



The Paper Modem

February 2006 Volume 6 Issue 1

Inside this issue:

Page

Goodbye, Au Revoir, Adios, Totsiens	1
Happy Birthday Computer Virus 20 Years old Now	2
Internet Explorer 7	2
Google? Napster ?	4
High-Tech Hits the Road	4
PC Humour	4/5/10
Build A Better Password	6-10
BlackWorm	10
What is	11



What Happens After June 30th, 2006?

Microsoft's support for Windows 98 & Windows Millennium ends on June 30th, 2006.

Windows 2000 moves out of Mainstream support into Extended Support on June 30th, which means that you must have Service Pack 4 to receive further Security Updates, support for Windows 2000 ends June 30th, 2010. *(To download SP4 for Windows 2000, type the following into your Google Search Window "Download SP4 for Windows 2000", this will lead you several links to Microsoft's Download page.)*

Microsoft is working on releasing Internet Explorer 7, Minimum requirements to run this new version of IE is expected to be Windows, XP with SP2, and the yet to be released Windows Vista. According to Microsoft IE7 will be loaded with security items and new features.

Service Pack 3 for XP will be released after Windows Vista, expected to be in the 3rd quarter of 2006. *(Please note that Microsoft has not given a definite date for any of the releases)*

Do you know if your Windows 98 or Millennium computer is a good candidate for an Upgrade?

Submitted By: Y.Bulger



A day without sunshine is like, night.



Product Watch

By: Kamil Z. Skawinski

Sure, you've got some impressive hardware, but are you protecting it?

Believe it or not, the computer virus has just celebrated its twentieth birthday-and ever since "Brain" was first discovered in the wild back in early 1986, computer users have

found themselves continually on the defensive, protecting their hardware and software with technologies that in many ways mimic the defenses of Medieval times.

Just as in ages past, much treasure has been sacrificed to keep all and sundry besieging barbarians at bay. But instead of building ramparts, moats, drawbridges, towers and keeps, our hard-earned dollars are being expended on up-to-date anti-spam, anti-spyware, antivirus and fire-wall applications to keep code-borne mischief-makers out

of our digital domains.

It's estimated that over 150,000 malicious programs are floating around within the digital universe today and, according to the FBI, dealing and recovering from their attacks costs the average U.S. business about \$24,000. If you own or operate a small office or home office, you can ill afford such a financial burden (not to mention the downtime and data loss). Consequently, you need to be adequately prepared.

The good news is that the vast majority of available retail anti-virus and Internet security products are all rock-solid and dependable in terms of the protection they yield. That said, however, you will find there are differences among products that make some a better choice than others depending on your particular needs, preferences and/or your computer platform. Below are synopses of Internet-security products worthy of consideration, among them a new and compelling product you'll now find appearing at retailers this month.

Submitted by: G. Bulger

Microsoft Releases IE 7 Beta to public

By [Alorie Gilbert](#), CNET

[News.com](#)

Published on [ZDNet News](#): January 31, 2006, 9:00 AM PT



said.

The new browser also includes tabbed browsing and a search box on a more streamlined toolbar, con-

cepts that should be familiar to users of Firefox, a rival browser distributed by the Mozilla Foundation.

Microsoft took the wraps off Internet Explorer 7 Tuesday, releasing the new "preview" version of its Web browser to the general public for testing. The latest version works only with Windows XP Service Pack 2 and includes many of the features Microsoft has been touting for months. Among them are new security and privacy protection capabilities such as mechanisms designed to combat phishing attacks, spyware and other threats.

Microsoft said that the new Printing Enhancements and Shrink to Fit printing features enable users to adjust margins, change the page layout, remove headers or footers, and increase or decrease the print space.

Another new feature lets users clear their browsing history more easily and thus wipe out passwords, form data and cookies in one click, the company

Tabbed browsing lets users open multiple Web pages in a single browser window. Microsoft has tried to best Firefox with something called Quick Tabs. That feature provides an at-a-glance, thumbnail view of all open tabs in a single window.

