half years. The group possessed 32,000 stolen credit card numbers. Officials suspect the stolen data came from a US database. The five used the stolen credit card numbers to fund a profligate lifestyle. All have been recommended for deportation upon completion of their sentences.
[Editor's Note (Northcutt): The photo mug shots are priceless, worth clicking on the link. Speaking of link, all the articles on this subject refer to a "link man" from Estonia. This is a new term for me, and I couldn't find it commonly used outside of the article. The following snippet from the story is also illuminating: "The computer encryption systems which were used were very sophisticated and they have to some extent, despite police efforts, defied attempts to decode them." Shucks, in another couple thousand years you'll have it, keep at it is my advice *grin*.]

--Malware For All
(May 17, 2007)
As a social experiment, someone bought an ad on Google that offered to infect people's machines with malware. The ad read, "Drive-By Download. Is your PC virus-free? Get it infected here!" Over a period of six months, the ad was clicked on 409 times; it was displayed 259,723 times. That works out to a rate of 0.16 percent. Clicking on the link supplied took users to a .info web site. This particular site did not contain any malicious code.
Internet Storm Center:
http://isc.sans.org/diary.html?storyid=2811
http://www.theregister.co.uk/2007/05/17/spoof_malware_campaign/print.html
http://it.slashdot.org/article.pl?sid=07/05/15/2216235
http://www.eweek.com/article2/0,1759,2132447,00.asp?kc=EWRSS03119TX1K0000594
[Editor's Note (Northcutt): Great story. From memory, the researcher spent a total of 208 dollars. However what is interesting is that some of the convictions for people setting up malicious web sites to load bots on vulnerable web surfing computers explicitly stated they had loaded the code without the user's

permission. A 0.16 acceptance rate for a "get out of jail free card;" that gets interesting. (Schultz): Although a gullibility rate of only 0.16 percent is in theory good, it is still troubling that anyone would be so foolish as to intentionally infect one's own computer. What would be even more interesting would be to compare gullibility rates over time, e.g., at six month intervals, to see if there are any changes and if so, why. (Liston): It would be interesting to compare the click-through rate on the bogus ad to the click-throughs on, say, an ad for anti-virus or anti-spyware software.]

--Glitch Leaves Office 2007 Users Running Vista Unprotected
(May 21, 2007)
Microsoft has "updated the detection logic for the May 8th Security and Non-Security Updates for Office 2007." The original detection logic in some cases failed to offer the updates or failed to install updates correctly on systems running Vista. Vista users who are offered the updates again should install them. The issue affects MS07-023 and MS07-025.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020262&source=rss_topic17
http://blogs.technet.com/msrc/archive/2007/05/17/new-detection-logic-for-may-8th-office-2007-updates.aspx

--New Gozi Trojan Variant Spreading
(May 19, 2007)
A new variant of the Gozi Trojan horse program has been spreading since mid-April. The malware grabs data from encrypted SSL streams and sends them back to a server in Russia. The upstream ISP cut the server off from Internet connection once it was alerted to the situation. The malware has gathered sensitive information, including bank account and credit card numbers, user names, passwords and Social Security numbers (SSNs) of more than 2,000 people. Changes apparent in the new version of Gozi include the addition of a packer utility that helps the malware evade detection by standard virus signatures and a keystroke logging capability that increases the amount of information it can steal. Gozi exploits a known flaw in Microsoft's Internet Explorer (IE) iFrame tags.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019978&source=rss_topic17

--Critical Flaws in Java Development Kit
(May 17, 2007)
Java Development Kit users running version 1.x are encouraged to upgrade to protect their systems from two remotely exploitable flaws. The first flaw is an integer overflow error in the image parser that occurs when processing ICC profiles embedded in JPEG images; the flaw could be exploited to crash the JVM (Java Virtual Machine) and possibly allow arbitrary code execution. The second flaw is due to an error in the BMP image parser when parsing malformed files on Unix/Linux systems and could be exploited to cause denial-of-service conditions.

Sun Microsystems has released JDK versions 1.5.0_11-b03 and 1.6.0_01-b06 to address the flaws.
http://www.eweek.com/print_article2/0,1217,a=207757,00.asp

NEWS FROM SNOPES.COM
Does the oceanliner the QE2 use a gallon of fuel for every six inches she travels?
Strange and unusual demises populate the "2006 Darwin Award" list.
Pet danger warning: Xylitol, a sugar substitute used in sugar-free gum, is toxic to dogs.
Sofa set sold in Canada bore a surprisingly racist tag.
Drug user attempts to beat drug test by drinking bleach.
Mother's Day special: Deceased mom finds a way to tell her son what their last dinner together meant to her.
Legend from the 1980s about a driving examiner run over during a road test he was administering.

WORMS, ACTIVE EXPLOITS, VULNERABILITIES & PATCHES
From SANS:
--Microsoft Advanced Notice Service Will Add More Details
(May 17, 2007)
Starting in June, Microsoft will provide more details about upcoming security bulletins in its advanced notification service (ANS). Information provided through ANS has been limited to software affected, maximum severity ratings for each bulletin, and whether or not each bulletin would require a restart. As of Thursday, June 7, advance notices will include vulnerability impact and necessary detection information as well as the information noted above. The change was made in response to customers' feedback indicating they want "more time and information ... to plan for testing and deployment." The format of the bulletins has been revised as well.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019720&source=rss_topic17
http://blogs.technet.com/msrc/archive/2007/05/16/ans-and-security-bulletin-updates.aspx
[Editor's Note (Ullrich): The purpose of these advanced notices is to enable companies to schedule manpower ahead of time. With the current system, one never knew how many critical patches Microsoft would announce. The new system should be more granular, and I doubt it will provide information of value to the "bad guys". (Honan): Microsoft's monthly release of patches has improved the security of many organisations by allowing them to better plan and prepare for patching their Microsoft based systems. This improvement in the Advanced Notice Service further enhances this capability and Microsoft should be commended for listening to their customer feedback and improving the service. Hopefully other vendors will follow suit.]

HIGH: Symantec Norton Internet Security and Personal Firewall ActiveX Control Vulnerabilities Affected:

Symantec Norton Internet Security 2004
Symantec Norton Personal Firewall 2004
Description: The Symantec Norton Internet Security and Personal Firewall products are shipped with an ActiveX control. This control is vulnerable to a buffer overflow that can be triggered by specially crafted parameters to its "Get" and "Set" methods. A malicious web page that instantiates this control can successfully exploit the buffer overflow to execute arbitrary code with the privileges of the current user.
Status: Symantec confirmed, updates available.
Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the responding council sites. They reported that no action was necessary.
References:
Symantec Security Advisory
http://www.symantec.com/avcenter/security/Content/2007.05.16.html
SecurityFocus BID
http://www.securityfocus.com/bid/23936

Peace,
Kat

Kat Lehman
Information Technology Coordinator
Diocese of Bethlehem
610-691-5655 x235
klehman@diobeth.org