(Continued on page 3)



Artificial Intelligence usually beats real stupidity.

(Continued from page 2)

In addition, the program is supposed to let users more easily subscribe to syndicated feeds from news and sports sites, blogs and stores.

The browser detects feeds enabled by Real Simple Syndication, or RSS, technology, illuminating an icon on the toolbar. Users can preview, subscribe and scan syndicated headlines directly through the browser, Microsoft said.

IE 7 also includes a number of new features for Web developers, including support for up-and-

coming Web-programming technologies known collectively as Ajax.

Microsoft plans to release a final version of IE 7 later this year, around the time the company debuts the next version of its Windows operating system, Windows Vista.

Submitted by: Y. Bulger



Google Denies Napster Tie-Up, Music Store Plan



Juan Carlos Perez, IDG News Service Tue Jan 31, 5:00 PM ET

Google today refuted recent reports that it will open an online music store and that it plans to acquire Napster.

In the digital music market, Google is sticking with its strategy of delivering music information via its search engine and providing its users with links to third-party online music stores, the Mountain View, California, company said in a statement.

Napster's stock shot up more than 50 percent at one point on Tuesday after the *New York Post* reported in an anonymously sourced article that Google "is considering an extensive alliance with Napster, which could include an outright acquisition."

Napster

Napster operates an online music store and an

online music subscription service, a hybrid model in this market. Users can purchase songs or entire albums, download them from the store and keep them forever. They can also pay a monthly fee and get unlimited access to the contents of the Napster music library.

Napster's stock closed at \$3.12 per share on Monday, but climbed as high as \$4.95 on today, fueled by the *Post* story. At press time, it was trading at \$3.77, up about 21 percent. In the past 12 months, it has fluctuated between \$2.95 and \$9.84.

Last week, Bear Stearns financial analysts speculated in a research report that Google is building an online music store to rival Apple Computer's iTunes.

Making clear that Google hadn't confirmed their speculation, the analysts wrote that they expect the search giant to release a beta, or test, online music store in the next three to six months.

Submitted by: Y. Bulger



C program run. C program crash. C programmer quit.

High Tech Hits the Road

PC World

For many people, their cars have become an extension of their homes--and we're not just talking about all the food wrappers on the floor. In fact, the evidence was all over this month's Consumer Electronics Show in Las Vegas: High technology is hitting the highway in a big way. What does that mean exactly? It means if there's a high-tech device in your house, you're likely to find a version of it for your car--if not this year, then soon after.

Case in point: In 2006 we'll see navigational devices that not only tell you where to go when you're lost, but also play satellite radio, movies, and MP3s. We may even see the first true off-the-shelf car PCs, though whether you'll want to buy one is another story.

At CES, AudioVox unveiled its \$2999 ICNAV3PC, a fully functional Microsoft Windows XP system that squeezes into your car's dashboard and sports

a 7-inch touch-screen LCD, a 40GB hard drive, a 1-GHz processor, 512MB of RAM, and a Global Positioning System receiver, plus navigation software.

The computers are supposed to be available this spring. Just make sure that when Windows inevitably crashes, the car doesn't.

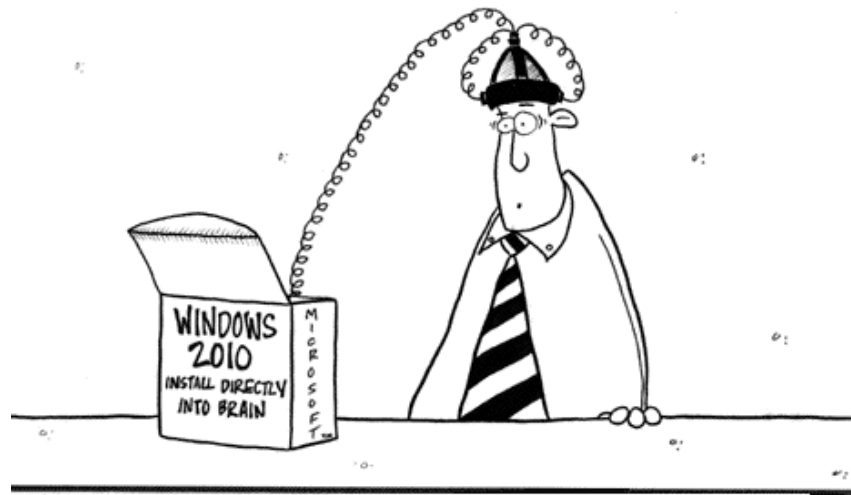
A PC may be the last thing you want to put in your car. If you've got the cash, though, there are plenty of other high-tech ways to impress your neighbors. Here's a view of the road ahead.

DVD players and little LCD displays are already de rigueur if you want to travel with kids without losing your sanity; satellite radio has gone mainstream; and a slew of gadgets can connect your favorite MP3 player to your car stereo. But you ain't seen nothing yet.

Submitted by: *Y. Bulger*

To read the rest of this article go to:

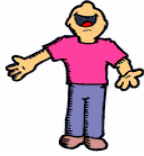
http://www.cesweb.org/default_flash.asp



Windows 2010. Instalation straight into your brain



Don't take life too seriously, you won't get out alive.



Just for Laughs

Things You Don't Want To Hear From Technical Support

- "Do you have a sledgehammer or a brick handy?"
- "That's right, not even McGyver could fix it."
- "So -- what are you wearing?"
- "Duuuuuude! Bummer!"
- "Looks like you're gonna need some new dilithium crystals, Cap'n."
- "We can fix this, but you're gonna need a

butter knife, a roll of duct tape, and a car battery."

- "In layman's terms, we call that the Hindenburg Effect."
- "Hold on a second... Mom! Timmy's hitting me!"
- "Okay, turn to page 523 in your copy of Dianetics."
- "Please hold for Mr. Gates' attorney."

Submitted by: Y. Bulger



Remember when.....

A computer was something on TV
from a science fiction show of note
a window was something you hated to clean
And ram was the cousin of a goat

Meg was the name of my girlfriend
and gig was a job for the nights
now they all mean different things
and that really mega bytes

An application was for employment
a program was a TV show
a cursor used profanity
a keyboard was a piano



Memory was something that you lost
with age
a cd was a bank account
and if you had a 3.5" floppy
you hoped nobody found out

Compress was something you did to the garbage
not something you did to a file
and if you unzipped anything in public
you'd be in jail for a while

Log on was adding wood to the fire
hard drive was a long trip on the road
a mouse pad was where a mouse lived
and a backup happened to your commode

Cut you did with a pocket knife
paste you did with glue
a web was a spider's home
and a virus was the flu

I guess I'll stick to my pad and paper
and the memory in my head
I hear nobody's been killed in a computer crash
but when it happens, they will wish they were dead.



Friends may come and go, but enemies tend to accumulate.

Build A Better Password

Enhance Your Online Security

Online passwords are a lot like visits to the dentist--we know we need them, but they can be an ordeal. They are a necessary security measure but can also be a huge annoyance. Forget one, and you could spend the next hour searching your file cabinet for a hard copy of the email tech support sent you two years ago. Let one slip into the wrong hands, and you could lose your privacy, your money, or perhaps even your identity.

According to the latest FBI Computer Crime Survey, cyber-criminals pilfered more than \$1.25 billion in 2004, an increase of 22% from the previous year. Online theft and fraud--136,572 separate incidents--accounted for more than half of the total. Most of the fraud losses were the result of brute force break-ins, purloined personal data, or unsuspecting computer users duped (often through phishing schemes) into revealing login information.

As online crime is increasing, we are also becoming more dependent on online services. There's the bank, stock broker, news service, music-download site, health provider, auction house, employer site, florist, and a host of others. Every one of those services represents an opportunity for online theft.

The danger is real and immediate. However, before you cut your DSL (Digital Subscriber Line) cable, read ahead for several simple techniques and one powerful mathematical tool that can greatly increase your on-line security.

Password DOs & DON'Ts

The quickest way to improve your defenses is to make sure your password and username choices are not actually making the job easier for password crackers. Here are some simple guidelines that will immediately improve your passwords.



Don't use your actual name for your username. It's a point of pride for many early joiners of online services that they were able to snag their real names as usernames. It may be a badge of honor and quite convenient, but having your full or partial name as your username means that you've made the Internet intruder's job only half as difficult--now he only has to discover your name to figure out your password.

Do use an unassociated or random word as your username. This will make it twice as hard to break through your security screen. You can use the same username for all your logins, but using a different username for each login or online site will provide the best security. The bad news is that many companies have standardized the way they assign usernames--such as using users' email addresses--and some won't allow their customers to change them.

Don't use a common word, name, or phrase. Crackers, who are basically online crooks, will often attempt brute force attacks. They program automated cracking computers to toss every word in the English language at your login screen until they get in. It may take them hours or days, but their computers don't care. They just keep going until they find the right combination. So if you thought the word "zygote" was a powerful password, it might only provide only a few more minutes of security than the word "aardvark."

Don't use personal information. More sophisticated crackers may have access to some of your personal information, giving them clues to obvious password choices, such as a child's name, mother's maiden name, or birth date. This is called a **familiarity crack**. Much of this information is available online or can be purchased at low cost. So, even though your daughter's birthday is easy to remember, you should never use it as your password.

(Continued on page 7)



If you lend someone \$20, and never see that person again; it was probably worth it.

(Continued from page 6)

Do use a combination of random letters and numbers. This will protect you against most brute force or familiarity attacks.

Throw Away The Key & Burn The Sacred Scrolls

Even if you've created a challenging login, you still need a way to manage the plethora of passwords from all those sites. However, many of us rely on one of two common methods--Master Key or Sacred Scrolls--that actually make us more vulnerable to unscrupulous netizens.

Practitioners of the Master Key method solve the problem of password glut by using the same password for everything. Sure, it's easy, but the really bad news is that if the wrong person gets hold of your Master Key password, you will be left naked on the Internet.

Subscribers to the Sacred Scrolls method use multiple passwords, but write them all on a single list and hide it somewhere--often on a Post-it Note stuck to the underside of the desk drawer. (And you thought you were the only one.) This is the digital equivalent of hiding a key under the doormat: It's the first place a crook looks. Sacred Scrolls aren't very convenient, either. You can only access password-secured sites from a computer near the list--unless you foolishly carry a copy of the list in your wallet, store the list on the computer you're trying to protect, or hide duplicate lists in other locations.

A Little Math Goes A Long Way

There is another option for password protection--the password algorithm.

A **password algorithm** is a simple mathematical formula used to create a unique, memorable password for each login. It offers significantly enhanced security compared to the Master Key or Sacred Scrolls methods because each password is differ-

ent and you don't need to write anything down.

The basic password algorithm starts with a **root string**, which is modified according to a particular site's name. The root string can be a common word or even memorable gibberish. It's best not to use an obvious word such as your child's or spouse's first name. Your middle name or the name of the street where you grew up would be a better choice.

Here's an example of a simple password algorithm. We'll use Edward, as the "middle name" root string. Then, we'll add the two-digit numeric equivalent of the first letter of a Web site name to the end of the root word to generate a unique password for the site. According to this simple algorithm, the password for Yahoo! would be edward25, your middle name plus the number 25, as "Y" is the 25th letter of the alphabet. Using the same algorithm, the password for Amazon.com would be edward01, "A" being the first letter of the alphabet. The password for eBay would be edward05. Get the idea?

Another variation is to increase the number of letters of the Web site name used to create the numeric values and then interleave them with the root word. For example, if we interleave Mr. Brown's first name, Buster, and the first three letters of Yahoo!, the resulting password would be 25b01u08s.

Using the same algorithm, a Hertz.com password would be 08b05u18s.

While this basic algorithm offers substantial security compared to the Master Key or Sacred Scrolls methods, someone might be able to deduce what you're doing from a single password. However, add a trick or two, and you will baffle even the most clever cracker.

For example, take a look at this password for Yahoo!:

dr09aw02de26. To the



8)



Hard work has a future payoff. Laziness pays off now.

(Continued from page 7)

uninformed, it looks like another random computer-generated password--pretty tough to crack. Looks are deceiving--this algorithm is almost as simple as the previous examples. There are just two simple twists. First, the spelling of the root word, Edward, has been reversed. Second, each of the alphanumeric values from the Web site name has been increased by one. Using this algorithm, the password for Expedia is dr06aw25de17:

dr The last two letters of the root reversed

06 The alphanumeric for the first letter of Expedia (e) + 1

aw The two middle letters of the root reversed

25 The alphanumeric for the second letter of Expedia (x) + 1

de The first two letters of the root reversed

17 The alphanumeric for the third letter of Expedia (p) + 1

While this algorithm is a little more difficult than the first examples, when used often, it will be easy to remember because the dr, aw, and de segments will always be the same.

You can mask the algorithm even more by using a memorable date or number as your root. As with your selection of a root word, it's best not to use an obvious number or date, such as a family birthday or street address. An anniversary or high school graduation date is a better choice. For this example, a let's use Sept. 11, 2001. We'll write that as 010911. To obscure things even more, let's increase each letter's numeric value by



one. For this example, a let's use Sept. 11, 2001. We'll write that as 010911. To obscure things even more, let's increase each letter's numeric value by

one.

With this algorithm, the Expedia password would be 010609251117:

01 The year

06 The alphanumeric for the first letter of Expedia (e) + 1

09 The month

25 The alphanumeric for the second letter of Expedia (x) + 1

11 The day

17 The alphanumeric for the third letter of Expedia (p) + 1

The same algorithm generates 010909021126 as the password for Yahoo!.

The combination of methods greatly enhances password security. Even if a cracker has an idea what you are doing, it would be difficult to reverse-engineer the algorithm.

Here are a few more variations that will also enhance security:

- If the site name ends in a vowel, add to the numeric values. If it ends in a consonant, subtract.
- Use a different root word for each type of domain.
- If there is an odd number of letters in the site name, reverse the order.
- Add a short string of mixed letters and numbers to the end or beginning of the password.
- Periodically change your algorithm. It's a lot of

(Continued on page 9)



If you choke a Smurf, what colour does it turn?

(Continued from page 8)

work, but your security is worth it.

- If you can change your username, use an algorithm for it, too. It's double the math, but it's also double the security.

Make The Changes

You can mix and match any or all of the above options to create an amazingly cryptic--but easily calculated--personal password algorithm. With just a little practice, you'll be able to easily reconstruct the password in your head in just a few seconds. Don't be too concerned about the letter-to-number



D-Day for virus

By Louisa Hearn
February 2, 2006 - 4:05PM



Tomorrow is D-Day for a dangerous computer virus which has spread throughout the world via email and is programmed to destroy PC files on February 3.

Email messages with risqué subjects like "give me a kiss" and "school girl fantasies" have helped to spread the virus across about 300,000 computers worldwide according to a taskforce set up to monitor the threat.

The virus is known under several different names including Blackworm, Nyxem, CME-24, Blackmal, Kama Sutra and MyWife.

The Blackworm taskforce, which comprises a large number of security organisations, warns that although those with recently updated anti-virus and anti-spyware should be protected from attacks, the virus was built to disable a number of security packages. This means that those PCs that were already infected before the most recent anti-virus signatures were downloaded could still be vulnerable. Once a PC is infected, the virus will replicate and send itself to all of the user's email contacts and will then lie dormant until February 3. On this date it will begin destroying a wide

range of files including Word, Powerpoint, Excel and Acrobat on infected machines. If it is not removed, it will attack again on the third day of each month going forward.

According to computer emergency response team AusCERT, the virus has attracted so much attention because it is the first to carry such a destructive payload for quite some time.

"Recent movement has been away from purely destructive worms towards for-profit viruses like keystroke loggers for and bot net clients," said security analyst, Chris Horsley.

AusCERT has been tracking its frequency in Australia and said that based on worldwide infection figures, it estimated that about 1000 PCs in Australia would be affected.

"The worst affected regions are India, Peru and the US," it said. AusCERT recommends applying strong passwords to all user accounts, updated anti-virus and anti-spyware protection, and the use of a firewall.

Submitted by: Y.Bulger



Laughing stock: cattle with a sense of humour.

(Continued from page 9)



translation. After a short time, you'll be translating entire words into numbers with ease.

The last step in the process is to get all of your online sites updated with your new passwords. Changing the password on many sites is as easy as clicking to the account setup page and selecting Change Password. For some sites, though, you may have to contact the administrators to request a change in your password or username.

Once you've reconfigured your passwords, your online life will be far more secure. You'll have a

unique password for every site, always know what they are, and never have to write anything down.

Just imagine . . . you could be in the middle of a Parisian vacation when, after some extreme shopping along the Champs-Élysées, you realize you need to transfer some money into your checking account. No problem. Just find an Internet café, head to your bank's online site, and calculate your password. Complete the transaction, secure in the knowledge that no one with access to the cyber café's system would be able to deduce the password you used.

Submitted by: Greg Wilson



Good judgment comes from bad experience and a lot of that comes from bad judgment.



What is



ActiveX

ActiveX is a technology developed by Microsoft which may make plug-ins less necessary. ActiveX offers the opportunity to embed animated objects, data, and computer code on Web pages. A web browser supporting ActiveX can render most items encountered on a Web page. For example, Active X allows users to view three-dimensional VRML worlds in a Web browser without the use of a VRML plug-in. As another example of the power of ActiveX, this technology can allow you to view and edit PowerPoint presentations directly within your Web browser. ActiveX works best with Microsoft's Internet Explorer browser.

Hypertext

The operation of the Web relies primarily on hypertext as its means of information retrieval. HyperText is a document containing words that connect to other documents. These words are called links and are selectable by the user. A single hypertext document can contain links to many documents. In the context of the Web, words or graphics may serve as links to other documents, images, video, and sound. Links may or may not follow a logical path, as each connection is programmed by the creator of the source document. Overall, the WWW contains a complex virtual web of connections among a vast number of documents, graphics, videos, and sounds.

Producing hypertext for the Web is accomplished by creating documents with a language

called HyperText Markup Language, or HTML. With HTML, tags are placed within the text to accomplish document formatting, visual features such as font size, italics and bold, and the creation of hypertext links. Graphics may also be incorporated into an HTML document. HTML is an evolving language, with new tags being added as each upgrade of the language is developed and released.

HTTP (HyperText Transfer Protocol)

Transmits hypertext over networks. This is the protocol of the WWW.

Many other protocols are available on the Web. To name just one example, the Voice over Internet Protocol (VoIP) allows users to place a telephone call over the Web.

The World Wide Web provides a single interface for accessing all these protocols. This creates a convenient and user-friendly environment. It is no longer necessary to be conversant in these protocols within separate, command-level environments. The Web gathers together these protocols into a single system. Because of this feature, and because of the Web's ability to work with multimedia and advanced programming languages, the World Wide Web is the fastest-growing component of the Internet.

Submitted by: Y. Bulger



The End